Руководство пользователя систем Dell™ PowerConnect™ 35xx

Введение
Описание аппаратного обеспечения
Установка PowerConnect 3524/P и PowerConnect 3548/P
Настройка PowerConnect 3524/P и 3548/P
Использование Dell OpenManage Switch Administrator
Информация о настройке системы
Информация о настройке коммутатора
Просмотр статистики
Настройка качества обслуживания
Глоссарий
Информация о взаимодействии параметров устройства

Примечания, предостережения и предупреждения

ПРИМЕЧАНИЕ содержит важную информацию, которая поможет использовать компьютер более эффективно.

ВНИМАНИЕ указывает на потенциально опасные ситуации, связанные с несоблюдением инструкций, которые могут повлечь за собой повреждение аппаратного обеспечения или потерю данных.

ОСТОРОЖНО! Указывает на потенциальную опасность повреждения имущества, получения легких травм или угрозу для жизни.

Ноябрь 2008 Ред. A01

Назад на страницу Содержание

Информация о взаимодействии параметров устройства

Руководство пользователя систем Dell™ PowerConnect™ 35xx

Приведенная ниже таблица содержит информацию о взаимодействиях параметров

Параметр	Примечания по параметру
802.1x неопознанная сеть VLAN	802.1x неопознанные сети VLAN обладают ограниченной функциональностью при работе со следующими элементами: • 802.1X гостевая сеть VLAN • Специальная сеть VLAN
802.1x неопознанный порт VLAN	802.1X неопознанные порты VLAN обладают ограниченной функциональностью при работе со следующими элементами: • Порты VLAN на базе MAC • Фильтрация входа
Список управления доступом ACL	Функции ACL не работают со следующими элементами: • Списки ACL, основанные на IP-адресах • Списки ACL, основанные на MAC-адресах • Специальные сети VLAN
Автоматическое согласование	Нет запретов или ограничений по взаимодействиям параметров.
Поддержка обратного давления	
Фильтрация мостовой многоадресной передачи	Нет запретов или ограничений по взаимодействиям параметров.
Проверка кабелей	Нет запретов или ограничений по взаимодействиям параметров.
Порты сообществ	Порты сообществ имеют ограниченную функциональность при работе с заблокированными портами.
Наблюдение по протоколу DHCP	Нет запретов или ограничений.
Система доменных имен DNS	Нет запретов или ограничений.
Дуплексный режим	
Управление потоком данных	Нет запретов или ограничений по взаимодействиям параметров.
GARP	Нет запретов или ограничений по взаимодействиям параметров.
Гостевые VLAN	Гостевые VLAN не работают со следующими элементами: • VLAN на базе MAC-адресов • Специальные VLAN
GVRP	Нет запретов или ограничений по взаимодействиям параметров.
Наблюдение по протоколу IGMP	Нет запретов или ограничений по взаимодействиям параметров.
Фильтрация входа	Нет запретов или ограничений по взаимодействиям параметров.
статистики группы LAG	Нет запретов или ограничений по взаимодействиям параметров.
Страница Link Aggregation (Объединение каналов)	Нет запретов или ограничений по взаимодействиям параметров. Однако, для этого параметра существует несколько правил для конфигурирования логического канала. Правила для этого параметра приведены в разделе Определение параметров LAG.
LLDP-MED	Нет запретов или ограничений по взаимодействиям параметров.
Заблокированные порты	Работа заблокированных портов запрещена со следующими элементами: • Списки ACL, основанные на MAC-адресах • Фильтрация входа
Вход в систему	Нет запретов или ограничений по взаимодействиям параметров.
Поддержка MAC-адресов	Нет запретов или ограничений по взаимодействиям параметров.
Обнаружение MDI/MDIX	Нет запретов или ограничений по взаимодействиям параметров.
Фильтрация многоадресной передачи	Нет запретов или ограничений по взаимодействиям параметров.
Несколько хостов	802.1X стандартная (для нескольких хостов) не может работать с: • Портом VLAN на базе MAC-адреса
Протокол Multiple Spanning Tree	Протокол Multiple Spanning Tree не может работать с: • Фильтрацией входа

Расширенная проверка подлинности на основе порта	Расширенная проверка подлинности на основе порта имеет ограниченную функциональность или не может работать с: • 802.1 одиночной • Заблокированными портами • Сетями VLAN на базе MAC-адресов • Входными портами
Страница Port Mirroring (Зеркалирование портов)	Нет запретов или ограничений по взаимодействиям параметров. Однако, для этого параметра есть несколько правил для конфигурирования контроля штормов. Правила для этого параметра приведены в разделе Определение сеансов зеркалирования портов.
статистики портов	Нет запретов или ограничений по взаимодействиям параметров
Частные сети VLAN	Частные сети VLAN не могут работать со следующими элементами: • Протокол регистрации GVRP • Наблюдение по протоколу IGMP • Специальная сеть VLAN
Частная сеть VLAN	Частные сети VLAN имеют ограниченную функциональность или не могут работать со следующими элементами: • Протокол GVRP • Наблюдение по протоколу IGMP • Специальные сети VLAN
Качество обслуживания	Нет запретов или ограничений по взаимодействиям параметров.
RMON Statistics (Статистика удаленного мониторинга)	Нет запретов или ограничений по взаимодействиям параметров.
Включение уведомлений о проверке SNMP	Нет запретов или ограничений по взаимодействиям параметров.
Включение уведомлений SNMP	Нет запретов или ограничений по взаимодействиям параметров.
Проверка подлинности SNTP	Нет запретов или ограничений по взаимодействиям параметров.
Протокол Spanning Tree	Нет запретов или ограничений по взаимодействиям параметров.
Специальная сеть VLAN	Нет запретов или ограничений по взаимодействиям параметров
Статические записи MAC	Нет запретов или ограничений по взаимодействиям параметров
контроля «лавины«	Нет запретов или ограничений по взаимодействиям параметров
Системные журналы	Нет запретов или ограничений по взаимодействиям параметров
Синхронизация системного времени	Нет запретов или ограничений по взаимодействиям параметров.
Голосовая сеть VLAN	Голосовая сеть VLAN имеет ограничения при работе с: • Протоколом GVRP

Назад на страницу "Содержание"

Назад на страницу Содержание

Руководство пользователя систем Dell™ PowerConnect™ 35xx

ПРИМЕЧАНИЕ содержит важную информацию, которая поможет использовать компьютер более эффективно.

ВНИМАНИЕ указывает на потенциально опасные ситуации, связанные с несоблюдением инструкций, могущие повлечь за собой повреждение аппаратного обеспечения или потерю данных.

ОСТОРОЖНО! указывает на потенциальную опасность повреждения имущества, получения телесных повреждений или летального исхода.

Товарные знаки, использованные в этом документе: *Dell*, логотип *DELL* , *Dell OpenManage*, и *PowerConnect* являются торговыми марками компании Dell Inc. *Microsoft* и *Windows* являются торговыми марками или зарегистрированными торговыми знаками компании Microsoft Corporation в США и/или других странах.

Прочие товарные знаки и названия продуктов могут использоваться в этом руководстве для обозначения фирм, заявляющих права на товарные знаки и названия, или продуктов этих фирм. Dell Inc. заявляет об отказе от всех прав собственности на какие-либо товарные знаки и названия, кроме своих собственных.

Ноябрь 2008 Ред. A01

Назад на страницу "Содержание"

Назад на страницу "Содержание"

Введение

Руководство пользователя систем Dell™ PowerConnect™ 35xx

- Описание системы
- Общее описание стекирования
- Обзор функций
- Дополнительная документация по режиму консоли

Системы PowerConnect 3524/3548 и PowerConnect 3524P/3548P представляют собой усовершенствованные стекирующие многоуровневые устройства. Блоки PowerConnect могут работать как одиночные многоуровневые коммутаторы, так и как коммутаторы или коммутирующие устройства с числом стекирующих элементов не более восьми.

Настоящее *Руководство пользователя* содержит информацию, необходимую для установки, настройки и технического обслуживания устройства.

Описание системы

Системы PowerConnect 3524/3548 и PowerConnect 3524P/3548P сочетают в себе универсальность и минимальные требования по обслуживанию. Системы серии PowerConnect 3524 и 3548 включают в себя следующие типы устройств:

- PowerConnect 3524
- PowerConnect 3524P
- PowerConnect 3548
- PowerConnect 3548P

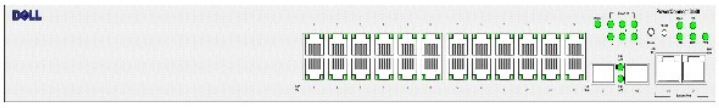
Коммутатор PowerConnect 3524

Коммутатор PowerConnect 3524 предоставляет 24 порта на 10/100 Мбит/с + два порта SFP и два медных порта, которые могут использоваться для переадресации трафика в автономном режиме или в качестве стековых портов в стековом режиме. Это устройство также имеет один порт RS-232 для подключения консоли. Коммутатор PowerConnect 3524 является стековым устройством, но может также работать и в качестве автономного устройства.

Коммутатор PowerConnect 3524P

Коммутатор The PowerConnect 3524P предоставляет 24 порта на 10/100 Мбит/с + два порта SFP и два медных порта, которые могут использоваться для переадресации трафика в автономном режиме или в качестве стековых портов в стековом режиме. Это устройство также имеет один порт RS-232 для подключения консоли. Коммутатор PowerConnect 3524P является стековым устройством, но может также работать и в качестве автономного устройства. PowerConnect 3524P также поддерживает систему питания Power over Ethernet (Питание через Ethernet, PoE).

Рис. 1-1. Коммутаторы PowerConnect 3524 и PowerConnect 3524P



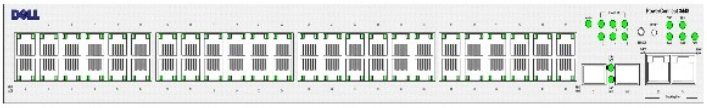
Коммутатор PowerConnect 3548

Коммутатор PowerConnect 3548 предоставляет 48 портов на 10/100 Мбит/с + два порта SFP и два медных порта, которые могут использоваться для переадресации трафика в автономном режиме или в качестве стековых портов в стековом режиме. Это устройство также имеет один порт RS-232 для подключения консоли. Коммутатор PowerConnect 3548 является стековым устройством, но может также работать и в качестве автономного устройства.

Коммутатор PowerConnect 3548P

Коммутатор PowerConnect 3548P предоставляет 48 портов на 10/100 Мбит/с + два порта SFP и два медных порта, которые могут использоваться для переадресации трафика в автономном режиме или в качестве стековых портов, если устройство является частью стека. Это устройство также имеет один порт RS-232 для подключения консоли. Помимо этого, коммутатор PowerConnect 3548P также поддерживает систему питания PoE.

Рис. 1-2. Коммутаторы PowerConnect 3548 и PowerConnect 3548P



Общее описание стекирования

Коммутаторы PowerConnect 3524/P и PowerConnect 3548/P обеспечивают стекирование и управление несколькими коммутаторами из одной точки, как если бы все компоненты стека были единым устройством. Доступ ко всем компонентам стека может осуществляться через один IP-адрес, через который и происходит управление стеком. Управление стеком осуществляется через:

- веб-интерфейс (сетевой интерфейс)
- станцию управления SNMP
- интерфейс командной строки (CLI)

Коммутаторы PowerConnect 3524/P и PowerConnect 3548/P поддерживают стекирование до восьми устройств в стеке, или могут работать как автономные устройства.

При настройке стекирования один коммутатор выбирается в качестве главного устройства (Stack Master) а другой компонент стека выбирается в качестве резервного устройства (Backup Master). Все остальные устройства выбираются в качестве компонентов стека, и им присваиваются уникальные идентификационные номера.

Программное обеспечение коммутатора загружается на каждый из компонентов стека отдельно. Однако, все блоки стека должны работать с одной и той же версией ПО.

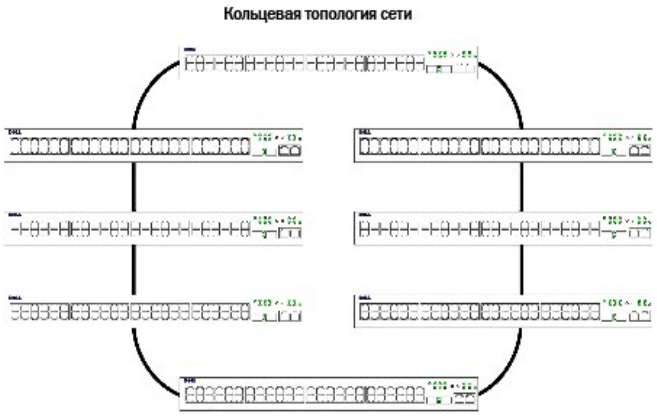
Стекирование и настройка коммутаторов осуществляется через главное устройство. Главное устройство стека определяет и переконфигурирует порты с минимальным вмешательством в систему в следующих случаях::

- При возникновении неполадки устройства
- При возникновении неполадки стековой связи между блоками одного стека
- При установке блока в стек
- При удалении блока из стека

Описание технологии стекирования

Системы серии PowerConnect 35xx работают по кольцевой топологии сети. Кольцевая топология предусматривает подключение всех устройств стека таким образом, что они образуют замкнутое кольцо. Каждое устройство стека осуществляет получение и пересылку данных только от тех или к тем устройствам, к которым оно подключено. Пакет данных перемещается по стеку до тех пор, пока не достигнет места назначения. Такая система определяет оптимальный путь пересылки трафика.

Рис.1-3. Кольцевая схема стека



Основные неполадки в кольцевой схеме происходят тогда, когда одно из устройств кольца перестает работать или связь между устройствами прерывается. В стеке коммутаторов PowerConnect 3524/P и PowerConnect 3548/P система автоматически переключает работу в режим восстановления после отказа (Stacking Failover) без перехода в нерабочий режим. Автоматически генерируется сообщение SNMP, но предпринимать какие-либо действия по управлению стеком не нужно. Однако, для обеспечения целостности стека, необходимо произвести ремонт стекового устройства или стековой связи.

После разрешения проблем устройство может быть подключено в стек снова, без прерывания работы, и кольцевая топология стека будет восстановлена.

Топология восстановления стека после отказа

Если при работе стека возникла неполадка, стек переходит в режим восстановления после отказа. В этом режиме устройства будут работать по схеме последовательного подключения. Главное устройство стека определяет направление пересылки пакетов данных. Каждый из блоков подключен к двум соседним устройствам, за исключением крайних устройств.

Устройства стека и идентификаторы блоков

Для настройки системы стека необходимы уникальные номера устройств, входящих в стек. Определение работы стека происходит в процессе загрузки. Рабочий режим определяется идентификатором устройства, выбранным в процессе инициализации. Например, если пользователь установил автономный режим, устройство загружается как автономное устройство.

Все блоки устройства поставляются с предустановленными заводскими идентификаторами автономных устройств. Если устройство работает автономно, все стековые индикаторы будут отключены.

Если пользователь выберет другой идентификатор, то предустановленный идентификатор не будет удаляться из памяти, а сохраняется там даже в случае перезагрузки.

Идентификаторы 1 и 2 зарезервированы под главные устройства стека. Идентификаторы 3 - 8 могут быть запрограммированы под устройства стека.

При загрузке главного устройства стека или при удалении одного из устройств стека, главное устройство запускает процесс организации стека.

ПРИМЕЧАНИЕ. Если обнаруживается два одинаковых идентификатора двух различных устройств стека, стек продолжает работу, но в стеке остается только то устройство, которое было подключено к нему позднее. В таком случае пользователю будет отправлено сообщение с указанием того, что одно из устройств не было включено в стек.

Удаление и замена устройств стека

Блоки 1 и 2 являются основными устройствами. Блоки 1 и 2 назначаются соответственно главным устройством и резервным устройством. Назначение главного устройства стека происходит в процессе конфигурации. В соответствии с описанным ниже алгоритмом, одно из устройств, которое может быть назначено в качестве главного, назначается в качестве главного устройства стека, а второе - в качестве резервного устройства:

- Если имеется только одно устройство с функциями главного, то ему присваиваются полномочия главного устройства.
- Если имеется два таких устройства, и одно из них вручную сконфигурировано в качестве главного, то оно будет назначено в качестве главного устройства.
- Если имеется два устройства с функциями главного, и ни одно из них не было вручную сконфигурировано в качестве главного, то в качестве главного устройства будет выбрано то, у которого длительность подключения к стеку больше.
- Если имеется два устройства с функциями главного, и оба они были вручную сконфигурированы в качестве главного, то в качестве главного устройства также будет выбрано то, у которого длительность подключения к стеку больше.
- Если у обоих устройств с функциями главного длительность пребывания в стеке одинаковая, то в качестве главного устройства выбирается устройство с идентификатором 1.

ПРИМЕЧАНИЕ. Два устройства одного стека воспринимаются в качестве устройств с одинаковым временем пребывания в стеке, если они установлены в течение одного десятиминутного интервала.

Так, например, если блок 2 подключен на первой минуте 10-минутного цикла, а блок 1 установлен на 5-й минуте того же цикла, то этим устройствам приписывается одинаковая длительность пребывания в стеке. Если имеется два устройства с функциями главного с одинаковым временем пребывания в стеке, то в качестве главного устройства выбирается устройство с идентификатором 1.

Главное устройство и резервное устройство поддерживают в режим «горячего резервирования». Режим «горячего резервирования» обеспечивает переход управляющих функций от главного устройства к резервному в случае его отказа. Это гарантирует непрерывность работы стека.

В режиме «горячего резервирования» главное и резервное устройство будут синхронизированы только статической синхронизацией. После того, как произошла настройка главного устройства стека, его необходимо синхронизировать с резервным устройством. Динамическая синхронизация не сохраняется, например, динамически определенный MAC-адрес сохранен не будет.

Каждый порт стека имеет специальный идентификатор блока, тип порта и номер порта, которые являются частью конфигурационных команд и конфигурационных файлов. Конфигурационными файлами можно управлять только с главного устройства стека, которое позволяет выполнять следующие функции:

- Сохранение во флэш-памяти
- Выгрузка конфигурационных файлов на внешний TFTP сервер / HTTP клиент
- Загрузка конфигурационных файлов с внешнего TFTP сервера / HTTP клиента

ПРИМЕЧАНИЕ. Конфигурационные настройки всех портов сохраняются даже после перезагрузки стека и/или после отключения этих портов.

При каждой перезагрузке начинается операция определения топологии стека, и главное устройство определяет элементы стека. Идентификаторы блоков хранятся в памяти блоков и определяются при определении топологии стека. Если блок пытается произвести загрузку без выбранного главного устройства, и этот блок не работает в автономном режиме, то его загрузка не произойдет.

Конфигурационные файлы изменяются только в случае, если переконфигурацию производит пользователь. Конфигурационные файлы будут изменены автоматически в следующих случаях:

- При добавлении устройств
- При удалении устройств

- При перераспределении идентификаторов устройств
- При переходе из стекового режима в автономный и наоборот

При каждой перезагрузке системы, для конфигурирования стека используется конфигурационный файл запуска главного устройства стека.

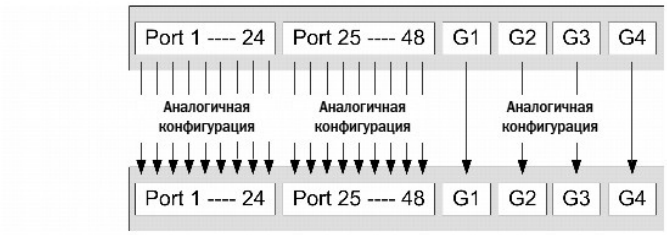
Если удалить устройство стека из стека. а затем заменить его на другое устройство с таким же идентификационным номером, это устройство будет сконфигурировано в соответствии с конфигурацией оригинального устройства. На домашней странице приложения PowerConnect OpenManage Switch Administrator будут отображаться только физически присутствующие порты, и только их можно будет сконфигурировать с помощью сетевой системы управления. Отсутствующие порты конфигурируются через интерфейсы CLI или SNMP.

Перестановка устройств стека

Если устройство стека с неким номером идентификатора заменяет существующее устройство с таким же номером, то конфигурация, установленная для первого блока, будет применена к новому. Если новое устройство имеет большее или меньшее число портов, чем предыдущее устройство, то к новому устройству будет применена конфигурация, соответствующая числу портов. Например,

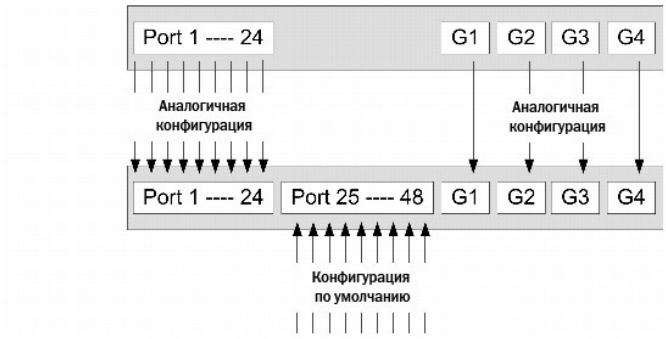
- Если коммутатор PowerConnect 3524/P устанавливается вместо PowerConnect 3524/P, все конфигурации портов остаются прежними.
- Если коммутатор PowerConnect 3548/P устанавливается вместо PowerConnect 3548/P, все конфигурации портов также остаются прежними.

Рис. 1-4. Установка коммутатора PowerConnect 3548/P вместо PowerConnect 3548/P.



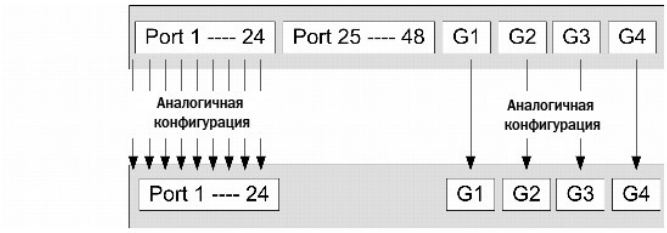
- Если коммутатор PowerConnect 3548/P устанавливается вместо PowerConnect 3524/P, то первые 24 порта FE блока 3548/P получают конфигурацию, аналогичную первым 24 портам FE блока 3524/P. Конфигурации портов GE остаются неизменными. Остальные порты получают конфигурацию по умолчанию.

Рис.1-5. Замещение порта коммутатора PowerConect 3548/P портом коммутатора PowerConnect 3524/P



- Если коммутатор PowerConnect 3524/P устанавливается вместо PowerConnect 3548/P, то 24 порта FE коммутатора PowerConnect 3524/P получают настройки первых 24 портов FE коммутатора PowerConnect 3548/P. Конфигурации портов GE остаются неизменными.

Рис. 1-6. Порт коммутатора PowerConnect 3548/P замещает собой порт коммутатора PowerConect 3524/P



Переключение с главного устройства стека на резервное

Резервное устройство стека замещает собой главное устройство стека в одном из следующих случаев:

- Главное устройство вышло из строя или удалено из стека.
- Связь между главным устройством стека и остальными устройствами прервана.
- Произведено «мягкое» переключение по команде от веб-интерфейса или интерфейса командной строки.

Переключение с главного устройства на приводит к незначительной потере производительности системы. При возникновении неполадки происходит повторный запрос динамических таблиц. Происходит синхронизация действующего конфигурационного файла между главным устройством и резервным устройством, и этот файл продолжает работать на резервном устройстве.

Обзор функций

В данном разделе описываются функции устройства. Полный список всех обновленных функций системы приведен в **сопроводительной записке** к последней версии ПО.

Поддержка IP версии 6 (IPv6)

Устройство работает в качестве IPv6-совместимого хоста, и одновременно IPv4-совместимого хоста (режим, известный как режим обработки двойного стека). Это позволяет устройству работать в полноценной сети IPv6 и в комбинированной сети IPv4/IPv6.

Питание через Ethernet

Функция питания через сеть Ethernet (PoE) обеспечивает питание устройств по существующим кабелям локальной сети, без изменения или внесения дополнений в инфраструктуру сети. Функция PoE устраняет необходимость установки сетевых устройств в зоне досягаемости блоков питания. Система питания PoE может использоваться в следующих случаях:

- IP-телефония
- Беспроводные точки доступа
- Шлюзы IP
- PDA
- Удаленный мониторинг звука и изображения

Для получения более подробной информации по системе питания через сеть Ethernet, см. раздел Управление питанием по сети Ethernet.

Защита от блокировки очереди

Защита от блокировки очереди (HOL) приводит к задержке трафика и потере пакетов в том случае, когда трафик направляется на одни и те же наборы выходных портов. Для предотвращения блокировки пакетов очередей данных на алгоритмическом уровне пакеты, находящиеся в голове очереди, переадресовываются перед пакетами, находящимися в ее хвосте.

Поддержка управления потоком (IEEE 802.3X)

Управление потоком позволяет низкоскоростным устройствам осуществлять связь с высокоскоростными устройствами. При этом высокоскоростные устройства делают паузы между отправкой пакетов. Передача будет временно приостанавливаться для предотвращения переполнения буфера.

Для получения более подробной информации по конфигурированию потока данных портов или LAG, см. разделы Определение конфигурации портов или Определение параметров LAG.

Поддержка обратного давления

При дуплексном соединении принимающий порт предотвращает переполнение буфера путем захвата канала связи, делая его недоступным для дополнительного трафика.

Для получения более подробной информации по конфигурированию потока данных портов или LAG, см. разделы Определение конфигурации портов или Определение параметров LAG.

Виртуальное тестирование кабеля (VCT)

VCT определяет и выдает отчет о критических состояниях кабелей, таких как разрыв или короткое замыкание. Для получения более подробной информации по тестированию кабелей, см. раздел Запуск диагностики кабеля.

Поддержка MDI/MDIX

При запуске автоматического согласования устройство определяет, имеется ли кроссировка или проходной соединитель на кабеле, подключенном к разъему порта RJ-45.

Стандарт кабелей для конечных станций - **MDI** (MDIMedia-Dependent Interface), а стандарт кабелей для концентраторов и коммутаторов называется **MDIX** (MDIXMedia-Dependent Interface with Crossover).

Для получения более подробной информации по конфигурированию MDI/MDIX для или LAG, обратитесь к разделу Определение конфигурации портов или Определение параметров LAG.

Автоматическое согласование

Автоматическое согласование позволяет устройству сообщать о режимах работы. Функция автоматического согласования обеспечивает возможность обмена информацией между двумя устройствами, которые используют общий двухточечный сегмент линии связи; она также применяется для автоматической настройки обоих устройств, что позволяет максимально эффективно использовать их возможности передачи данных.

Система серии PowerConnect 35xx обеспечивает автоматическое согласование путем выдачи отчета о проверке состояния портов. Проверка состояния портов позволяет системному администратору настроить скорость передачи данных по портам.

Для получения более подробной информации по автоматическому согласованию, см. раздел Определение конфигурации портов или Определение параметров LAG.

Голосовая сеть VLAN

Голосовая VLAN позволяет сетевым администраторам совершенствовать службу VoIP путем настройки портов на передачу голосового трафика IP с IP-телефонов на определенную сеть VLAN. Трафик VoIP имеет предварительно настроенный префикс OUI в исходном MAC-адресе. Сетевые администраторы могут выполнить настройку сетей VLAN, с которых пересылается голосовой IP-трафик. Трафик, не являющийся трафиком VoIP, выпадает из голосовой VLAN в автоматическом режиме безопасности голосовой VLAN. Голосовая VLAN также обеспечивает функционирование службы QoS (Качество обслуживания) для VoIP, благодаря чему качество голоса не ухудшается, если IP-трафик принимается неравномерно.

Для получения более подробной информации, см. раздел Конфигурирование голосовой сети VLAN.

Гостевая сеть VLAN

Гостевая сеть VLAN предоставляет ограниченный доступ к сети для неавторизованных портов. Если для порта запрещается доступ к сети через авторизацию на основе порта, а гостевая сеть VLAN включена, порт получает ограниченный доступ к сети.

Функции, поддерживающие MAC-адреса

Поддержка возможности MAC-адресов

Устройство поддерживает до 8 тыс. адресов MAC. Устройство резервирует определенные MAC-адреса для использования системой.

Статические записи MAC

Вместо распознавания адресов из входящих кадров можно вручную вводить в таблицу связей записи MAC. Эти определяемые пользователем записи не устаревают и сохраняются после сброса и перезагрузки системы.

Для получения более подробной информации, см. раздел Определение статических адресов.

Самораспознаваемые MAC-адреса

Устройство обеспечивает автоматическое запоминание MAC-адресов, поступающих во входящих пакетах. MAC-адреса сохраняются в таблице связей.

Автоматическое время хранения MAC-адресов

MAC-адреса, по которым не был получен трафик в течение определенного периода, признаются устаревшими. Это позволяет предотвратить переполнение таблицы связей.

Для получения более подробной информации по конфигурированию времени устаревания MAC-адресов, см. раздел Просмотр динамических адресов.

Коммутация, основанная на MAC-адресах, с поддержкой VLAN.

Устройство всегда выполняет коммутацию с поддержкой VLAN. Классический способ установки связи (IEEE802.1D), в котором кадры пересылаются только на основании MAC-адреса назначения, не используется. Однако, аналогичные функции могут конфигурироваться и для нетегированых кадров. Кадры, адресованные на MAC-адрес приемника, который не связан ни с каким портом, рассылаются «лавиной» на все порты соответствующей VLAN.

Поддержка передачи на несколько MAC-адресов

Служба многоадресной передачи представляет собой службу широковещательной передачи, которая позволяет устанавливать соединения «один ко многим» и «многие ко многим». В многоадресных службах Layer 2 принимается один кадр, адресованный указанному адресу многоадресной передачи, и создаются копии кадра, которые передаются на каждый соответствующий порт. Если включены статические группы многоадресной передачи, вы можете установить порт назначения зарегистрированных групп и определить поведение многоадресных кадров.

Для получения более подробной информации, см. раздел Назначение параметров переадресации многоадресной передачи.

Функции Layer 2

Наблюдение по протоколу IGMP

Наблюдение на базе протокола IGMP (Internet Group Membership Protocol) проверяет содержимое кадров IGMP, когда они пересылаются устройством от станций на многоадресные маршрутизаторы. Кадр позволяет устройству определить рабочие станции, настроенные для многоадресных сеансов, а также то, какие маршрутизаторы посылают многоадресные кадры. Опрашивающее устройство IGMP Querier моделирует поведение маршрутизатора многоадресной передачи, что позволяет отслеживать домен второго уровня даже в том случае, если многоадресный маршрутизатор отсутствует.

Дополнительную информацию см. в разделе Наблюдение по протоколу IGMP.

Страница Port Mirroring (Зеркалирование портов)

Зеркалирование портов контролирует и дублирует сетевой трафик путем пересылки копий входящих и исходящих пакетов с контролируемого порта на контролирующий порт. Пользователи определяют, какие целевые порты должны получать копии всего трафика, проходящего через указанный исходный порт.

Дополнительную информацию см. в разделе Определение сеансов с зеркалированием портов.

Защита от «лавины» широковещательной передачи

Защита от «лавины» ограничивает число многоадресных и широковещательных кадров, принятых и переданных коммутатором.

Когда передаются кадры Layer 2, широковещательные и многоадресные кадры рассылаются «лавиной» на все порты соответствующей VLAN. «Лавина» занимает всю полосу пропускания и загружает все узлы, подключенные ко всем портам.

Дополнительную информацию см. в разделе Включение контроля лавины.

Поддержка функций VLAN

Поддержка VLAN

VLAN представляют собой совокупности коммутируемых портов, входящих в состав одного домена широковещательной передачи. Принадлежность пакетов VLAN определяется либо на основе метки VLAN, либо на основе комбинации входящего порта и содержимого пакета. Пакеты с общими атрибутами могут быть сгруппированы в одну и ту же сеть VLAN.

Дополнительную информацию см. в разделе Настройка сетей VLAN.

VLAN, основанные на портах

В случае групп VLAN, основанных на портах, распределение по группам VLAN выполняется по входящим портам.

Дополнительную информацию см. в разделе Определение параметров портов VLAN.

Полное соответствие маркировке VLAN 802.1Q

IEEE 802.1Q определяет архитектуру для сетей с виртуальными мостами, службы, предоставляемые в группах VLAN, а также протоколы и алгоритмы, используемые для этих служб.

Поддержка GVRP

Протокол регистрации GARP VLAN (GVRP) обеспечивает отсечение групп VLAN, IEEE 802.1Q- в соответствии со стандартом IEEE 802.1Q, а также динамическое создание групп VLAN на портах транков 802.1Q. Когда включен протокол GVRP, коммутатор регистрирует, а затем распространяет данные о принадлежности VLAN на все порты, являющиеся частью активной топологии Функции протокола Spanning Tree.

Для получения дополнительной информации см. раздел Настройка параметров GVRP.

Private VLAN Edge

Портам могут назначаться группы Private VLAN Edge (PVE). Порт, назначенный как PVE, защищается линией связи с центральным узлом и, таким образом, изолируется от других портов той же сети VLAN. Такой линией связи должен быть порт GE.

Для получения более подробной информации по частным сетям VLAN, см. раздел Настройка портов.

Функции протокола Spanning Tree

Протокол STP (Spanning Tree Protocol)

802.1d STP - это стандартное требование коммутаторов Layer 2, которое позволяет мостам автоматически предотвращать и разрешать циклы пересылки L2. Коммутаторы обмениваются конфигурационными сообщениями, используя кадры специального формата, и выборочно включают и отключают передачу на порты.

Дополнительную информацию см. в разделе Настройка протокола STP.

Быстрая связь

Время реакции протокола STP может достигать 30-60 секунд. В это время протокол STP определяет возможные циклы. Кроме того, выделяется необходимое время для распространения данных об изменениях состояния, а также время на ответ соответствующих устройств. 30-60 секунд для многих приложений считается слишком большим временем ответа. Параметр Fast Link позволяет избежать этой задержки. Его можно использовать в сетевых топологиях, в которых отсутствуют циклы пересылки.

Дополнительную информацию по параметру Fast Link для портов и LAG см. в разделе Определение установок порта STP или Определение статических адресов.

Поддержка протокола IEEE 802.1w Rapid Spanning Tree

При использовании протокола Spanning Tree может потребоваться 30-60 секунд, пока каждый хост определит, выполняется ли на его портах активная пересылка трафика. Протокол Rapid Spanning Tree (RSTP) выявляет и использует топологию сети, обеспечивая лучшую сходимость для протокола STP без образования циклов пересылки.

Дополнительную информацию см. в разделе Определение протокола Rapid Spanning Tree.

Multiple Spanning Tree (IEEE 802.1)

Работа протокола Multiple Spanning Tree (MSTP) назначает сети VLAN различным копиям протокола STP. MSTP обеспечивает различные сценарии выравнивания нагрузки. Пакеты, назначенные разным сетям VLAN, передаются через разные пути в областях MSTP (области MST). Эти области представляют собой один или несколько мостов MSTP, по которым могут передаваться кадры. Этот стандарт позволяет сетевому администратору назначать трафик сети VLAN различным путям.

Дополнительную информацию см. в разделе Настройка протокола STP.

Страница Link Aggregation (Объединение каналов)

Страница Link Aggregation (Объединение каналов)

Можно определить до восьми объединенных каналов, каждый из которых будет содержать до восьми портов компонентов, формируя одну объединенную группу каналов LAG (Link Aggregated Group). Это обеспечивает:

- защиту от сбоев вследствие физического разрыва соединения
- соединение с большей полосой пропускания
- улучшенные возможности разбивки полосы пропускания
- соединения сервера с широкой полосой пропускания

Группа LAG состоит из портов с одинаковой скоростью, работающих в дуплексном режиме.

Дополнительную информацию см. в разделе Определение параметров LAG.

Объединение каналов и протокол LACP

Протокол LACP использует замену узлов в связях для определения, на постоянной основе, концентрационных способностей различных связей, и непрерывно обеспечивает максимальный уровень концентрационной способности, который можно установить между данной парой устройств. Протокол LACP автоматически определяет, конфигурирует, связывает и отслеживает связки портов внутри системы.

Дополнительную информацию см. в разделе Объединение каналов.

Клиенты BootP и DHCP

Протокол DHCP позволяет получать дополнительные параметры настройки от сетевого сервера во время запуска системы. Служба DHCP представляет собой непрерывный процесс. DHCP является расширением BootP.

Дополнительную информацию о протоколе DHCP см. в разделе Определение параметров интерфейса DHCP IPv4.

Функции качества обслуживания (Quality of Service)

Поддержка класса обслуживания 802.1p

Сигналы стандарта IEEE 802.1p - это стандарт OSI Layer 2 для пометки и определения приоритетов сетевого трафика на уровне канала передачи данных или подуровня MAC. Трафик 802.1p классифицируется и отправляется в место назначения. При этом не резервируется полоса пропускания и не устанавливаются ограничения. 802.1p - это производный стандарт от стандарта 802.1Q (VLAN). Стандарт 802.1p определяет восемь уровней приоритетов, аналогично битовому полю заголовка IP с указанием приоритетов IP-пакетов.

Дополнительную информацию см. в разделе Настройка качества обслуживания.

Функции управления устройствами

Сигналы и журналы прерываний SNMP

События журнала системы с кодами серьезности и отметками времени. События передаются как прерывания SNMP списку получателей прерываний.

Дополнительную информацию о сигналах и прерываниях SNMP см. в разделе Определение параметров SNMP.

SNMP версий 1, 2 и 3

По протоколу SNMP (Simple Network Management Protocol) на основе протокола UDP/IP осуществляется управление доступом к системе, определяется список записей сообщества, каждая из которых содержит строку сообщества и привилегии доступа. Существует 3 уровня привилегий пользователя SNMP: только чтение, чтение и запись, и максимальный (суперпользователь). К таблице сообщества имеет доступ только суперпользователь.

Дополнительную информацию см. в разделе Определение параметров SNMP.

Управление через веб-интерфейс

Управление через веб-интерфейс позволяет выполнять управление системой с любого браузера. Система содержит встроенный веб-сервер (EWS), обслуживающий HTML-страницы, с помощью которого можно контролировать и настраивать систему. Система выполняет внутреннее преобразование вводимых из веб-интерфейса данных в команды настройки, параметры переменной MIB и другие параметры, относящиеся к управлению.

Загрузка и выгрузка файла настройки

Настройки устройства сохраняются в конфигурационном файле. Файл настройки содержит данные настройки как всей системы, так и настройку определенного порта устройства. Система может отображать файлы настройки в форме набора команд интерфейса командной строки, которые хранятся и обрабатываются как текстовые файлы.

Дополнительную информацию см. в разделе Управление файлами.

Протокол TFTP (Trivial File Transfer Protocol)

Устройство поддерживает загрузку/выгрузку изображений, программного обеспечения и конфигураций через TFTP.

Удаленный мониторинг

Удаленный мониторинг (RMON) - это расширение протокола SNMP, предоставляющее широкие возможности контроля сетевого трафика (в отличие от протокола SNMP, в котором возможен контроль и управление сетевым устройством). RMON - это стандартная база MIB, в которой определены текущая и предыдущая статистика уровня MAC и объекты управления, предоставляющая данные в реальном времени для захвата по всей сети.

Дополнительную информацию см. в разделе Просмотр статистики.

Интерфейс командной строки

Интерфейс командной строки (CLI) максимально соответствует общим принципам, принятым в отрасли. Консоль состоит из обязательных и необязательных элементов. Интерпретатор CLI предоставляет список команд и ключевых слов для помощи пользователю и сокращению вводимых данных.

Syslog

Syslog - это протокол, который обеспечивает передачу уведомлений об ошибках удаленным серверам, где их можно сохранить, изучить, а также выполнить соответствующие действия. Система отправляет уведомления о значимых событиях в режиме реального времени и сохраняет записи об этих событиях для последующего использования.

Дополнительную информацию о Syslog см. в разделе Управление журналами.

SNTP

Протокол Simple Network Time Protocol (SNTP) обеспечивает синхронизацию встроенного синхрогенератора коммутатора сети Ethernet с точностью до миллисекунды. Синхронизация по времени выполняется сетевым сервером SNTP. Источники времени устанавливаются по уровням. Уровни определяют расстояние от генератора тактовых импульсов. Чем выше уровень (нуль - это самый высокий уровень), тем точнее генератор.

Дополнительную информацию см. в разделе Настройка параметров SNTP.

Система имен доменов

Система имен доменов (DNS) преобразует имена доменов, определенные пользователем, в IP-адреса. Каждый раз при назначении имени домена служба DNS переводит имя в числовой IP-адрес. Например, www.ipexample.com переводится в 192.87.56.2. Серверы DNS ведут базы данных имен доменов и соответствующие им IP-адреса.

Дополнительную информацию см. в разделе Настройка систем доменных имен.

Трассировка

Трассировка определяет маршруты IP, по которым направляются пакеты в процессе переадресации. Программу CLI Traceroute можно запустить в режимах user-exec или Privileged.

802.1ab (LLDP-MED)

Протокол LLDP позволяет сетевым администраторам выполнять поиск и устранение неисправностей и совершенствовать управление сетью путем выявления и сохранения топологии сети в средах, включающих оборудование самых разных поставщиков. С помощью протокола LLDP, используя стандартные методы, можно обнаружить сетевое окружение сетевых устройств, чтобы сообщить о них другим системам и сохранить обнаруженную информацию. Для отправки нескольких наборов сообщений используется поле пакета **Type Length Value** (TLV) (Ввод значения длины). Устройства LLDP должны поддерживать сообщения о корпусе и идентификаторе порта, а также имя системы, идентификатор системы, описание системы и сообщения о возможностях системы.

Протокол LLDP Media Endpoint Discovery (LLDP-MED) повышает гибкость сети, обеспечивая различным системам IP возможность использовать один протокол LLDP. Он предоставляет подробную информацию о топологии сети, о службе экстренных вызовов с использованием информации о расположении IP-телефона, а также информацию о поиске и устранении неисправностей.

Средства защиты

SSL

Протокол SSL (Secure Socket Layer) - это протокол на уровне приложения, который обеспечивает безопасные транзакции данных за счет обеспечения конфиденциальности, проверки подлинности, а также целостности данных. Он основывается на сертификатах, а также открытых и закрытых ключах.

Проверка подлинности на основе порта (802.1x)

Проверка подлинности на основе порта обеспечивает проверку подлинности пользователей системы на основе портов через внешний сервер. Только прошедшие проверку подлинности и одобренные пользователи системы могут передавать и принимать данные. Проверка подлинности портов выполняется с помощью сервера Remote Authentication Dial In User Service (RADIUS), использующего протокол EAP (Extensible Authentication Protocol). Функция динамического распределения VLAN (DVA) позволяет администраторам автоматически распределять пользователей по сетям VLANs при авторизации на сервере RADIUS.

Дополнительную информацию см. в разделе Проверка подлинности на основе порта.

Поддержка заблокированных портов

Заблокированные порты повышают безопасность сети, предоставляя доступ к порту только для пользователей с определенными MAC-адресами. Эти адреса вводятся вручную для порта или определяются. При получении кадра на заблокированном порту, если MAC-адрес источника кадра не связан с эти портом, срабатывает механизм защиты.

Дополнительную информацию см. в разделе Настройка безопасности портов.

Клиент RADIUS

RADIUS - это протокол типа «клиент/сервер». На сервере RADIUS ведется база данных пользователей, содержащая данные проверки подлинности для каждого пользователя, например, имя пользователя, пароль и данные учетной записи.

Дополнительную информацию см. в разделе Настройка параметров сервера RADIUS.

Страница SSH

Secure Shell (SSH) - это протокол, обеспечивающий защиту и удаленное подключение к устройству. В настоящее время поддерживается SSH версии 2. Функция сервера SSH позволяет клиенту SSH установить с устройством безопасное кодируемое соединение. Это соединение предоставляет функциональные возможности, аналогичные входящему соединению telnet. Протокол SSH использует криптографию RSA и DSA для соединений и определения подлинности устройства.

TACACS+

TACACS+ обеспечивает централизованную систему безопасности для проверки пользователей, получающих доступ к устройству. TACACS+ обеспечивает централизованную систему управления при соблюдении совместимости с RADIUS и другими процессами проверки подлинности.

Дополнительную информацию см. в разделе Определение параметров TACACS+.

Управление паролями

Управление паролями повышает безопасность сети и улучшает контроль паролей. Пароли для доступа через SSH, Telnet, HTTP, HTTPS, и SNMP являются назначенными параметрами безопасности. Для получения более подробной информации по управлению паролями, см. раздел Управление паролями.

Списки управления доступом ACL

Списки управления доступом (ACL) позволяют сетевым администраторам определять классификационные действия и правила для определенных входных портов. Пакеты, поступающие на входной порт с активным списком ACL, пропускаются или отбрасываются, а входной порт отключается. Если пакеты отбрасываются, пользователь может отключить порт.

Дополнительную информацию см. в разделе Обзор списка ACL.

Наблюдение по протоколу DHCP

Наблюдение по протоколу DHCP усиливает безопасность сети, обеспечивая с помощью брандмауэра защиту между серверами DHCP и ненадежными интерфейсами. Благодаря использованию наблюдения по протоколу DHCP сетевые администраторы могут различать доверенные интерфейсы, подключенные к компьютерам конечных пользователей или серверам DHCP, и ненадежные интерфейсы, отсутствующие в правилах сетевого брандмауэра.

Дополнительную информацию см. в разделе Настройка наблюдения по протоколу DHCP.

Дополнительная документация по режиму консоли

Справочное руководство по командной строке, которое находится на компакт-диске с документацией, содержит сведения о командах консоли, используемых для конфигурирования коммутаторов. В настоящем документе содержатся описание команд, синтаксические структуры команд, значения параметров по умолчанию, правила и примеры.

Назад на страницу "Содержание"

Назад на страницу Содержание

Описание аппаратного обеспечения

Руководство пользователя систем Dell™ PowerConnect™ 35xx

- Описание портов
- Габаритные размеры
- Описания индикаторов

Описание портов

Описание портов коммутатора PowerConnect 3524

Устройство PowerConnect 3524 оборудовано следующими портами.

- **24 порта Fast Ethernet** — порты RJ-45, назначенные как порты 10/100Base-T
- **2 оптоволоконных порта** — назначены как порты 1000Base-X SFP
- **2 гигабитных порта** — назначены как порты 1000Base-T
- **Порт для подключения консоли** — порт на базе RS-232

На рисунке (см. ниже) изображена передняя панель устройства PowerConnect 3524.

Рис 2-1. Передняя панель устройства PowerConnect 3524

На передней панели находятся 24 порта RJ-45 с номерами 1-24. Верхний ряд портов помечен нечетными номерами (1-23), и нижний - четными (2-24). Кроме этого, на передней панели находятся два оптоволоконных порта G1 - G2 и два порта для медных кабелей G3- G4. Порты G3 - G4 могут использоваться как порты для стекирования или для переадресации сетевого трафика в автономном режиме работы.

На передней панели имеются две кнопки. Кнопка Stack ID (идентификатор стека) используется для выбора номера устройства. Вторая кнопка - кнопка перезагрузки Reset, которая используется для ручной перезагрузки устройства. Кнопка перезагрузки не выходит за габариты плоскости передней панели, поэтому случайное ее нажатие невозможно. На передней панели имеются светодиодные индикаторы всех устройств.

На рисунке (см. ниже) показана задняя панель коммутатора PowerConnect 3524:

Рис. 2-2. Задняя панель коммутатора PowerConnect 3524

На задней панели устройства находятся гнездо RPS, порт для подключения консоли и гнездо для подключения блока питания.

Описание портов коммутатора PowerConnect 3548

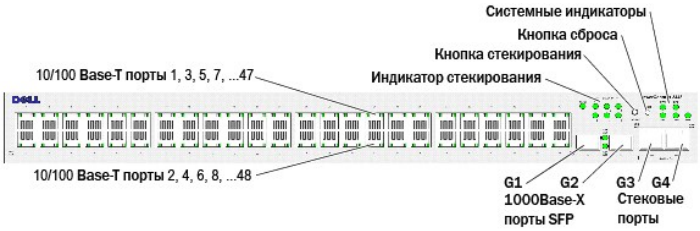
Устройство PowerConnect 3548 оборудовано следующими портами.

- **48 портов FE** — порты RJ-45, назначенные как порты 10/100Base-T
- **2 оптоволоконных порта** — назначены как порты 1000Base-X SFP
- **2 гигабитных порта** — назначены как порты 1000Base-T

- **Порт для консоли** — порт консоли RS-232

На рисунке (см. ниже) изображена передняя панель устройства PowerConnect 3548.

Рис 2-3. Передняя панель устройства PowerConnect 3548

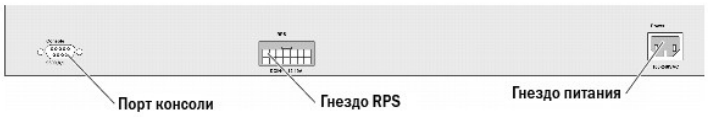


На передней панели находятся 48 портов RJ-45 с номерами 1-48. Верхний ряд портов обозначен нечетными номерами (1-47), а нижний - четными (2-48). Кроме того, на передней панели имеются оптоволоконные порты G1 - G2 и порты G3- G4 для подключения медных кабелей. Порты G3- G4 могут использоваться как для стекирования, так и для переадресации сетевого трафика в автономном режиме работы устройства.

На передней панели имеется две кнопки. Кнопка Stack ID (идентификатор стека) используется для выбора номера устройства. Вторая кнопка - кнопка перезагрузки Reset, которая используется для ручной перезагрузки устройства. Кнопка перезагрузки не выходит за габариты плоскости передней панели, поэтому случайное ее нажатие невозможно. На передней панели имеются светодиодные индикаторы всех устройств.

На рисунке (см. ниже) показана задняя панель коммутатора PowerConnect 3548:

Рис. 2-4. Задняя панель коммутатора PowerConnect 3548



На задней панели находятся гнездо RPS, порт для консоли и гнездо для подключения блока питания.

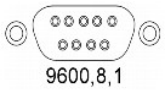
Порты SFP

Порты (SFP) являются волоконными трансиверами, назначенными как 10000 Base-SX или LX. В них имеются двухпроводные последовательные интерфейсы TWSI и внутренние ППЗУ.

Порт консоли RS-232

Одно гнездо DB-9 для подключения терминала используется для наладки, загрузки программного обеспечения и т.п. Скорость передачи по умолчанию для этого порта равна 9600 бит/с. Скорость передачи данных можно настроить в диапазоне от 2400 до 115200 бит/с.

Рис. 2-5. Порт консоли



Габаритные размеры

КоммутаторыPowerConnect 3524/P и PowerConnect 3548/P имеют следующие габаритные размеры:

Модель с питанием через Ethernet (PoE):

- **Ширина —** 440 мм (17,32 дюйма)
- **Длина** — 387 мм (15,236 дюйма)
- **Высота** — 43,2 мм (1,7 дюйма)

Модель без функции PoE:

- **Ширина —** 440 мм (17,32 дюйма)
- **Длина**— 257 мм (10,118 дюймов)
- **Высота** — 43,2 мм (1,7 дюйма)

Описание индикаторов

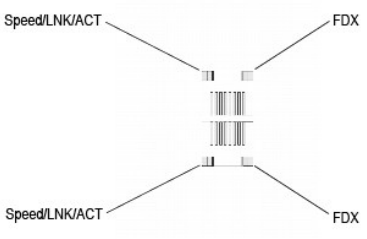
На передней панели находятся светодиодные индикаторы, которые показывают состояние связи, питания, вентиляторов и системы диагностики.

Индикаторы портов

У каждого порта 10/100/1000 Base-T и 10/100 Base-T имеется по два индикатора. Индикатор скорости расположен слева от порта, а индикатор связь/дуплекс/активность расположен с правой стороны.

На рисунке (см. ниже) показаны индикаторы порта 10/100 Base-T коммутаторов PowerConnect 3524 /P и PowerConnect 3548/P:

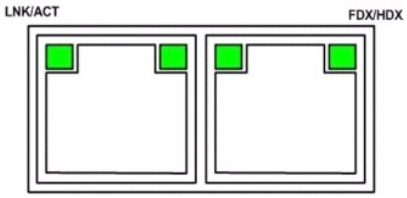
Рис. 2-6. Светодиодные индикаторы портов медных кабелей RJ-45 10/100 BaseT



Порты RJ-45 100 Base-T коммутатора PowerConnect 3524 /P и PowerConnect 3548/P имеют два светодиодных индикатора, обозначенные как LNK/ACT.

На рисунке (см. ниже) показаны индикаторы портов 100 Base-T.

Рис. 2-7. Индикатор порта RJ-45 1000 BaseT



Индикаторы RJ-45 LED коммутатора PowerConnect 3524 и PowerConnect 3548 описаны в следующей таблице:

Таблица 2-1. Режимы работы индикаторов портов RJ-45 100BaseT коммутаторов PowerConnect 3524 и PowerConnect 3548

Индикатор	Цвет	Описание
Link/Activity/Speed	Горит зеленым	Порт работает на скорости 100 Мбит/с.
	Мигает зеленым	Порт получает или передает данные со скоростью 100 Мбит/с.
	Горит желтым	Порт работает на скорости 10 Мбит/с.
	Мигает желтым	Порт получает или передает данные со скоростью 10 Мбит/с.
	Не горит	Порт в данный момент не работает.
FDX	Горит зеленым	Порт работает в режиме полного дуплекса.
	Не горит	Порт работает в полудуплексном режиме

Индикаторы порта RJ-45 коммутаторов PowerConnect 3524P и PowerConnect 3548P описаны в следующей таблице:

Таблица 2-2. Режимы работы индикаторов портов RJ-45 100BaseT для медных кабелей коммутаторов PowerConnect 3524P и PowerConnect 3548P

Индикатор	Цвет	Описание
Speed/Link/Act	Горит зеленым	Порт соединяется на скорости 100 Мбит/с.
	Мигает зеленым	Порт работает на скорости 100 Мбит/с.
	Не горит	Порт в настоящий момент работает на скорости 10 Мбит/с или не соединен.
FDX	Горит зеленым	Обнаружен включенный потребитель (PD), работающий на нормальной нагрузке. Подробную информацию о включенных потребителях (PD), см. в разделе *Управление питанием через Ethernet*.
	Мигает зеленым	Порт работает в неустановившемся режиме. Идет процесс поиска потребителя или потребитель работает с неполадками. Более подробная информация по питанию через Ethernet приведена в разделе *Управление питанием через Ethernet*.
	Горит желтым	Обнаружена перегрузка или короткое замыкание в подключенном потребителе. Более подробная информация по неполадкам в режиме питания по сети Ethernet приведена в разделе *Управление питанием через Ethernet*.
	Мигает желтым	Потребляемая мощность потребителя превышает установленные для него пределы. Более подробная информация по установке пределов потребления мощности приведена в разделе *Управление питанием через Ethernet*.
	Не горит	Потребители не обнаружены.

Индикаторы гигабитных портов

В таблице (см. ниже) показаны индикаторы стековых (гигабитных) портов:

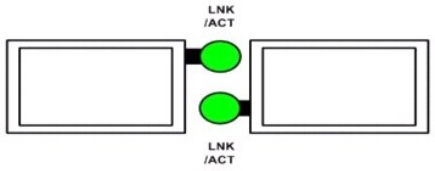
Таблица 2-3. Режимы работы индикаторов портов RJ-45 100BaseT для медных кабелей коммутаторов PowerConnect 3524 и PowerConnect 3548

Индикатор	Цвет	Описание
Link/Activity/Speed	Горит зеленым	Порт работает на скорости 1000 Мбит/с.
	Мигает зеленым	Порт получает или пересылает данные на скорости 1000 Мбит/с.
	Горит желтым	Порт работает на скорости 10 или 100 Мбит/с.
	Мигает желтым	Через порт осуществляется прием или передача данных на скорости 10 или 100 Мбит/с.
	Не горит	В настоящее время порт не работает.
FDX	Горит зеленым	В настоящее время порт работает в режиме полного дуплекса.
	Не горит	В настоящее время порт работает в полудуплексном режиме.

Индикаторы SFP

Каждый и портов SFP снабжен одним индикатором, обозначенным LNK/ACT. У коммутаторов PowerConnect 3524/P и PowerConnect 3548/P индикаторы имеют круглую форму и расположены между портами. На рисунках (см. ниже) показаны индикаторы портов каждого из устройств.

Рис. 2-8. Индикаторы порта SFP



Описание показаний индикаторов порта SFP приведено в следующей таблице.

Табл. 2-4. Показания индикаторов порта SFP

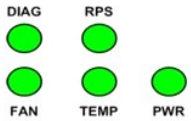
Индикатор	Цвет	Описание
Link/Activity	Горит зеленым	Связь установлена.
	Мигает зеленым	Через порт осуществляется прием или передача данных.

	Не горит	Связь с портом не установлена.

Системные индикаторы

Системные индикаторы устройств PowerConnect 3524 /P и PowerConnect 3548/P выдают информацию об источниках питания, работе вентиляторов, температурных условиях работы и диагностике. На рисунке (см. ниже) показаны системные индикаторы.

Рис. 2-9. Системные индикаторы



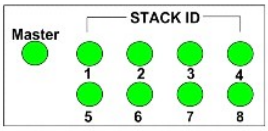
Описание показаний индикаторов приведено в следующей таблице.

Таблица 2-5. Системные светодиодные индикаторы

Индикатор	Цвет	Описание
Питание (PWR)	Горит зеленым	Коммутатор включен.
	Не горит	Коммутатор выключен.
Резервные источники питания (RPS) (модели: 3524 и 3548)	Горит зеленым	RPS работает.
	Горит красным	Неполадка RPS.
	Не горит	Резервный источник питания не подключен.
Резервные источники питания (RPS) (модели: 3524P и 3548P)	Горит зеленым	RPS работает.
	Не горит	Неполадка RPS или он не подключен.
Диагностика (DIAG)	Мигает зеленым	Идет процесс диагностики системы.
	Горит зеленым	Диагностика систему прошла успешно.
	Горит красным	Диагностика завершилась неудовлетворительно.
	Не горит	Система работает нормально.
Температура (TEMP)	Горит красным	Превышен допустимый температурный диапазон.
	Не горит	Устройство работает в допустимом температурном диапазоне.
Вентилятор (FAN)	Горит зеленым	Вентиляторы устройства работают нормально.
	Горит красным	Один или несколько вентиляторов устройства не работают.

Индикация стековых индикаторов показывает место устройства в стеке. На рисунке (см. ниже) показаны индикатора на передней панели устройства.

Рис. 2-10. Стековые индикаторы



Стековые индикаторы имеют номера 1- 8. Каждый из элементов стека включает один из индикаторов, и номер индикатора соответствует идентификационному номеру элемента в стеке. Если горит стековый индикатор й или 2, то устройство является главным устройством стека или резервным устройством стека.

Таблица 2-6. Режим работы стековых индикаторов

Индикатор	Цвет	Описание
Все стековые индикаторы	Не горит	Коммутатор находится в автономном режиме.
Стековые индикаторы 1-8 (S1-S8)	Горит зеленым	Устройство включено в стек под номером N.
	Не горит	Устройство не включено в стек.
Индикатор главного устройства стека	Горит зеленым	Устройство является главным устройством стека.

	Не горит	Устройство не является главным устройством стека.

Источники питания

Устройство снабжено встроенным блоком питания (переменного тока) и штекером для подключения коммутаторов PowerConnect 3524/P и PowerConnect 3548/P к блоку питания PowerConnect EPS-470, или для подключения коммутаторов PowerConnect 3524 и PowerConnect 3548 к блоку питания PowerConnect RPS-600. Коммутаторы PowerConnect 3524/P и PowerConnect 3548/P имеют встроенный источник питания (12 В).

Работа с двумя источниками питания регулируется с помощью распределения нагрузки. Индикаторы питания отображают состояние источника питания.

Коммутаторы PowerConnect 3524/P и PowerConnect 3548/P имеют встроенные источники питания мощностью 470 Вт (12В/-48В), с общей мощностью 370 Вт (для всех 24 портов устройства PoE).

Источник питания переменного тока

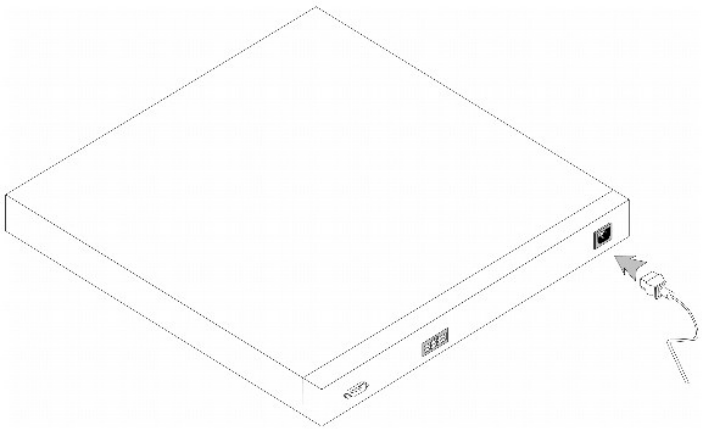
Источник питания переменного тока работает от сети с напряжением 90 - 264 В и частотой 47 - 63 Гц. Блок питания переменного тока снабжен стандартной сетевой вилкой. Индикатор на передней панели показывает, подключен ли источник питания.

Источник питания постоянного тока

Для обеспечения резервного питания, коммутаторы PowerConnect 3524 и PowerConnect 3548 подключаются к внешнему блоку питания RPS-600. Производить настройку не требуется. Индикатор «RPS» на передней панели показывает, подключен ли внешний блок питания RPS-600. Описание индикатора RPS дано в таблице 2-5.

Для обеспечения резервного питания, коммутаторы PowerConnect 3524/P и PowerConnect 3548/P подключаются к внешнему блоку питания EPS-470. Производить настройку не требуется. Индикатор «RPS» на передней панели показывает, подключен ли внешний источник питания EPS-470. Описание индикатора RPS дано в таблице 2-5.

Рис. 2-11. Подключение к источнику питания



При подключении устройства к различным источникам питания уменьшается вероятность сбоя из-за перебоев в электропитании.

Кнопка Stack ID

На передней панели устройства имеется кнопка Stack ID, предназначенная для выбора идентификатора устройства стека и главного устройства вручную.

Главное устройство стека и прочие устройства стека должны быть выбраны в течение 15 секунд при загрузке устройства. Если главное устройство стека не выбрано в течение 15 секунд, устройство будет загружено в автономном режиме. Для выбора идентификатора устройства, перегрузите устройство.

Главное устройство стека принимает номер 1 или 2. Если присутствуют оба устройства 1 и 2, не выбранное устройство будет работать в качестве резервного устройства стека. Устройства стека принимают отдельные идентификационные номера (3-8). Пример: если в стеке имеется 4 устройства и главное устройство имеет номер 1 или 2, то резервное устройство принимает номер 1 или 2 в зависимости от идентификатора главного устройства стека, третье устройство получает номер 3, а четвертое - 4.

ПРИМЕЧАНИЕ. Устройство не определяет автономное устройство автоматически. Если устройство уже было выбрано, нажимайте кнопку Stack ID до тех пор, пока все стековые индикаторы не погаснут.

Кнопка Reset (Сброс)

Коммутаторы PowerConnect 3524/P и PowerConnect 3548/P снабжены кнопкой перезагрузки, расположенной на передней панели и предназначенной для ручной перезагрузки устройства. Если главное устройство перезагружено, то будет перегружен весь стек. Если перезагружается только одно из рядовых устройств стека, перезагрузка остальных устройств производиться не будет.

При включении питания или снижении рабочего напряжения источника питания ниже допустимых пределов запускается контур перезагрузки коммутатора.

Система вентиляции

Коммутаторы PowerConnect 3524/P и PowerConnect 3548/P с функцией питания через Ethernet (PoE) имеют пять встроенных вентиляторов. Модели коммутаторов PowerConnect 3524 и PowerConnect 3548 без функции PoE имеют два встроенных вентилятора. Работу вентиляторов можно проверить по показаниям индикаторов, которые отображают аварийное (отключенное) состояние одного или нескольких вентиляторов.

Назад на страницу "Содержание"

Назад на страницу Содержание

Установка коммутаторов PowerConnect 3524/P и PowerConnect 3548/P

Руководство пользователя систем Dell PowerConnect 35xx

- Подготовка места установки
- Распаковка
- Установка устройства
- Подключение устройства к источнику питания
- Установка стека
- Запуск и настройка устройства

Подготовка места установки

Коммутаторы PowerConnect 3524 /P и PowerConnect 3548/P могут монтироваться на стандартной аппаратурной стойке 48,26-см (19-дюймов) в настольном или настенном исполнении. Перед установкой устройства убедитесь, что выбранное место для установки отвечает следующим требованиям:

- **Питание** — Устройство следует устанавливать поблизости от источников питания переменного тока напряжением 100-240 В, 50-60 Гц (сетевай розетки).
- **Общие положения** — Проверка правильности работы резервного источника питания (RPS) осуществляется по показаниям индикаторов на передней панели.
- **Модели с функцией PoE** — Проверка правильности работы резервного источника питания (RPS) осуществляется по показаниям индикаторов PoE на передней панели.
- **Зазор** — Имеется достаточное расстояние спереди для доступа оператора. Оставьте некоторое расстояние для силовых и сигнальных кабелей, а также для вентиляции.
- **Подключение кабелей** — Прокладка кабелей должна выполняться таким образом, чтобы предотвратить радиопомехи от передатчиков, усилителей, высоковольтных линий и ламп дневного освещения.
- **Требования к окружающей среде** — во время работы температура окружающей среды должна быть в диапазоне от 0 до 45 C (от 32 до 113 F) при относительной влажности от 10% до 90 % без образования конденсата.

Распаковка

Комплект поставки

При распаковке устройства убедитесь, что в комплект поставки входят следующие компоненты:

- Устройство/коммутатор
- Кабель питания
- Кроссоверный кабель RS-232
- Самоклеющиеся резиновые прокладки
- Комплект для крепления на стойке в настенном или настольном исполнении
- Компакт-диск с документацией
- Информационное руководство на изделие

Распаковка устройства

ПРИМЕЧАНИЕ. Перед распаковкой устройства осмотрите упаковку и в случае обнаружения повреждений немедленно сообщите об этом.

1. Установите коробку на чистую гладкую поверхность.
2. Откройте коробку или снимите крышку.
3. Аккуратно извлеките устройство из коробки и положите его на гладкую чистую поверхность.
4. Удалите весь упаковочный материал.
5. Проверьте устройство и принадлежности на предмет отсутствия повреждений. В случае обнаружения повреждений немедленно сообщите об

этом.

Установка устройства

Для установки коммутаторов PowerConnect 3524/P и PowerConnect 3548/P выполняйте следующие указания. Порт консоли находится на задней панели устройства. Гнезда для подключения питания находятся на задней панели. Подключение запасного блока питания (RPS) является необязательным, но рекомендуется. Гнездо резервного источника питания RPS находится на задней панели.

Установка на стойке

Меры предосторожности и указания техники безопасности по установке устройства и подключению других устройств даны в "Информационном руководстве" на изделие.

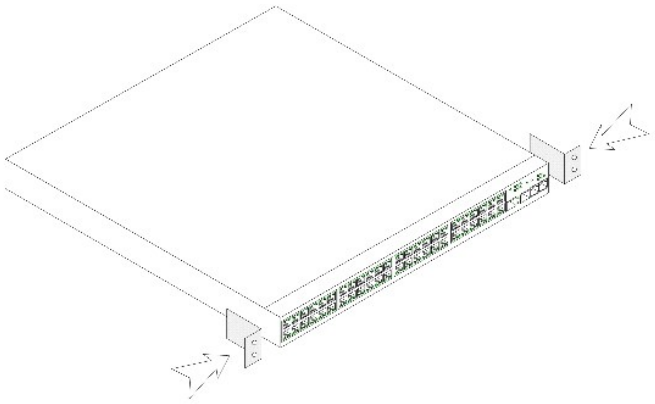
Перед установкой устройства в стойку или шкаф отсоедините от него все кабели.

При установке нескольких устройств в стойку устанавливайте устройства снизу вверх.

1. Установите прилагаемый кронштейн для установки в стойку с одной стороны устройства, чтобы крепежные отверстия на устройстве были совмещены с крепежными отверстиями на кронштейне.

   На следующем рисунке показано, куда следует устанавливать кронштейны.

   Рис. 3-1. Установка монтажного кронштейна и крепление устройства на стойке



2. Вставьте прилагаемые винты в отверстия и затяните с помощью отвертки.

3. Повторите то же самое для кронштейна установки в стойку с другой стороны устройства.

4. Вставьте устройство в 48,26-см (19 дюймов) стойку так, чтобы установочные отверстия на устройстве были совмещены с крепежными отверстиями в стойке.

5. Прикрепите устройство к стойке с помощью винтов (не входят в комплект). Сначала затяните нижнюю пару винтов, а затем верхнюю. Убедитесь, что вентиляционные отверстия не закрыты.

Установка на ровной поверхности

Если устройство не устанавливается в стойку, его следует установить на ровной поверхности. Эта поверхность должна выдерживать вес устройства и кабелей.

1. Прикрепите самоклеющиеся резиновые ножки в каждой отмеченной точке на нижней стороне корпуса.

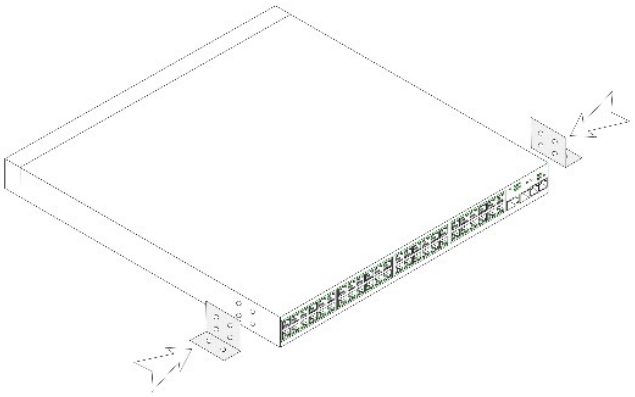
2. Установите устройство на ровную поверхность, оставляя с каждой стороны зазоры шириной 5,08 см (2 дюйма) и зазор шириной 12,7 см (5 дюймов) за задней панелью.

3. Убедитесь, что обеспечивается достаточная вентиляция устройства.

Установка устройства на стене

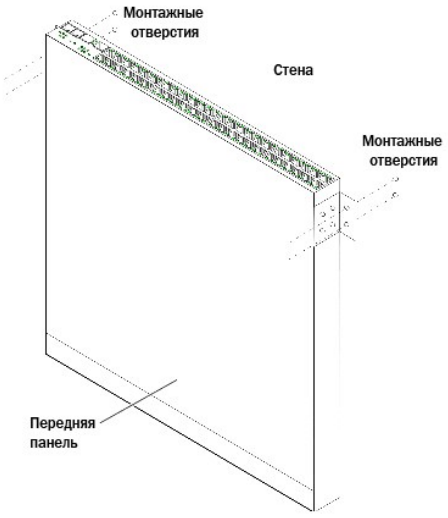
1. Установите монтажный кронштейн, входящий в комплект поставки, на боковую панель устройства, совмещая монтажные отверстия на корпусе устройства с отверстиями кронштейна. На следующем рисунке показано, куда следует устанавливать кронштейны.

   Рис. 3-2. Установка скобы для настенного крепления



2. Вставьте прилагаемые винты в отверстия и затяните с помощью отвертки.
3. Повторите процедуру для другой стороны корпуса устройства.
4. Приложите устройство на стене в месте установки.
5. Разметьте место для монтажных винтов на стене.
6. В размеченных местах просверлите отверстия и вставьте дюбеля (не входят в комплект).
7. Закрепите устройство на стене винтами (в комплект поставки не входят). Убедитесь, что вентиляционные отверстия не закрыты.

   Рис. 3-3. Крепление устройства на стене



Подключение к терминалу

1. Подсоедините кроссоверный кабель RS-232 к терминалу ASCII или к разъему последовательного интерфейса настольного компьютера, на котором установлено программное обеспечение эмуляции терминала.

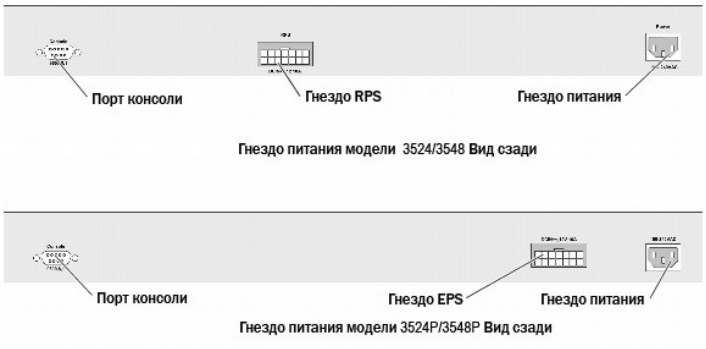
2. Подключите штекер DB-9 кабеля к последовательному порту на задней панели устройства.

Подключение устройства к источнику питания

Подключите сетевой кабель к гнезду питания, находящемуся на задней панели устройства.

ПРИМЕЧАНИЕ. На этом этапе не подключайте кабель питания к заземленной розетке. Процедура подключения устройства к источнику питания подробно описана в разделе Начало работы и настройка устройства.

Рис. 3-4. Гнездо питания на задней панели устройства



После подключения устройства к источнику питания убедитесь, что устройство подключено правильно и работает. Для этого проверьте показания индикаторов на передней панели.

Установка стека

Общие сведения

Каждое устройство может работать как в автономном режиме, так и в качестве одного из устройств стека. В стеке можно объединить до 8 устройств или до 384 портов.

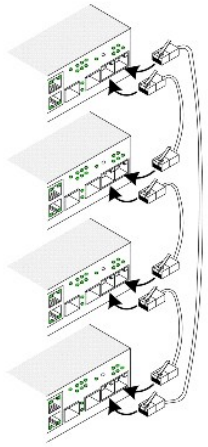
Все стеки должны иметь "Главное устройство" и могут иметь "Резервное устройство", все остальные устройства стека являются рядовыми.

Подключение в стек коммутаторов серии Stacking PowerConnect 35xx

Каждый стек коммутаторов серии PowerConnect 35xx должен иметь одно главное устройство и может иметь одно резервное устройство, все остальные устройства стека являются рядовыми.

Для объединения в стек коммутаторы серии PowerConnect 35xx используют порты RJ-45 Gigabit Ethernet (G3 и G4). Это позволяет добавлять новые стековые возможности без установки дополнительных принадлежностей стековых устройств. Для объединения устройства в стек, вставьте стандартный кабель категории 5 в гнездо порта G3 самого верхнего устройства стека, и в гнездо порта G4 следующего за ним устройства в стеке. Повторяйте эту процедуру, пока не будут подключены все устройства стека. Подключите порт G3 самого последнего устройства стека к порту G4 верхнего устройства стека.

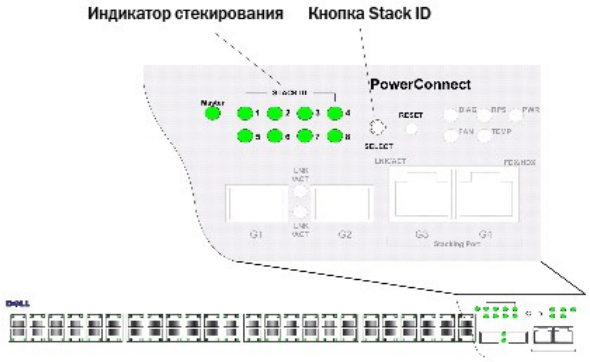
Рис. 3-5. Электрическая схема стека



ПРИМЕЧАНИЕ. В стековом режиме порты G3 и G4 не отображаются во встроенном веб-сервере EWS. Эффект будет таким, как если бы этих портов в устройстве не было. Причина этого в том, что эти порты получают различные индексы стекирования.

Идентификация устройства стека выполняется на передней панели устройства, с помощью кнопки Stack ID.

Рис. 3-6. Настройка стека и идентификационная табличка



Каждое устройство стека имеет уникальный идентификационный номер, определяющий положение и функционал элемента в стеке. Если устройство работает в качестве автономного блока, светодиодный индикатор стека не горит. Установка устройства по умолчанию - автономный режим.

Установка идентификатора устройства производится вручную кнопкой Stack ID. Идентификационный номер устройства отображается светодиодными индикаторами. Идентификационные номера 1 и 2 зарезервированы для главного устройства стека и резервного устройства стека, а номера 3-8 зарезервированы для остальных устройств.

Установка идентификатора устройства

Идентификационный номер устройства устанавливается следующим образом:

1. Убедитесь, что порт консоли автономного/главного устройства подключен к устройству терминала VT100 или эмулятору терминала VT100 с помощью кроссоверного кабеля RS-232.
2. Найдите розетку питания переменного тока.
3. Обесточьте розетку питания переменного тока.
4. Подключите устройство к розетке сети переменного тока.
5. Подайте напряжение на розетку питания переменного тока.

   При включении устройства, начинает мигать светодиодный индикатор, соответствующий идентификатору устройства (в соответствии с ранее запрограммированным и сохраненным номером). Этот индикатор мигает в течение 15 секунд. В течение этого периода необходимо вручную установить конкретный номер идентификатора нажатиями кнопки Stack ID, пока не загорится индикатор нужного номера.

6. **Процесс установки номера** — Нажимайте кнопку Stack ID для выбора светодиодного индикатора с нужным номером. При мигающем индикаторе 8 нажатие кнопки Stack ID конфигурирует автономный режим работы устройства. Повторное нажатие кнопки Stack ID устанавливает номер 1. Устройства с номерами 1 и 2 являются привилегированными устройствами стека. См. раздел Общая информация о стекировании, описание процесса выбора основного устройства стека.

7. **Окончание процесса установки номера** — Процесс установки автоматически завершается по истечение 15-секундного интервала, пока мигает индикатор. Кнопка Stack ID перестает быть активной и номер блока отображается мигающим индикатором по окончании этого периода.

ПРИМЕЧАНИЕ. Эту процедуру необходимо выполнить с каждым блоком, до тех пор пока не будут включены блоки и не будут выбраны идентификаторы блоков Последовательное выполнение указанной операции для каждого из блоков по-отдельности позволяет получить достаточно времени для установки идентификационного номера каждого из блоков. Однако, перед тем, как включать устройства, необходимо подключить их кабелями в соответствии с Электрической схемой стека.

Запуск и настройка устройства

После выполнения всех внешних подключений, подключите к устройству терминал для настройки устройства. Процедура выполнения более сложных пользовательских установок описана в разделе Расширенная настройка.

ПРИМЕЧАНИЕ. Перед выполнением дальнейших действий прочтите примечания к выпуску для этого продукта. Загрузите примечания к выпуску с веб-сайта поддержки Dell **support.dell.com**.

ПРИМЕЧАНИЕ. Рекомендуется получить самую последнюю версию документации пользователя на веб-сайте поддержки Dell **support.dell.com**.

Подключение к устройству

Для настройки устройства, его необходимо подключить к консоли. Однако, если устройство является частью стека, достаточно подключить только одно устройство к терминалу - главное устройство стека. Поскольку управление стеком происходит как управление единым устройством, достаточно произвести настройку только главного устройства стека.

Подключение терминала к устройству

На устройстве имеется порт консоли, который позволяет выполнять подключение к настольному компьютеру с программным обеспечением эмуляции терминала для контроля и настройки устройства. Разъем порта консоли представляет собой штырьковый разъем DB-9, выполненный в виде разъема DTE (data terminal equipment).

Для использования порта консоли требуется следующее:

- VT100-совместимый терминал или настольный / переносной компьютер с последовательным портом, на котором установлено программное обеспечение эмуляции терминала VT100
- Кроссоверный кабель RS-232 с гнездовым разъемом DB-9 для порта консоли и соответствующим разъемом для терминала

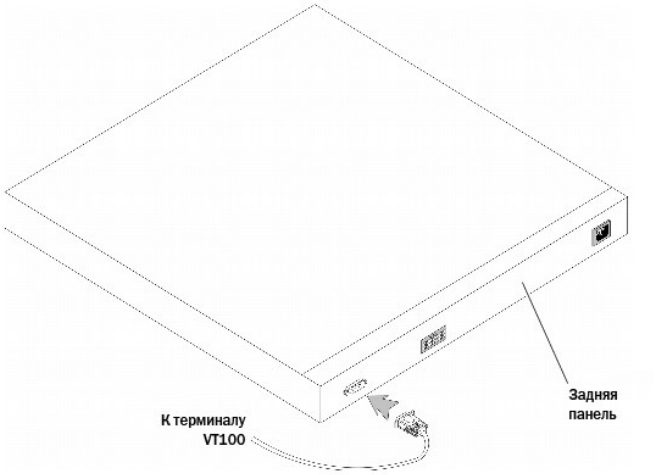
Для подключения терминала к порту консоли устройства, требуется следующее:

1. Подключите кроссоверный кабель RS-232, входящий в комплект поставки, к терминалу, на котором запущена программа эмуляции VT100.
2. Выберите соответствующий последовательный порт (последовательный порт 1 или последовательный порт 2) для подключения к консоли.
3. Задайте скорость передачи данных 9600 бод.
4. Задайте следующий формат данных: 8-битные данные, 1 стоповый бит, без контроля четности.
5. Установите для параметра управления потоком значение *none* (нет).
6. В разделе Properties (Параметры) выберите режим VT100 for Emulation (Эмуляция VT100).
7. Выберите значение Terminal keys (Клавиши терминала) для Function (Функциональные клавиши), Arrow (Клавиши со стрелками) и Ctrl. Убедитесь, что выбраны Terminal keys, а не Windows keys.

ВНИМАНИЕ. При использовании терминала HyperTerminal с операционной системой Microsoft® Windows® 2000 обязательно должен быть установлен пакет обновления 2 или более поздней версии. При наличии пакета обновления 2 для Windows 2000 клавиши со стрелками правильно работают в программе эмуляции HyperTerminal VT100. Информацию о пакетах обновления для Windows 2000 можно найти на сайте www.microsoft.com.

8. Подключите штекер кроссоверного кабеля RS-232 к гнезду консоли главного устройства стека / автономного устройства и зажмите крепежные винты разъема. Гнездо консоли коммутатора серии PowerConnect 35xx находится на задней панели.

Рис. 3-7. Подключение к порту консоли систем серии PowerConnect 35xx



ПРИМЕЧАНИЕ. Консоль может подключаться к порту консоли любого блока стека, но управление стеком может осуществляться только через главное устройство стека (с идентификаторами 1 или 2).

Назад на страницу "Содержание"

Назад на страницу Содержание

Настройка коммутаторов PowerConnect 3524/P и 3548/P

Руководство пользователя систем Dell™ PowerConnect™ 35xx

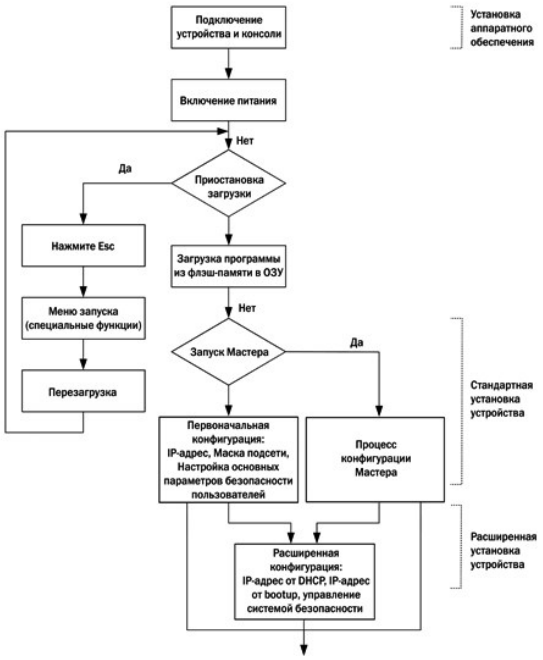
- Процедуры настройки
- Расширенная настройка
- Конфигурация баннеров входа в систему
- Процедуры запуска
- Настройки порта по умолчанию

Процедуры настройки

После выполнения подключений устройства к другим внешним устройствам, к устройству необходимо подключить терминал, предназначенный для управления загрузками и прочими процедурами. Порядок установки и выполнения процедур настроек показан на следующем рисунке:

ПРИМЕЧАНИЕ. Перед выполнением дальнейших действий прочтите примечания к выпуску для этого продукта. Загрузить примечания по продукту можно с официального сайта **support.dell.com**.

Рис. 4-1. Процесс установки и настройки



Загрузка коммутатора

При включении питания с уже подключенным локальным терминалом коммутатор выполняет процедуру проверки при включении питания (POST). Процедура POST выполняется каждый раз при инициализации устройства. Во время этой процедуры выполняется проверка компонентов оборудования и определяется полная работоспособность устройства перед окончательным запуском. В случае обнаружения критической ошибки, выполнение программы прекращается. В случае успешной проверки POST в память ОЗУ загружается действующий образ исполняемого файла. На терминале отображаются сообщения POST, которые показывают успешное или неудачное выполнение процедуры.

Процесс загрузки длится около 30 секунд.

Начальная настройка

ПРИМЕЧАНИЕ. Перед выполнением дальнейших действий прочтите примечания к выпуску для этого продукта. Загрузите примечания к выпуску с веб-сайта поддержки Dell **support.dell.com**.

ПРИМЕЧАНИЕ. Конфигурация по умолчанию предполагает следующее.

- Устройство PowerConnect ранее не настраивалось и находится в том же состоянии, в котором оно было получено.

- Устройство PowerConnect загружено успешно.
- Установлено соединение консоли, а на экране устройства терминала VT100 отображается приглашение консоли.

Начальная конфигурация устройства задается через порт консоли. После начальной конфигурации можно выполнять управление устройством либо через подключенный порт консоли, который уже подключен, либо удаленно через интерфейс, определенный во время начальной конфигурации.

Если устройство запускается в первый раз или если файл конфигурации пуст по причине того, что устройство не настроено, пользователю необходимо использовать "Мастер настройки". "Мастер настройки" осуществляет руководство начальной настройкой устройства и максимально быстро подготавливает и запускает устройство.

ПРИМЕЧАНИЕ. Перед настройкой устройства необходимо получить у администратора сети следующую информацию.

- IP-адрес, который необходимо назначить для VLAN 1, через который будет выполняться управление устройством (по умолчанию, все порты входят в VLAN 1)
- IP-маска подсети для сети
- IP-адрес шлюза по умолчанию (маршрутизатор ближайшего узла) для настройки маршрута по умолчанию.
- IP-адрес строки сообщества SNMP и системы управления SNMP (необязательно)
- Имя пользователя и пароль

"Мастер настройки" осуществляет руководство начальной настройкой коммутатора и максимально быстро подготавливает и запускает систему. Можно пропустить операции Мастера настройки и настроить устройство вручную в режиме интерфейса командной строки.

"Мастер настройки" настраивает следующие поля.

- IP-адрес строки сообщества SNMP и системы управления SNMP (необязательно)
- Имя пользователя и пароль
- IP-адрес устройства
- IP-адрес шлюза по умолчанию

Отобразится следующее:

```
Welcome to Dell Easy Setup Wizard (Добро пожаловать в программу "Мастер настройки" компании Dell)

The Setup Wizard guides you through the initial switch configuration, and gets you up and running as quickly as possible ("Мастер
настройки" позволит вам произвести первоначальные настройки коммутатора и запустить его в кратчайшие сроки). You can skip the setup
wizard, and enter CLI mode to manually configure the switch (Вы можете пропустить "Мастер настройки" и вручную ввести команды консоли для
настройки коммутатора).
The system will prompt you with a default answer; by pressing enter, you accept the default (Система выдает подсказки, содержащие
установки по умолчанию. Нажатие кнопки ввода принимает настройку по умолчанию).
You must respond to the next question to run the setup wizard within 60 seconds, otherwise the system will continue with normal operation
using the default system configuration (Вы должны ответить на следующий вопрос в течение 60 секунд, в противном случае система
возвратится к нормальному режиму работы с использованием настройки по умолчанию ).

Would you like to enter the Setup Wizard (you must answer this question within 60 seconds? (Вы хотите запустить "Мастер настройки"?
(Необходимо ответить в течение 60 секунд.)) (Y/N)[Y]Y
(Да/Нет) You can exit the Setup Wizard at any time by entering [ctrl+Z] Закрыть "Мастер настройки" можно в любое время нажатием [ctrl+Z].
```

При вводе [N] "Мастер настройки" закроется. Если ответа на запрос не будет в течение 60 секунд, "Мастер настройки" закроется автоматически, и отобразится приглашение консоли.

При вводе [Y] "Мастер настройки" будет осуществлять интерактивное руководство начальной настройкой устройства.

ПРИМЕЧАНИЕ. Если ответа на запрос не будет в течение 60 секунд, а к сети подключен сервер BootP, адрес можно получить с сервера BootP.

ПРИМЕЧАНИЕ. Можно в любой момент закрыть "Мастер настройки", нажав комбинацию клавиш [ctrl+z].

Мастера настройки - шаг 1

Отобразится следующее:

```
The system is not setup for SNMP management by default (Система не установлена для управления по SNMP по умолчанию).
To manage the switch using SNMP (required for Dell Network Manager) you can (Для управления коммутатором с помощью SNMP (требуется для
программы Dell Network Manager) вы можете):

   l Setup the initial SNMP version 2 account now (Установить первоначальный профиль SNMP версии 2).

   l Return later and setup additional SNMP v1/v3 accounts (Возвратиться позднее и установить дополнительные профили SNMP версий 1/3).

For more information on setting up SNMP accounts, please see the user documentation (Дополнительную информацию по профилям SNMP см. в
документации пользователя).

Would you like to setup the SNMP management interface now? (Вы хотите установить интерфейс управления SNMP сейчас?) (Y/N)[Y]Y (Д/Н)
```

Введите [N], чтобы пропустить шаг 2.

Введите [Y], чтобы продолжить работу Мастера настройки. Отобразится следующее:

```
To setup the SNMP management account you must specify the management system IP address and the "community string" or password that the
particular management system uses to access the switch (Чтобы установить управление SNMP, вам необходимо указать IP-адрес системы
управления и «строку сообщества» или пароль, которые использует конкретная система управления для доступа к коммутатору). The wizard
```

automatically assigns the highest access level [Privilege Level 15] to this account ("Мастер настройки" автоматически назначает этому профилю самый высокий уровень доступа (15)).
You can use Dell Network Manager or CLI to change this setting, and to add additional management systems (Вы можете использовать Dell Network Manager или команды консоли для добавления других систем управления). For more information on adding management systems, see the user documentation (Более подробная информация по добавлению систем управления см. в пользовательской документации).
To add a management station: (Для добавления станции управления:)
Please enter the SNMP community string to be used: (Введите строку сообщества SNMP, которое будет использоваться) [Dell_Network_Manager]
Please enter the IP address of the Management System (A.B.C.D) or wildcard (0.0.0.0) to manage from any Management Station: (Введите IP-адрес системы управления (A.B.C.D) или маску ввода (0.0.0.0) для управления с любой станции:) [0.0.0.0]

Введите следующие сведения.

- Строку сообщества SNMP, например Dell_Network_Manager.
- IP-адрес системы управления (A.B.C.D) или маску ввода (0.0.0.0) для управления с любой станции управления.

ПРИМЕЧАНИЕ. Нельзя использовать IP-адрес и маски ввода, начинающиеся с нуля.

Нажмите клавишу **Enter**.

Мастер настройки - шаг 2

Отобразится следующее:

Now we need to setup your initial privilege (Level 15) user account (Теперь необходимо установить начальный уровень привилегии профиля пользователя (Уровень 15)).
This account is used to login to the CLI and Web interface (Этот профиль используется для доступа к системе команд консоли и к веб-интерфейсу).
You may setup other accounts and change privilege levels later (Вы можете установить другие профили и изменить уровень привилегии позднее).
For more information on setting up user accounts and changing privilege levels, see the user documentation (Более подробную информацию по установке пользовательских профилей и изменению уровней привилегии см. в документации пользователя).
To setup a user account: (Для того, чтобы установить профиль пользователя:)
Enter the user name<1-20>: (Введите имя пользователя (1-20 символов))[admin]
Please enter the user password:* (Введите пароль)
Please reenter the user password:* (Введите пароль повторно)

Введите следующие сведения.

- Имя пользователя, например «admin»
- Пароль и подтверждение пароля.

ПРИМЕЧАНИЕ. Если первый и второй пароли не совпадают, запрос будет появляться, пока они не станут одинаковыми.

Нажмите клавишу **Enter**.

Мастер настройки - шаг 3

Отобразится следующее:

Next, an IP address is setup. (Теперь необходимо установить IP-адрес)

The IP address is defined on the default VLAN (VLAN #1), of which all ports are members. (Ip-адрес определен по умолчанию в сети VLAN (VLAN#1), в которой зарегистрированы все порты) This is the IP address you use to access the CLI, Web interface, or SNMP interface for the switch.To setup an IP address: (Это тот IP-адрес, который вы будете использовать для доступа к командам консоли, веб-интерфейсу или SNMP-интерфейсу коммутатора. Для того, чтобы установить IP-адрес:)

Please enter the IP address of the device (A.B.C.D):[1.1.1.1] (Введите IP-адрес устройства (A.B.C.D):[1.1.1.1])

Please enter the IP subnet mask (A.B.C.D or nn): (Введите маску подсети IP (A.B.C.D или nn)) [255.255.255.0]

Enter the IP address and IP subnet mask, for example 1.1.1.1 as the IP address and 255.255.255.0 as the IP subnet mask. (Введите IP-адрес или маску подсети IP, например, 1.1.1.1 в качестве IP-адреса и 255.255.255.0 в качестве маски подсети IP.)

Нажмите клавишу **Enter**.

Мастер настройки - шаг 4

Отобразится следующее:

Finally, setup the default gateway (Теперь установите шлюз по умолчанию).
Please enter the IP address of the gateway from which this network is reachable (e.g. 192.168.1.1).Default gateway (A.B.C.D):[0.0.0.0]
(Введите IP-адрес шлюза, с которого доступна сеть (например, 192.168.1.1). Шлюз по умолчанию (A.B.C.D):[0.0.0.0]).

Введите шлюз по умолчанию.

Нажмите клавишу **Enter**. Отобразятся следующие сообщения (в каждом примере описаны разные параметры).

```
This is the configuration information that has been collected: (Ниже приведены параметры настройки:)

============================================================

SNMP Interface = Dell_Network_Manager@0.0.0.0
User Account setup = admin
Password = *
Management IP address = 1.1.1.1 255.255.255.0
Default Gateway = 1.1.1.2 (Интерфейс SNMP = Dell_Network_Manager@0.0.0.0
Профиль пользователя = admin
Пароль= *
IP-адрес системы управления = 1.1.1.1 255.255.255.0
Шлюз по умолчанию = 1.1.1.2)

============================================================
```

Мастер настройки - шаг 5

Отобразится следующее:

```
If the information is correct, please select (Y) to save the configuration, and copy to the start-up configuration file (Если информация правильная, нажмите Y(Д), чтобы сохранить настройки и скопировать их в конфигурационный файл запуска). If the information is incorrect, select (N) to discard configuration and restart the wizard: (Если информация неправильная, выберите N(Н) чтобы удалить установки и запустить "Мастер настройки" повторно:) (Y/N)[Y]Y (Д/Н [Д]Д)
```

Введите [N], чтобы не перезагружать Мастер настройки.

Введите [Y], чтобы завершить работу Мастера настройки. Отобразится следующее:

```
Configuring SNMP management interface
Configuring user account......
Configuring IP and subnet......
(Идет настройка интерфейса управления SNMP. Идет настройка профиля пользователя...Идет настройка IP и маски подсети...)

Thank you for using Dell Easy Setup Wizard (Спасибо, что воспользовались "Мастером настройки"). You will now enter CLI mode (Теперь вы будете перенаправлены в режим ввода команд консоли).
```

Мастер настройки - шаг 6

Отобразится приглашение команд консоли.

Расширенная настройка

В этом разделе дается информация о динамическом распределении IP-адресов и управлении безопасности на основе механизма протокола AAA (проверка подлинности, авторизация и ведение профилей пользователя), и включает в себя следующие подразделы:

- Настройка IP-адресов с использованием протокола DHCP.
- Настройка IP-адресов с использованием протокола BOOTP.
- Управление системой безопасности и настройка паролей

При настройке или получении IP-адресов через DHCP и BOOTP, полученная от этих серверов конфигурация содержит IP-адрес и может содержать маску подсети и шлюз по умолчанию.

Получение IP-адреса от сервера DHCP

Если для получения IP-адреса используется протокол DHCP, то устройство работает как DHCP-клиент. При перезагрузке устройства, команда сервера DHCP будет сохранена в конфигурационном файле, но IP-адрес сохранен не будет. Чтобы получить IP-адрес от сервера DHCP, необходимо выполнить следующие действия:

1. Выберите и подсоедините любой порт к серверу DHCP или к подсети, в которой имеется сервер DHCP, чтобы получить IP-адрес.
2. Введите следующие команды, чтобы использовать выбранный порт для получения IP-адреса. В следующем примере команды зависят от типа порта, используемого для настройки.
   - Назначение динамического IP-адреса:

     ```
     console# configure

     console(config)# interface ethernet 1/e1

     console(config-if)# ip address dhcp hostname powerconnect

     console(config-if)# exit
     ```

```
console(config)#
```

- Назначение динамического IP-адреса (на VLAN):

```
console# configure

console(config)# interface ethernet vlan 1

console(config-if)# ip address dhcp hostname device

console(config-if)# exit

console(config)#
```

Интерфейс получает IP-адрес автоматически.

3. Для проверки IP-адреса введите команду **show ip interface** в приглашении системы, как показано в следующем примере.

```
console# show ip interface

IP Address I/F Type

------------- ------ -------

100.1.1.1/24 vlan 1 dynamic
```

ПРИМЕЧАНИЕ. Не нужно удалять конфигурацию устройства, чтобы получить IP-адрес и загрузить его на сервер DHCP.

ПРИМЕЧАНИЕ. При копировании файлов настройки не используйте файл настройки, содержащий инструкцию для включения протокола DHCP для интерфейса, который подключен к тому же серверу DHCP или к серверу с аналогичной настройкой. В этом примере устройство получает новый файл настройки и выполняет загрузку на основе данных из этого файла. Затем коммутатор включает протокол DHCP в соответствии с инструкциями в новом файле настройки, а затем DHCP выдает указание на повторную загрузку того же файла.

ПРИМЕЧАНИЕ. При конфигурировании IP-адреса на сервере DHCP, этот адрес вызывается автоматически, и `ip address dhcp` команда будет сохранена в конфигурационном файле. В случае возникновения неполадок главного устройства, резервное устройство начнет повторную попытку вызова адреса DHCP. Это может привести к одному из следующих результатов:

- Может быть назначен тот же IP-адрес.
- Может быть назначен другой IP-адрес, и это может повлечь за собой потерю связи со станцией управления.
- Сервер DHCP может отключиться, что приведет к ошибке получения IP-адреса и к возможной потере связи со станцией управления.

Получение IP-адреса от сервера BOOTP

Поддерживается стандартный протокол BOOTP, позволяющий коммутатору автоматически загружать настройку своего хоста IP с любого стандартного сервера BOOTP в сети. В этом случае устройство работает как клиент BOOTP.

Чтобы получить IP-адрес от сервера BOOTP:

1. Выберите и подсоедините любой порт к серверу BOOTP или к подсети, в которой имеется такой сервер, чтобы получить IP-адрес.

2. В командной строке системы введите команду **delete startup configuration**, чтобы удалить запускаемую настройку из флэш-памяти.

Устройство перезагружается без настройки и через 60 секунд начинает посылать запросы BOOTP. Устройство получает IP-адрес автоматически.

ПРИМЕЧАНИЕ. Когда устройство начинает перезагружаться, любой ввод с терминала ASCII или клавиатуры автоматически отменяет процесс BOOTP до его завершения, и устройство не получает IP-адрес от сервера BOOTP.

Этот процесс показан в следующем примере:

```
console> enable

console# delete startup-config

Startup file was deleted (Файл запуска был удален)

console# reload

Изменения не были сохранены. Are you sure you want to continue (y/n) [n] (Вы уверены, что хотите продолжить (д/н) [н])?

This command will reset the whole system and disconnect your current session (Эта команда приведет к перезагрузке системы и отключит
текущий сеанс). Do you want to continue (y/n) [n] (Вы хотите продолжить (д/н) [н]))?

*****************************************************

/* устройство перезагрузится */
```

Чтобы проверить IP-адрес, введите команду **show ip interface**.

Теперь для устройства настроен IP-адрес.

Управление системой безопасности и настройка паролей

Безопасность системы обеспечивается механизмом AAA (authentication, authorization, accounting - проверка подлинности, авторизация и учетные записи), который управляет правами доступа и привилегиями пользователей, а также способами администрирования. AAA использует как локальные, так и удаленные пользовательские базы данных. Шифрование данных производится посредством механизма SSH.

Система поставляется без настроенного пароля по умолчанию; все пароли определяются пользователем. Если определенный пользователем пароль утрачен, то можно вызвать процедуру восстановления пароля из меню **Startup** (Запуск). Эта процедура применима только для локального терминала и допускает однократный доступ к устройству с локального терминала без ввода пароля.

Настройка паролей системы безопасности

Можно настроить пароли системы безопасности для следующих служб:

- Терминал
- Telnet
- SSH
- HTTP
- HTTPS

ПРИМЕЧАНИЕ. Пароли определяются пользователем.

ПРИМЕЧАНИЕ. При создании имени пользователя по умолчанию назначается приоритет 1, который разрешает доступ, но не дает прав на настройку. Для разрешения доступа и предоставления прав настройки устройства необходимо установить приоритет 15. Несмотря на то, что уровень привилегий 15 можно указать для пользователей, не назначая пароля, рекомендуется всегда назначать пароль. Если пароль не определен, привилегированные пользователи могут получить доступ к веб-интерфейсу под любым паролем.

ПРИМЕЧАНИЕ. Пароли устанавливаются командами управления паролями, с помощью которых можно определить устаревшие пароли и срок действия паролей. Более подробная информация дана в разделе Управление безопасностью и настройка паролей.

Настройка первоначального пароля терминала

Для настройки первоначального пароля терминала введите следующие команды:

```
console(config)# aaa authentication login default line

console(config)# aaa authentication enable default line

console(config)# line console

console(config-line)# login authentication default

console(config-line)# enable authentication default

console(config-line)# password george
```

- Во время первоначальной регистрации в устройстве через сеанс консоли в ответ на приглашение ввести пароль введите `george`.`george`
- При установке режима устройства «включено» в ответ на приглашение ввести пароль введите `georgegeorge`.

Настройка первоначального пароля Telnet

Для настройки первоначального пароля Telnet введите следующие команды:

```
console(config)# aaa authentication login default line

console(config)# aaa authentication enable default line

console(config)# line telnet

console(config-line)# login authentication default

console(config-line)# enable authentication default

console(config-line)# password bob
```

- При первоначальном входе в устройство с вводом пароля во время сеанса Telnet, введите пароль `bob` в строке приглашения ко вводу пароля.
- При установке режима устройства «включено» введите `bob`.

Настройка первоначального пароля SSH

Для настройки начального пароля SSH введите следующие команды:

```
console(config)# aaa authentication login default line
```

```
console(config)# aaa authentication enable default line

console(config)# line ssh

console(config-line)# login authentication default

console(config-line)# enable authentication default

console(config-line)# password jones.
```

- При первоначальном подключении к устройству с вводом пароля во время сеанса SSH, введите jones в строке приглашения.
- При установке режима устройства «включено» введите jones.

Настройка первоначального пароля HTTP

Для настройки первоначального пароля HTTP введите следующие команды:

```
console(config)# ip http authentication local

console(config)# username admin password user1 level 15
```

Настройка первоначального пароля HTTPS

Для настройки первоначального пароля HTTPS введите следующие команды:

```
console(config)# ip https authentication local

console(config)# username admin password user1 level 15
```

Сразу после настройки сеансов терминала, Telnet или сеанса SSH для использования сеанса HTTPS необходимо ввести следующие команды.

ПРИМЕЧАНИЕ. В веб-браузере включите отображение на странице данных SSL 2.0 и последующих версий.

```
console(config)# crypto certificate generate key_generate

console(config)# ip https server
```

При первоначальном запуске сеанса http или https, введитеadmin в качестве имени пользователя и user1 в качестве пароля.

ПРИМЕЧАНИЕ. Службы Http и Https требуют уровня доступа 15 и соединяются непосредственно с уровнем доступа настройки.

Конфигурация баннеров входа в систему

Вы можете определить 3 типа баннеров входа в систему:

- **Баннер «Совет дня»:** Отображается при подключении к устройству, перед входом в систему.
- **Баннер входа в систему:** Отображается после баннера «Совет дня», и перед тем, как пользователь войдет в систему.
- **Баннер успешного входа:** Отображается после успешного входа пользователя в систему (на всех уровнях пользовательских привилегий и при всех способах авторизации).

Для просмотра и настройки баннеров входа в систему:

```
console# banner motd Welcome

console# show banner motd

console# banner login Please log in

console# show banner login

console# banner exec Successfully logged in

console# show banner exec
```

Процедуры запуска

Процедуры меню Startup (Запуск)

Запускаемые из меню Startup (Запуск) процедуры включают загрузку программного обеспечения, работу с флэш-памятью и восстановление пароля. Процедуры диагностики должны выполняться только персоналом службы технической поддержки и в этом документе не описываются.

Вход в меню запуска осуществляется при загрузке устройства. Пользователь должен ввести данные сразу после прохождения проверки POST.

Для входа в меню Startup (Запуск):

1. Включите питание и дождитесь появления сообщения автозагрузки.

   ```
   ************************************************

   ***************** SYSTEM RESET (ПЕРЕЗАПУСК СИСТЕМЫ) *****************

   ************************************************

   Boot1 Checksum Test (Загрузка 1 проверка контрольной суммы).............................PASS (УСПЕШНО)

   Boot2 Checksum Test (Загрузка 2 Проверка контрольной суммы).............................PASS (УСПЕШНО)

   Flash Image Validation Test (Проверка пригодности образа флэш-памяти).....................PASS (УСПЕШНО)

   BOOT Software Version 1.0.0.05 Built 06-Jan-xxxx 14:46:49 (ЗАГРУЗКА ПО версия 1.0.0.05 от 6 января xxxx 14:46:49)

   Ryan board, based on PPC8247 (Плата Ryan на базе PPC8247)

   128 MByte SDRAM (128 МБ памяти SDRAM). I-Cache 16 KB (Кэш-память 16 КБ). D-Cache 16 KB (Кэш-память 16 КБ). Cache Enabled (Включена
   функция сохранения в кэш-памяти).

   Autoboot in 2 seconds - press RETURN or Esc to abort and enter prom (Автозагрузка через 2 секунды – нажмите RETURN или Esc, чтобы выйти).
   ```

2. При появлении сообщения автозагрузки нажмите клавишу **<Enter>** для входа в меню Startup (Запуск). Выполнять процедуры меню Startup (Запуск) можно с помощью терминала ASCII или терминала HyperTerminal Windows.

   ```
   [1] Download Software (Загрузка программы)

   [2] Erase Flash File (Удаление файла из флэш-памяти)

   [3] Password Recovery Procedure (Процедура восстановления пароля)

   [4] Enter Diagnostic Mode (Вход в режим диагностики)

   [5] Set Terminal Baud-Rate (Установка скорости передачи данных терминала)

   [6] Back (Назад)
   ```

В следующих разделах описаны доступные параметры меню Startup (Запуск).

ПРИМЕЧАНИЕ. При выборе опций и меню Запуск, запускается таймер реакции: Если в течение 35 секунд (по умолчанию) не будет выбран ни один из пунктов меню, истечет время ожидания команды. Значение времени ожидания по умолчанию можно изменить с помощью команд консоли.

ПРИМЕЧАНИЕ. К работе в режиме диагностики допускается только квалифицированный технический персонал (**option[4]**). По этой причине параметры пункта Enter Diagnostics Mode (Перейти в режим диагностики) не описаны в этом руководстве.

Загрузка программного обеспечения – пункт меню [1]

Процедура загрузки программного обеспечения используется, когда необходима загрузка новой версии программного обеспечения для замены поврежденных файлов или обновления системного программного обеспечения. Для того, чтобы загрузить программное обеспечение через меню запуска:

1. В меню Startup (Запуск) нажмите клавишу [1]. Появится следующее сообщение:

   ```
   Downloading code using XMODEM (Загрузка с использованием XMODEM)

   ********************************************************************

   *** Running SW Ver. 21_08 (Текущая версия ПО) Date 21-Aug-xxxx Time 17:22:25 *** (Дата и время)

   ********************************************************************

   HW version is 00.00.00 (версия системы)

   Base Mac address is: 00:14:47:78:89:96 (Mac-адрес)

   Dram size is (Размер диска) : 128M bytes (128 Мб)

   Dram first block size is (Размер первого блока динамической памяти) : 102400 K bytes (102 400 КБ)

   Dram first PTR is (Первое считывание) : 0x1800000
   ```

```
Dram second block size is (Размер второго блока динамической памяти) : 4096 K bytes (4 096 КБ)

Dram second PTR is (Второе считывание) : 0x7C00000

Flash size is (Размер флэш-памяти): 16M

01-Jan-xxxx 01:01:07 %CDB-I-LOADCONFIG: Loading running configuration (Загрузка текущей конфигурации).

01-Jan-xxxx 01:01:07 %CDB-I-LOADCONFIG: Loading startup configuration (Загрузка текущей конфигурации).

Device configuration: (Конфигурация устройства)

CPLD revision: (Редакция CPLD) 1.01

Slot 1 - PowerConnect 35xx HW Rev. 1.1 (Слот 1 - PowerConnect 35xx )

------------------------------------

-- Unit Standalone (Компонент – автономный режим) --

------------------------------------

Tapi Version:(Версия Tapi) v1.3.3.1

Core Version:(Версия Core v1.3.3.1

01-Jan-xxxx 01:01:19 %INIT-I-InitCompleted: Initialization task is completed (Инициализация завершена)

01-Jan-xxxx 01:01:19 %SNMP-I-CDBITEMSNUM: Number of running configuration items loaded:(Количество рабочих параметров) 0

01-Jan-xxxx 01:01:19 %SNMP-I-CDBITEMSNUM: Number of startup configuration items loaded: (Количество параметров загрузки) 0

01-Jan-xxxx 01:01:20 %Box-I-SFP-PRESENT-CHNG: unit_id 1 SFP 0 status is not present (Отсутствует статус 0 для unit_id 1 SFP).

01-Jan-xxxx 01:01:20 %Box-I-SFP-PRESENT-CHNG: unit_id 1 SFP 1 status is not present (Отсутствует статус 0 для unit_id 1 SFP).
```

2. При использовании HyperTerminal нажмите **Transfer** (Передача) в строке меню HyperTerminal.
3. В поле **Filename** (Имя файла) укажите путь к файлу, который необходимо загрузить.
4. Убедитесь, что в поле **Protocol** (Протокол) выбран протокол Xmodem.
5. Нажмите **Send** (Переслать). Начнется загрузка программного обеспечения.

ПРИМЕЧАНИЕ. После загрузки программного обеспечения устройство перезагружается автоматически.

Удаление файла FLASH - опция[2]

В некоторых случаях требуется стереть настройку устройства. Если настройка удалена, все параметры, настроенные с помощью команд консоли, встроенного веб-сервера или SNMP, должны быть настроены заново.

Чтобы удалить настройку устройства:

1. В меню Startup (Запуск) нажмите [2] на 6 секунд, чтобы удалить файл флэш-памяти. Появится следующее сообщение:

   ```
   Warning! About to erase a Flash file. (Внимание! Вы собираетесь удалить файл флэш-памяти)

   Are you sure (Y/N)? (Вы действительно хотите это сделать? Д/Н) y
   ```

2. Нажмите клавишу Y. Появится следующее сообщение.

   ```
   Write Flash file name (Up to 8 characters, Enter for none.):config (введите имя файла флэш-памяти, максимум 8 символов)

   File config (if present) will be erased after system initialization (Файл config (если имеется) будет удален после инициализации системы)

   ======== Press Enter To Continue (Нажмите Enter, чтобы продолжить)========
   ```

3. Введите config в качестве имени файла флэш-памяти. Конфигурация будет удалена, а устройство перезагружено.
4. Повторите начальную настойку устройства.

Восстановление пароля - опция [3]

Если определенный пользователем пароль утрачен, то можно вызвать процедуру восстановления пароля из меню Startup (Запуск). Эта процедура

позволяет пользователю один раз войти в устройство без пароля.

Для восстановления утраченного пароля только для входа в локальный терминал:

1. В меню Startup (Запуск) нажмите [3], а затем нажмите клавишу **<Enter>**. Пароль будет удален.

   Введите нужное значение или нажмите **ESC** для выхода

   `Current password will be ignored! (Текущий пароль будет проигнорирован!)`

ПРИМЕЧАНИЕ. Чтобы обеспечит безопасность устройства, заново настройте пароль для соответствующих методов управления.

Вход в режим диагностики (Diagnostic Mode) - опция[4]

Только для авторизованного сервисного персонала.

Установка скорости передачи данных терминала - опция [5]

Для установки скорости передачи данных терминала, введите [5] и нажмите <Enter>.

Введите нужное значение или нажмите 'ESC' для выхода:

`Set new device baud-rate (Новое значение скорости передачи): 38,400`

Загрузка программного обеспечения через сервер TFTP

В этом разделе содержатся инструкции для загрузки программного обеспечения (системного и загрузочного образа) через сервер TFTP. Перед началом загрузки программного обеспечения необходимо настроить сервер TFTP.

Загрузка системного образа

Устройство загрузится и выполнит распаковку образа системы из флэш-памяти, где хранится копия образа системы. При загрузке нового образа он сохраняется в другой области, выделяемой для дополнительной копии образа системы.

При следующей загрузке устройство разархивирует данные и запустится, используя текущий активный системный образ, если не выбрано иное.

Для загрузки системного образа через сервер TFTP:

1. Убедитесь, что IP-адрес настроен для одного из портов устройства, и поверьте соединение с сервером TFTP с помощью команды ping.

2. Убедитесь, что файл, подлежащий загрузке, сохранен на сервере TFTP (файлarc).

3. Введите команду **show version** для проверки версии ПО, работающего на устройстве. Далее приведен пример отображаемой на экране информации:

   `console# show version`

   `SW version 1.0.0.30 (date 27-Jan-xxxx time 13:42:41) (версия ПО, дата, время)`

   `Boot version 1.0.0.05 (date 27-Jan-xxxx time 15:12:20) (версия загрузчика, дата, время)`

   `HW version (версия аппаратного обеспечения)`

4. Введите команду **show bootvar** для проверки текущего активного системного образа. Далее приведен пример отображаемой на экране информации:

   `console# show bootvar`

   `Images currently available on the Flash (образ, имеющийся во флэш-памяти)`

   `Image-1 active (selected for next boot) (активен образ 1—он выбран для следующей загрузки)`

   `Image-2 not active (образ 2 не активен)`

   `console#`

5. Введите команду **copy tftp:**//{tftp address}/{file name} **image** для копирования нового системного образа на устройство. При загрузке нового образа он сохраняется в другой области, выделяемой для следующей копии образа системы (image-2, как указано в данном примере). Далее приведен пример отображаемой на экране информации:

   `console# copy tftp://176.215.31.3/file1.ros image`

```
Accessing file `file1' on 176.215.31.30 (поиск файла file1 на 176.215.31.30)

Loading file1 from 176.215.31.3:(загрузка файла)

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Copy took 00:01:11 [hh:mm:ss]
```

Знаки восклицания указывают, что процесс не завершен. Каждый символ (!) соответствует 512 байтам информации, которые были успешно переданы. Точка указывает, что истекло время ожидания для процесса копирования. Несколько точек в строке показывают, что возникла ошибка в процессе копирования.

6. Выберите образ для следующей загрузки, введя системную команду boot. После ввода этой команды, введите команду **show bootvar** для проверки того, что эта копия, указанная в качестве параметра в команде **boot system**, выбрана для следующей загрузки.

   Далее приведен пример отображаемой на экране информации:

   ```
   console# boot system image-2

   console# show bootvar

   Images currently available on the Flash (образ, имеющийся во флэш-памяти)

   Image-1 active (образ 1 активен)

   Image-2 not active (selected for next boot) (образ 2 не активен— выбран для следующей загрузки)
   ```

   Если не выбрать образ для следующей загрузки путем ввода команды boot system, то система выполнит загрузку с использованием текущего активного образа.

7. Введите команду **reload**. Появится следующее сообщение:

   ```
   console# reload

   This command will reset the whole system and disconnect your current session. Do you want to continue (y/n) [n]? (Вы действительно хотите продолжить?)
   ```

8. Введите y Устройство будет перезагружено.

Загрузка загрузочного образа

При загрузке нового загрузочного образа с сервера TFTP и программировании его во флэш-память обновляется загрузочный образ. Загрузочный образ загружается при включении питания устройства. У пользователя *нет* возможности управлять копиями загрузочного образа. Для загрузки загрузочного образа через сервер TFTP:

1. Убедитесь, что IP-адрес настроен для одного из портов устройства, и поверьте соединение с сервером TFTP с помощью команды ping.

2. Убедитесь, что файл, который нужно загрузить (файл rfb), сохранен на сервере TFTP.

3. Введите команду отображения версии ПО и проверьте текущий номер версии программного обеспечения, работающего на устройстве. Далее приведен пример отображаемой на экране информации:

   ```
   console# show version

   SW version 1.0.0.30 (date 27-Jan-xxxx time 13:42:41) (версия ПО, дата, время)

   Boot version 1.0.0.05 (date 27-Jan-xxxx time 15:12:20) (версия загрузчика, дата, время)

   HW version (версия аппаратного обеспечения)
   ```

4. Введите команду **copy tftp:**//{tftp address}/{file name} **boot** для копирования образа загрузки на устройство. Далее приведен пример отображаемой на экране информации:

   ```
   console# copy tftp://176.215.31.3/332448-10018.rfb boot

   Erasing file..done (Удаление файла..выполнено).

   !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

   Copy: 2739187 bytes copied in 00:01:13 [hh:mm:ss]
   ```

5. Введите команду **reload** (перезагрузить). Появится следующее сообщение:

   ```
   console# reload

   This command will reset the whole system and disconnect your current session (По этой команде сеанс работы будет прерван и произойдет перезагрузка системы). Do you want to continue (y/n) [n]? (Вы действительно хотите продолжить?)
   ```

6. Введите Y .y Устройство будет перезагружено.

Настройки порта по умолчанию

Общая информация по настройке портов устройства включает краткое описание механизма автоматического согласования и параметры по умолчанию для коммутируемых портов.

Автоматическое согласование

Автоматическое согласование позволяет выполнять автоматическое определение скорости, режима дуплекса и выполнять управление потоком данных на всех портах 10/100/1000BaseT коммутатора. Функция автоматического согласования по умолчанию включена на каждом порту.

Автоматическое согласование - это механизм, установленный между двумя партнерами по связи, который позволяет порту оповестить партнера по связи о своей скорости передачи, возможности работы в дуплексном режиме и управления потоком (функция управления потоком по умолчанию отключена). Порты затем работают с максимальным общим знаменателем.

Если подсоединен контроллер сетевого интерфейса (NIC), который не поддерживает или не настроен на автосогласование, то и коммутируемый порт устройства, и NIC необходимо настроить вручную на одинаковую скорость передачи и дуплексный режим.

Если станция на другом конце связи совершает попытку автоматического согласования с портом 100BaseT устройства, который настроен для работы в полном дуплексном режиме, результатом такого согласования будет работа этой станции в полудуплексном режиме.

MDI/MDIX

Устройство автоматически обнаруживает, какие кабели подключены - перекрестные или кабели прямого подключения на всех коммутируемых портах 10/100/1000BaseT. Эта функция является частью функции автоматического согласования и включается при включении автосогласования.

Если включен интерфейс MDI/MDIX (зависимый от среды интерфейс с кроссоверным кабелем), возможно выполнение автоматического исправления ошибок передачи по кабелю. Тем самым устраняется необходимость делать различия между проходным кабелем и кроссоверным кабелем. (Стандартный тип кабельного подключения для конечных станций - MDI (зависимый от среды интерфейс), а стандартный тип кабельного подключения для коммутаторов и концентраторов - MDIX.

Flow Control (Управление потоком)

Устройство поддерживает управление потоком 802.3x для портов, настроенных для полнодуплексного режима. По умолчанию эта функция отключена. Ее можно включить для каждого порта. Механизм управления потоком позволяет принимающей стороне посылать сигнал передающей стороне о том, что необходимо временно приостановить передача для предотвращения переполнения буфера.

Back Pressure (Обратное давление)

Устройство поддерживает «обратное давление» для портов, настроенных для работы в режиме полудуплекса. По умолчанию эта функция отключена. Ее можно включить для каждого порта. Механизм этой функции временно закрывает для передающего устройства передачу дополнительного трафика. Принимающее устройство может занимать линию связи и она становится недоступной для дополнительного трафика.

Настройки по умолчанию для коммутируемых портов

В следующей таблице содержится описание настроек по умолчанию для порта.

Таблица 4-1. Настройки порта по умолчанию

Функция	**Настройка по умолчанию**
Скорость и режим работы порта	Порт медного кабеля 10/100BaseT: автосогласование 100 Мбит/с полный дуплекс
	Порт медного кабеля 10/100/1000BaseT / SFP: автосогласование 1000 Мбит/с полный дуплекс
Состояние пересылки пакетов для порта	Enabled (Включено)
Маркировка портов	Без маркировки
Flow Control (Управление потоком)	Выкл (отключено на входе)
Back Pressure (Обратное давление)	Выкл (отключено на входе)

Назад на страницу "Содержание"

Назад на страницу Содержание

Использование Dell OpenManage Switch Administrator

Руководство пользователя систем Dell™ PowerConnect™ 35xx

- Запуск приложения
- Элементы интерфейса
- Использование кнопок программы Switch Administrator
- Настройки поля
- Доступ к устройству с помощью консоли
- Использование консоли

В этом разделе дается информация по работе с интерфейсом пользователя Dell OpenManage Switch Administrator

---

Запуск приложения

ПРИМЕЧАНИЕ. Перед запуском приложения необходимо определить IP-адрес. Более подробную информацию см. в разделе Первоначальные настройки.

1. Откройте веб-браузер.
2. Введите IP-адрес устройства в поле адреса и нажмите <Enter>.
3. При появлении окна **Log In** (Вход в систему) введите имя пользователя и пароль.

ПРИМЕЧАНИЕ. В паролях можно использовать буквы и цифры. При вводе учитывается состояние регистра.

4. Нажмите кнопку **OK**.

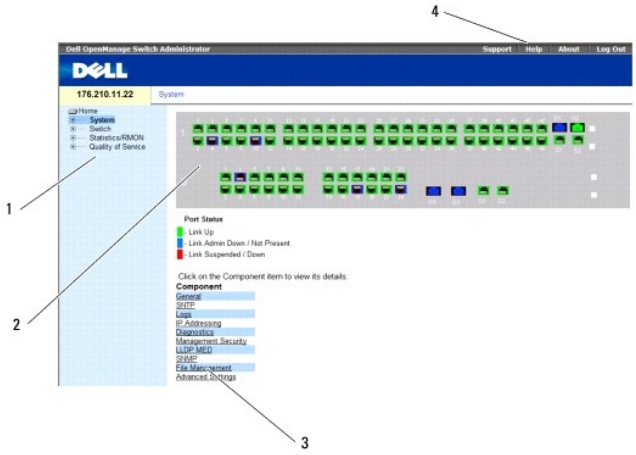
   Откроется главная страница приложения **Dell OpenManage™ Switch Administrator**.

Элементы интерфейса

Домашняя страница содержит следующие панели:

- **Tree view (Панель дерева).** Расположена в левой части главной страницы и отображает развернутый древовидный каталог функций и компонентов.
- **Device view (Панель устройства).** Расположена с правой стороны домашней страницы и отображает вид устройства, информационную или табличную область и инструкции по настройке.

Рис. 5-1. Компоненты программы Switch Administrator



В таблице 5-1 приведен список компонентов интерфейса с соответствующими номерами.

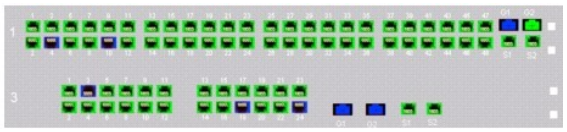
Табл. 5-1. Компоненты интерфейса

Компонент	Описание
1	Панель дерева содержит список различных параметров устройства. Ветви дерева можно раскрывать для просмотра всех компонентов параметра или сворачивать, скрывая эти компоненты. Чтобы расширить панель дерева для просмотра полного названия компонента, перетащите вертикальную полосу вправо.
2	На панели устройства приведены сведения о портах устройства, текущей настройке и состоянии устройства, табличная информация и компоненты параметров. В зависимости от выбранного параметра, в нижней области панели устройства отображается прочая информация об устройстве и диалоговые окна для настройки параметров.
3	В списке компонентов приведен список компонентов параметров. Компоненты также можно просмотреть, раскрыв параметр на панели дерева.
4	Информационные кнопки предоставляют доступ к сведениям об устройстве, а также доступ на веб-узел поддержки Dell. Дополнительную информацию см. в разделе Информационные кнопки.

Представление устройства

Главная страница содержит графическое изображение передней панели устройства.

Рис. 5-2. Индикаторы портов устройства PowerConnect



Цвет порта показывает, активен ли определенный порт в настоящий момент. Порты могут отображаться следующими цветами:

Таблица 5-2. Индикаторы портов и стековые индикаторы коммутатора PowerConnect

Компонент	Описание
Индикаторы портов	
Зеленый	Порт включен.
Красный	Произошла ошибка порта.
Синий	Порт отключен.
Красный	Устройство в настоящий момент не подключено к стеку.

ПРИМЕЧАНИЕ. Индикаторы портов не отражены на изображении передней панели коммутатора в приложении OpenManage Switch Administrator. Состояние индикаторов можно выяснить, только посмотрев на реальное устройство. Однако, стековые индикаторы отображают состояние портов. Более подробную информацию об индикаторах см. в разделе Описания индикаторов.

Использование кнопок программы Switch Administrator

В этом разделе описаны кнопки, которые находятся в интерфейсе OpenManage Switch Administrator. Кнопки интерфейсов делятся на следующие категории:

Информационные кнопки

Информационные кнопки обеспечивают доступ к онлайновой помощи и связи с центром технической поддержки, а также информацию об интерфейсах приложения OpenManage Switch Administrator.

Таблица 5-3. Информационные кнопки

Кнопка	Описание
Support	Открывает страницу службы поддержки Dell **support.dell.com**

(Поддержка)	
Help (Справка)	Онлайновая справка, которая содержит информацию по настройке и управлению устройством. Онлайновая справка делится на контекстные разделы. Так, например, если открыта страница справки **IP Addressing** (Система IP-адресов), то при нажатии кнопки **Help** (Справка), отобразятся тематические разделы этой страницы.
About (О компьютере)	Содержит номер версии и сборки, а также информацию об авторских правах Dell.
Log Out (Выход)	Открывает окно выхода.

Кнопки управления устройством

Кнопки управления устройством обеспечивают упрощенный доступ к информации по настройке устройства, а именно:

Таблица 5-4. Кнопки управления устройством

Кнопка	Описание
Apply Changes (Применить изменения)	Применяет заданные изменения для устройства.
Add (Добавить)	Добавляет информацию в таблицы или диалоговые окна.
Telnet	Запускает сеанс Telnet.
Query (Запрос)	Запрашивает таблицы.
Show All (Показать все)	Отображает таблицы устройств.
Стрелки влево/вправо	Перемещает информацию между списками.
Refresh (Обновить)	Обновляет информацию об устройстве.
Reset All Counters (Сбросить все счетчики)	Сбрасывает статистические счетчики.
Print (Печать)	Распечатывает страницу **Network Management System** (Система сетевого управления) и табличную информацию.
Draw (Нарисовать)	Быстро создает статистические диаграммы.
Details (Подробности)	Отображает более подробную информацию по теме текущей страницы.
Back (Назад)	Переход к предыдущей странице.

Настройки поля

Если иное не указано на веб-странице OpenManage Switch Administrator, пользовательские поля могут содержать от 1 до 159 символов. В полях могут использоваться все символы и буквы, кроме:

- \
- /
- :
- *
- ?
- <
- >
- |

Доступ к устройству с помощью команд консоли

Пользователь может управлять устройством, подключив напрямую терминал к порту терминала или через Telnet. В случае доступа через соединение Telnet, необходимо убедиться, что для устройства предварительно установлен IP-адрес, и что рабочая станция, используемая для доступа к устройству, подключена к нему до начала подачи команд CLI.

Дополнительную информацию по настройке первоначального IP-адреса см. в разделе Первоначальная настройка.

ПРИМЕЧАНИЕ. Перед использованием команд CLI для удаленного доступа убедитесь, что на устройство было загружено программное обеспечение.

Подключение терминала

1. Включите питание устройства и дождитесь завершения запуска.

2. Когда появится приглашение консоли Console>, введите команду enable и нажмите <Enter>.

3. Настройте устройство и введите необходимые команды для выполнения нужных задач.

4. После окончания введите команду выхода из режима Privileged EXEC.

   Сеанс будет закончен.

ПРИМЕЧАНИЕ. Если другой пользователь войдет в систему в привилегированном режиме команд Privileged EXEC, то текущий пользователь будет отключен от системы, а новый пользователь подключен в систему.

Подключение Telnet

Telnet - это протокол TCP/IP эмуляции терминала. Терминалы RS-232 могут виртуально подключаться к локальному устройству через сеть по протоколу TCP/IP. Telnet - это альтернатива терминалу с локальной регистрацией, в котором требуется удаленная регистрация.

Это устройство поддерживает до четырех одновременных сеансов управления по каналам Telnet. Во время сеанса Telnet можно использовать все команды консоли.

Чтобы запустить сеанс Telnet:

1. Нажмите **Start** (Пуск)→ **Run** (Запуск).

   Открывает диалоговое окно **Запуск** программы.

2. В окне **Запуск** программы введите *Telnet <IP address>* (Telnet <IP-адрес>) в поле **Открыть**.

3. Щелкните на кнопке OK.

   Начнется сеанс связи Telnet.

Использование консоли

В этом разделе содержится информация по использованию режима командной строки.

Обзор режима командной строки

Режим командной строки подразделяется на несколько командных режимов. Каждый из них имеет свой собственный набор команд. Ввод вопросительного знака в строке приглашения терминала отображает список команд, доступных в данном командном режиме.

В каждом режиме существует особая команда, позволяющая переключаться из одного командного режима в другой.

Во время инициализации сеанса командной строки (CLI) консоль находится в режиме User EXEC. В нем доступен только ограниченный набор команд. Этот уровень зарезервирован только для тех задач, которые не изменяют конфигурацию терминала и используются для доступа к конфигурационным подсистемам, таким как CLI. Для перехода на следующий уровень (Privileged EXEC) необходимо ввести пароль (если настроен).

Режим Privileged EXEC обеспечивает доступ к общей настройке устройств. Для специальной настройки внутри устройства необходимо перейти в режим следующего уровня, Global Configuration. Пароль для входа не требуется.

Режим Global Configuration управляет настройкой устройства на глобальном уровне.

Режим Interface Configuration настраивает устройство на уровне физического интерфейса. Команды интерфейса, требующие выполнения подкоманд, расположены на другом уровне - Subinterface Configuration Mode (Режим конфигурации субинтерфейса). Пароль для входа не требуется.

Режим User EXEC

После входа на устройство включается командный режим User EXEC. Приглашение на пользовательском уровне состоит из имени хоста, за которым следует символ угловой скобки (>). Например:

```
console>
```

ПРИМЕЧАНИЕ. Имя хоста по умолчанию - console, если оно не было изменено в ходе начальной настройки.

Команды пользователя EXEC позволяют подключаться к удаленным устройствам, временно изменять установки терминала, выполнять основные проверки и выводить списки системной информации.

Чтобы отобразить список команд режима User EXEC, введите в командной строке знак вопроса.

Режим Privileged EXEC

Привилегированный доступ можно защитить от несанкционированного доступа и обеспечить рабочие параметры. Пароли отображаются на экране. При вводе учитывается состояние регистра.

Для того, чтобы получить доступ и вывести список привилегированных команд режима Privileged EXEC:

1. В строке приглашения введите команду enable и нажмите <Enter>.
2. Когда появится запрос на ввод пароля, введите пароль и нажмите клавишу <Enter>.

   Приглашение режима Privileged EXEC состоит из имени хоста устройства, за которым следует символ решетки (#). Например:

   ```
   console#
   ```

   Для вывода списка команд режима Privileged EXEC введите знак вопроса в командной строке.

   Для возврата из режима Privileged EXEC в режим User EXEC, введите disable и нажмите <Enter>.

На следующем примере показан доступ к режиму Privileged EXEC и возврат в режим User EXEC:

```
console> enable

Enter Password (введите пароль): ******

console#

console# disable

console>
```

Для перехода в предыдущий режим используйте команду **exit**. Например, можно переключиться из режима Interface Configuration в режим Global Configuration или из режима Global Configuration в режим Privileged EXEC.

Режим Global Configuration

Команды режима Global Configuration применяются к системным функциям, а не к конкретному протоколу или интерфейсу.

Для доступа к режиму Global Configuration, в командной строке режима Privileged EXEC введите команду **configure** и нажмите <Enter>. Режим Global Configuration отображается в виде имени хоста устройства, оператором (config) и символом #.

```
console(config)#
```

Чтобы отобразить список команд режима Global Configuration, введите в командной строке знак вопроса.

Для возврата из режима Global Configuration в режим Privileged EXEC, введите команду **exit** или используйте комбинацию клавиш <Ctrl>+<Z>.

На следующем примере показан переход к режиму Global Configuration и возврат в режим Privileged EXEC:

```
console#

console# configure

console(config)# exit

console#
```

Для получения полного списка режимов CLI, обратитесь к Руководству по работе с интерфейсом командной строки (CLI) **коммутаторов Dell™ PowerConnect™3524/P и PowerConnect 3548/P**.

Назад на страницу Содержание

Назад на страницу Содержание

Информация о настройке системы

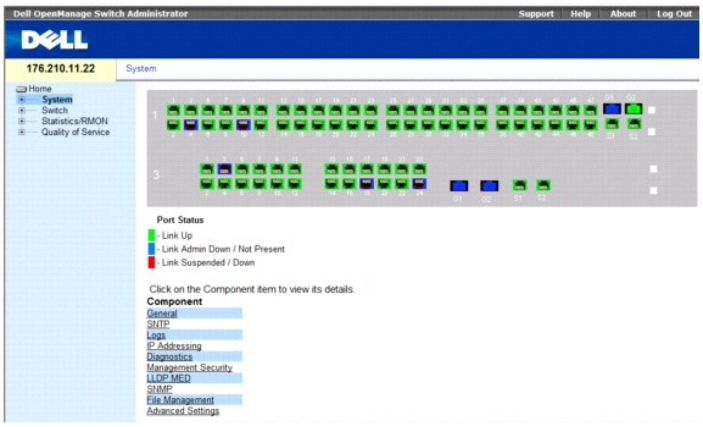
Руководство пользователя систем Dell™ PowerConnect™ 35xx

- Определение основных настроек коммутатора
- Настройка параметров SNTP
- Управление журналами
- Определение IP-адресации
- Запуск диагностики кабелей
- Управление безопасностью
- Настройка LLDP и MED
- Определение параметров SNMP
- Управление файлами
- Настройка расширенных установок

В настоящем разделе приводится информация по определению системных параметров, таких как параметры безопасности, загрузка программного обеспечения коммутатора и перезагрузка коммутатора. Для того, чтобы открыть страницу **System** (Система), нажмите на ссылку под строкой помощи для текущей страницы.

Нажмите **System** (Система) на панели дерева.

Рис. 6-1. Система



В этом разделе имеются следующие тематические подразделы:

- Определение основных настроек коммутатора
- Настройка параметров SNTP
- Управление журналами
- Определение IP-адресации
- Запуск диагностики кабелей
- Управление безопасностью
- Настройка LLDP и MED
- Определение параметров SNMP
- Управление файлами
- Настройка расширенных установок

Определение основных настроек коммутатора

На странице **General** (Главная) имеются ссылки на страницы, с помощью которых сетевые администраторы могут настраивать параметры коммутатора.

В настоящем разделе имеются следующие тематические подразделы:

- Просмотр информации о ресурсах коммутатора
- Asset (Ресурсы)
- Определение параметров системного времени
- Просмотр сведений о состоянии системы
- Управление питанием через Ethernet

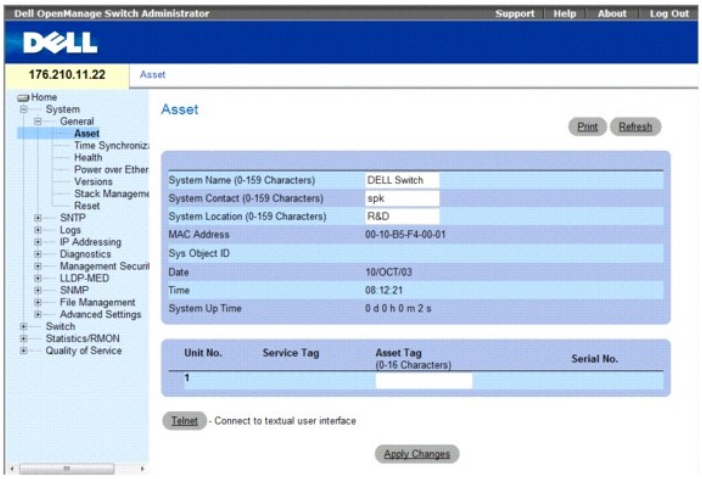
- Просмотр информации о версии ПО
- Управление устройствами стека
- Восстановление заводских параметров устройства

Просмотр информации о ресурсах коммутатора

Asset (Ресурсы)

Страница **Asset** (Ресурсы) содержит параметры, предназначенные для настройки и просмотра основной информации об устройстве, включая системное имя, местоположение, контактную информацию, системный MAC-адрес, идентификатор системного объекта, дата, время и время пребывания системы в рабочем состоянии. Чтобы открыть страницу **Asset** (Ресурсы), на панели дерева выберите **System** (Система)→ **General** (Общее) → **Asset** (Ресурсы).

Рис. 6-2. Ресурсы



Страница **Asset** (Ресурсы) содержит следующие поля.

- **System Name** (Имя системы) (0-159 символов). Определенное пользователем имя устройства.
- **System Contact** (Контактное лицо) (0-159 символов). Имя контактного лица.
- **System Location** (Местоположение системы) (0-159 символов). Место установки и работы системы.
- **MAC Address** (MAC-адрес). MAC-адрес устройства.
- **Sys Object ID** (Объектный идентификатор системы). Определяет утвержденный поставщиком идентификатор подсистемы сетевого управления, содержащийся в системе.
- **Date** (Дата). Текущая дата. Дата указывается в формате день/месяц/год, например 15/FEB/07 - 15 февраля 2007 г.
- **Time** (Время). Указывает текущее время. Формат времени - часы:минуты:секунды, например, 20:12:21 - восемь часов 12 минут 21 секунда пополудни.
- **System Up Time** (Время включения системы). показывает, сколько времени прошло с момента последней перезагрузки системы. Формат отображения системного времени: дни, часы, минуты и секунды. Например, 41 день 2 часа 22 минуты 15 секунд.
- **Unit No.** (Номер устройства). Указывает номер устройства, для которого отображается информация о ресурсах.
- **Service Tag** (Метка производителя). Справочный номер, используемый при обслуживании устройства.
- **Asset Ta**g (Дескриптор ресурса) (0-16 символов). Отображает определенный пользователем справочный номер устройства.
- **Serial No.** (Серийный номер). Серийный номер устройства.

Определение сведений о системе

1. Откройте страницу **Asset** (Ресурсы).
2. Определите соответствующие поля.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Системные параметры будут определены, а устройство обновлено.

Запуск сеанса Telnet

1. Откройте страницу **Asset** (Ресурсы).
2. Нажмите **Telnet**.

   Будет запущен сеанс Telnet.

Настройка информации об устройстве с помощью команд интерфейса командной строки (CLI)

В следующей таблице приведены команды консоли для просмотра и настройки полей, отображаемых на странице **Asset** (Ресурсы).

Команда консоли	**Описание**
hostname *имя*	Указывает или изменяет имя хоста устройства.
snmp-server contact *текст*	Задает контактные сведения для системы.
snmp-server location *текст*	Вводит сведения о местонахождении устройства.
clock set *чч*:*мм*:*сс день месяц год*	Ввод системного времени и даты вручную.
show clock [detail]	Отображает системное время и дату.
show system id (системный идентификатор)	Выводит информацию метки производителя.
show system (система)	Отображает информацию о системе.
asset-tag *текст*	Определяет дескриптор ресурса для устройства.
show stack <1-8> (стек)	Отображает информацию о системном стеке.
show system [устройство *устройство***]**	Отображает информацию о системе.
show system id [устройство *устройство*]	Отображает идентификатор системы.

Ниже показан пример определения имени хоста устройства, контактов и расположения системы, а также установки системного времени и даты с помощью команд консоли:

```
console(config)# hostname dell(config)# dell

dell (config)# snmp-server contact Dell_Tech_Supp

dell (config)# snmp-server location New_York

dell (config)# exit

Console(config)# snmp-server host 10.1.1.1 management 2

Console# clock set 13:32:00 7 Mar 2002

Console# show clock

15:29:03 Jun 17 2002
```

Ниже приведен пример отображения системной информации для автономного устройства с помощью команд консоли:

console# **show system id**	
Service tag (Метка производителя):	
Serial number (Серийный номер): 51	
Asset tag (Дескриптор ресурса):	
console# **show system**	
System Description (Описание системы):	Ethernet Switch (Коммутатор Ethernet)
System Up Time (days,hour:min:sec) (Время включения системы, дней,ч:мин:с):	0,00:00:57
System Contact (Контактное лицо):	
System Name (Имя системы):	Коммутатор PowerConnect-1
System Location (Местонахождение системы):	
System MAC Address (MAC-адрес системы):	00:00:00:08:12:51
System Object ID (Объектный идентификатор):	1.3.6.1.4.1.674.10895.3006

Type (Тип):	Коммутатор PowerConnect 3524
Main Power Supply Status (Состояние основного источника питания):	OK
Fan 1 Status (Состояние вентилятора 1):	NOT OPERATIONAL (НЕ РАБОТАЕТ)
Fan 2 Status (Состояние вентилятора 2):	NOT OPERATIONAL (НЕ РАБОТАЕТ)
Temperature (Celsius) (Температура, град. Цельсия):	30
Temperature Sensor Status (Состояние температурного датчика):	OK

Ниже показан пример отображения системной информации для устройств стека с помощью команд консоли:

console# **show system id**					
Unit (Устройство)	Serial number (Серийный номер)		Asset tag (Дескриптор ресурса)	Service tag (Метка производителя)	
----	----------		---------	----------	
1	893658972		mkt-1	89788978	
2	893658973		mkt-2	89788979	
3	893658974		mkt-3	89788980	
4	893658975		mkt-4	89788981	
5	893658976		mkt-5	89788982	
6	893658977		mkt-6	89788983	
7	893658978		mkt-7	89788984	
8	893658979		mkt-8	89788985	
console# **show system**					
Unit (Устройство)	Type (Тип)				
----	----------				
1	Коммутатор PowerConnect 3524				
2	Коммутатор PowerConnect 3524				
3	Коммутатор PowerConnect 3524				
4	Коммутатор PowerConnect 3524P				
5	Коммутатор PowerConnect 3524P				
6	Коммутатор PowerConnect 3524P				
7	Коммутатор PowerConnect 3524P				
8	Коммутатор PowerConnect 3524P				
Unit (Устройство)	Main Power Supply (Основной источник питания)		Redundant Power Supply (Резервный источник питания)		
----	----------		----------		
1	OK				
2	OK				
3	OK				
4	OK				
5	OK		OK		
6	OK		OK		
7	OK		OK		
8	OK		OK		
Unit (Устройство)	Fan1 (Вентилятор 1)	Fan2 (Вентилятор 2)	Fan3 (Вентилятор 3)	Fan4 (Вентилятор 4)	Fan5 (Вентилятор 5)
----	----	----	----	----	----

1	OK	OK			
2	OK	OK			
3	OK	OK			
4	OK	OK			
5	OK	OK	OK	OK	OK
6	OK	OK	OK	OK	OK
7	OK	OK	OK	OK	OK
8	OK	OK	OK	OK	OK
Unit (Устройство)	Temperature (Celsius) (Температура, град. Цельсия)		Temperature Sensor Status (Состояние температурного датчика)		
----	----------		----------		
1	30		OK		
2	30		OK		
3	30		OK		
4	30		OK		
5	30		OK		
6	30		OK		
7	30		OK		
8	30		OK		

Определение параметров системного времени

Страница **Time Synchronization** (Синхронизация по времени) содержит поля для определения параметров системного времени для часов локального оборудования и внешних часов SNTP. Если поддержка системного времени осуществляется при помощи внешнего синхрогенератора SNTP, и внешний генератор SNTP выйдет из строя, то система будет переключена на часы локального оборудования. На устройстве можно включить переход на летнее время. Следующий список содержит начало и конец периода летнего времени для определенных стран:

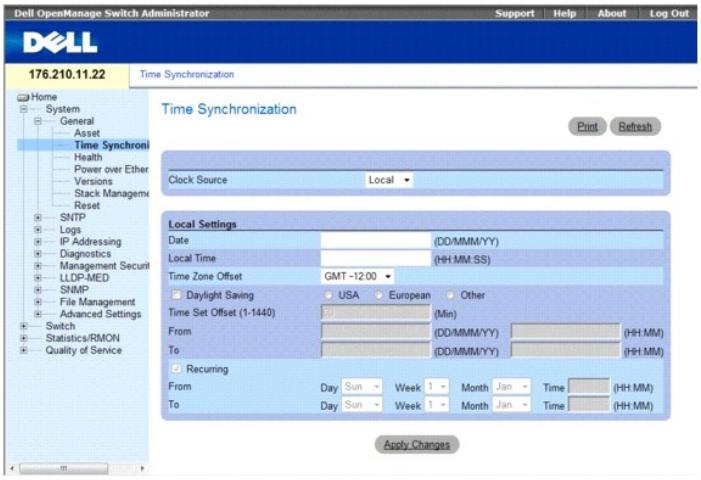
- **Албания** - с последних выходных марта по последние выходные октября.
- **Австралия** - с конца октября по конец марта.
- **Австралия** - **Тасмания** - с начала октября по конец марта.
- **Армения** - с последних выходных марта по последние выходные октября.
- **Австрия** - с последних выходных марта по последние выходные октября.
- **Багамские о-ва** - с апреля по октябрь, в сочетании с часами летнего времени США.
- **Белоруссия** - с последних выходных марта по последние выходные октября.
- **Бельгия** - с последних выходных марта по последние выходные октября.
- **Бразилия** - с 3-го воскресенья октября по 3-е воскресенье марта. В течение периода перехода на летнее время часы в Бразилии переводятся на один час вперед в большинстве областей юго-востока Бразилии.
- **Чили** - о. Пасхи с 9-го марта по 12-е октября. Первое воскресенье марта или после 9-го марта.
- **Китай** - Китай не переходит на летнее время.
- **Канада** - с первого воскресенья апреля по последнее воскресенье октября. Управление переходом на летнее время обычно осуществляется правительствами провинций и территорий. В некоторых городах переход на летнее время не выполняется.
- **Куба** - с последнего воскресенья марта по последнее воскресенье октября.
- **Кипр** - с последних выходных марта по последние выходные октября.
- **Дания** - с последних выходных марта по последние выходные октября.
- **Египет** - с последней пятницы апреля по последний четверг сентября.
- **Эстония** - с последних выходных марта по последние выходные октября.
- **Финляндия** - с последних выходных марта по последние выходные октября.
- **Франция** - с последних выходных марта по последние выходные октября.
- **Германия** - с последних выходных марта до последних выходных октября.
- **Греция** - с последних выходных марта по последние выходные октября.
- **Венгрия** - с последних выходных марта по последние выходные октября.
- **Индия** - Индия не переходит на летнее время.
- **Иран** - с 21-го марта по 23-е сентября.
- **Ирак** - с 1-го апреля по 1-е октября.
- **Ирландия** - с последних выходных марта по последние выходные октября.

- **Израиль** - в разные годы по-разному.
- **Италия** - с последних выходных марта по последние выходные октября.
- **Япония** - Япония не переходит на летнее время.
- **Иордания** - с последних выходных марта по последние выходные октября.
- **Латвия** - с последних выходных марта по последние выходные октября.
- **Ливан** - с последнего воскресенья марта по последнее воскресенье октября.
- **Литва** - с последних выходных марта по последние выходные октября.
- **Люксембург** - с последних выходных марта по последние выходные октября.
- **Македония** - с последних выходных марта по последние выходные октября.
- **Мексика** - с первого воскресенья апреля в 02:00 по последнее воскресенье октября в 02:00.
- **Молдавия** - с последних выходных марта по последние выходные октября.
- **Черногория** - с последних выходных марта по последние выходные октября.
- **Нидерланды** - с последних выходных марта по последние выходные октября.
- **Новая Зеландия** - с первого воскресенья октября по первое воскресенье 15-го марта или после этой даты.
- **Норвегия** - с последних выходных марта по последние выходные октября.
- **Парагвай** - с 6-го апреля по 7-е сентября.
- **Польша** - с последних выходных марта по последние выходные октября.
- **Португалия** - с последних выходных марта по последние выходные октября.
- **Румыния** - с последних выходных марта по последние выходные октября.
- **Россия** - с 29-го марта по 25-е октября.
- **Сербия** - с последних выходных марта по последние выходные октября.
- **Словацкая республика** - с последних выходных марта по последние выходные октября.
- **ЮАР** - ЮАР не переходит на летнее время.
- **Испания** - с последних выходных марта по последние выходные октября.
- **Швеция** - с последних выходных марта по последние выходные октября.
- **Швейцария** - с последних выходных марта по последние выходные октября.
- **Сирия** - с 31-го марта по 30-е октября.
- **Тайвань** - Тайвань не переходит на летнее время.
- **Турция** - с последних выходных марта по последние выходные октября.
- **Великобритания** - с последних выходных марта по последние выходные октября.
- **США** - со второго воскресенья марта в 02:00 по первое воскресенье ноября в 02:00.

Более подробная информация по SNTP дана в разделе Настройка параметров SNTP.

Чтобы открыть страницу **Time Synchronization** (Синхронизация по времени), на панели дерева выберите **System** (Система)→ **General** (Общие)→ **Time Synchronization** (Синхронизация по времени).

Рис. 6-3. Синхронизация по времени



Страница Time Synchronization (Синхронизация по времени) содержит следующие поля.

- **Clock Source** (Источник синхронизации). источник, используемый для установки системных часов. Возможные значения поля:
  - **Local**. Указывает, что системное время не было установлено по внешнему источнику.
  - **SNTP**. определяет, что системное время будет установлено через сервер SNTP. Дополнительную информацию см. в разделе Configuring SNTP Settings (Настройка параметров SNTP).

Local Settings (Локальные настройки)

- **Date** (Дата). определяет системную дату. Формат поля - ДД/МММ/ГГ, например, 04/Май/07.
- **Local Time** (Локальное время). определяет системное время. Формат поля ЧЧ:ММ:СС, например, 21:15:03.
- **Time Zone Offset** (Смещение часового пояса). разница между временем по Гринвичу (GMT) и местным временем. Например, разница времени для Парижа составляет GMT +1:00, в для Нью-Йорка GMT –5:00.

Существуют два типа параметров перехода на летнее время: в определенный день в определенный год или в один день каждый год. Чтобы определить параметр перехода в определенный год, укажите значение в области **Daylight Savings** (Переход на летнее время). Чтобы настроить ежегодный переход, введите значение в области **Recurring** (Повторяющийся).

- **Daylight Savings** (Переход на летнее время). Позволяет выполнять переход на летнее время (DST) для устройства, установленного в определенной местности. Возможные значения:
  - **USA** (США). устройство переключается на летнее время в 2 часа ночи во второе воскресенье марта, а на стандартное время - в 2 часа ночи в первое воскресенье ноября.
  - **European** (Европа). устройство переключается на летнее время в час ночи в последнее воскресенье марта, а на стандартное время в час ночи в последнее воскресенье октября. Параметр *European* (Европейское) применяется для членов Европейского союза и других стран Европы, использующих стандарты Европейского союза.
  - **Other** (Другое). переход на летнее время определяется пользователем на основе местоположения устройства. Если выбран параметр Other (Другое), то должны быть определены поля **From** (С) и **To** (По).
- **Time Set Offset** (Смещение времени) (1-1440). разница в минутах между летним и стандартным местным временем. Время по умолчанию - 60 минут.
- **From** (С). определяет время перехода на летнее время для всех стран, кроме США и стран Европы. Формат: ДеньМесяцГод в одном поле и время в другом поле. Например, если переход на летнее время должен быть выполнен 25 октября 2007 года в 5:00 утра, в поля необходимо ввести следующие значения: 25Oct07 и 5:00. Возможные значения:
  - **DD/MMM/YY** (ДД/МММ/ГГ). дата (день, месяц и год), с которой началось летнее время.
  - **HH/MM** (ЧЧ/ММ). время (часы и минуты) начала летнего времени. Формат поля ЧЧ/ММ, например, 05:30.
- **To** (По). определяет окончание действия летнего времени для стран отличных от США и Европы. Формат: ДеньМесяцГод в одном поле и время в другом поле. Например, если действие летнего времени должно закончится 23 марта 2008 года в 12:00, в поля необходимо ввести следующие значения: 23Mar08 и 12:00. Возможные значения:
  - **DD/MMM/YY** (ДД/МММ/ГГ). дата (день, месяц и год), окончания летнего времени.
  - **HH/MM** (ЧЧ/ММ). время (часы и минуты) окончания летнего времени. Формат поля ЧЧ/ММ, например, 05:30.
- **Recurring** (Повторение). определяет время перехода на летнее время для всех стран, кроме США и стран Европы, в которых переход на летнее время повторяется каждый год. Возможные значения:
- **From** (С). определяет время перехода на летнее время каждый год. Например, переход на летнее время выполняется во вторую субботу апреля в 5:00. Возможные значения:
  - **Day** (День). день недели, в который каждый год выполняется переход на летнее время. Возможные значения поля: Sunday-Saturday (воскресенье-суббота).
  - **Week** (Неделя). неделя месяца, в течение которой каждый год выполняется переход на летнее время. Возможные значения поля: 1-5.
  - **Month** (Месяц). месяц года, в течение которого каждый год осуществляется переход на летнее время. Возможные значения поля: Jan-Dec (янв-дек).

- **Time** (Время). время, когда каждый год осуществляется переход на летнее время. Формат поля часы:минуты, например, 02:10.

- **To** (По). определяет окончание действия летнего времени каждый год. Например, действие летнего времени каждый год заканчивается в четвертую пятницу октября в 5:00 утра. Возможные значения:
  - **Day** (День). день недели, в который каждый год заканчивается действие летнего времени. Возможные значения поля: Sunday-Saturday (воскресенье-суббота).
  - **Week** (Неделя). неделя месяца, в течение которой каждый год заканчивается действие летнего времени. Возможные значения поля: 1-5.
  - **Month** (Месяц). месяц, с которого каждый год заканчивается действие летнего времени. Возможные значения поля: Jan-Dec (янв-дек).
  - **Time** (Время). время, когда каждый год заканчивается действие летнего времени. Формат поля часы:минуты, например, 05:30.

Выбор источника синхронизации

1. Откройте страницу **Time Synchronization** (Синхронизация по времени).
2. Укажите значение поля **Clock Source** (Источник синхронизации).
3. Нажмите кнопку **Apply Changes** (Применить изменения).

   Будет выбран источник синхронизации, а устройство обновлено.

Определение параметров локальных часов

1. Откройте страницу **Time Synchronization** (Синхронизация по времени).
2. Определите поля.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

   Будут использоваться локальные часы.

Определение параметров часов с помощью команд консоли

В следующей таблице приведены команды консоли для настройки полей, отображаемых на странице **Time Synchronization** (Синхронизация по времени).

Перед установкой перехода на летнее время необходимо выполнить следующие действия.

1. Настройте переход на летнее время.
2. Определите часовой пояс.
3. Установите часы.

   Например:

```
console(config)# clock summer-time recurring usa
console(config)# clock timezone 2 zone TMZ2
console(config)# clock set 10:00:00 apr 15 2004
```

Таблица 6-2. Команды консоли для определения параметров часов

Консоль	**Описание**
clock source sntp	Определяет внешний источник времени для системных часов.
clock time zone *hours-offset* [**minutes** *minutes-offset*][**zone** *acronym*]	Устанавливает часовой пояс для отображения.
clock summer-time	Настраивает в системе автоматическое переключение на летнее время.
clock summer-time recurring {**usa** | **eu** | *week day month hh:mm week day month hh:mm}* [**offset** *offset*] [**zone** *acronym*]	Настраивает систему на автоматическое переключение на летнее время (в соответствии со стандартами США и Европы).
clock summer-time date *date month year hh:mm date month year hh:mm* [**offset** *offset*] [**zone** *acronym*]	Настраивает систему для автоматического переключения на летнее время для указанного периода в формате день/месяц/год.

Далее приведен пример команд консоли.

```
console(config)# clock timezone -6 zone CST
```

```
console(config)# clock summer-time recurring first sun apr 2:00 last sun
oct 2:00

console(config)# clock source sntp

console(config)# interface ethernet e14

console(config-if)# sntp client enable

console(config-if)# exit

console(config)# sntp broadcast client enable
```

Просмотр сведений о состоянии системы

Страница ***System Health*** (Состояние системы) отображает физическую информацию об устройстве, в т.ч. о состоянии источников питания и вентиляционной системы. Чтобы открыть страницу ***System Health*** (Состояние системы), на панели дерева выберите **System** (Система)→ **General** (Общее)→ **Health** (Состояние).

Рис. 6-4. Состояние системы

Страница ***System Health*** (Состояние системы) содержит следующие поля:

- **Unit No.** (Номер устройства). номер устройства, для которого отображается состояние системы.
- **Power Supply Status** (Состояние источников питания). устройство имеет два источника питания. Возможные значения:
  - Флажок установлен — источник питания работает нормально.
  - Флажок снят — неполадки источника питания.
  - **Not Present** (Отсутствует) — источник питания не установлен.
- **Fan Status** (Состояние вентилятора). коммутаторы, не предназначенные для питания через Ethernet, имеют два встроенных вентилятора, а PoE-модели - пять вентиляторов. Каждый вентилятор на интерфейсе обозначается значком вентилятора с номером. Возможные значения:
  - Флажок установлен — Вентилятор работает нормально.
  - Флажок снят — Неполадки вентилятора
  - **Not Present** (Отсутствует) — вентилятор не установлен.
- **Temperature** (Температура). текущая температура работающего устройства. Температура отображается по шкале Цельсия. Нормальный рабочий диапазон температур для устройства составляет 0-40 C (32-104 F). В следующей таблице показана таблица соответствия температурных шкал Фаренгейта и Цельсия с дискретностью 5 градусов.

Таблица 6-3. Шкала перевода градусов Цельсия в градусы Фаренгейта

Градусы Цельсия.	Градусы Фаренгейта.
0	32
5	41
10	50
15	59
20	68
25	77
30	86
35	95
40	104

Просмотр сведений о состоянии системы с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для просмотра полей, отображаемых на странице ***System Health*** (Состояние системы).

Команда консоли	**Описание**
show system [**unit** *устройство*]	Отображает информацию о системе.

Ниже приведен пример команды консоли для вывода информации о состоянии системы.

console#	**show system (система)**			
Unit (Устройство)	**Type (Тип)**			
1	Коммутатор PowerConnect 3524			
Unit (Устройство)	**Main Power Supply (Основной источник питания)**	**Redundant Power Supply (Резервный источник питания)**		
1	OK			
Fan1 (Вентилятор 1)	**Fan2 (Вентилятор 2)**	**Fan3 (Вентилятор 3)**	**Fan4 (Вентилятор 4)**	**Fan5 (Вентилятор 5)**
1	OK	OK	OK	OK
Unit (Устройство)	**Temperature (Celsius) (Температура, град. Цельсия)**	**Temperature Sensor Status (Состояние температурного датчика)**		
1	27	OK		
Unit (Устройство)	**Up time (Время включения)**			
1	00,09:30:36			

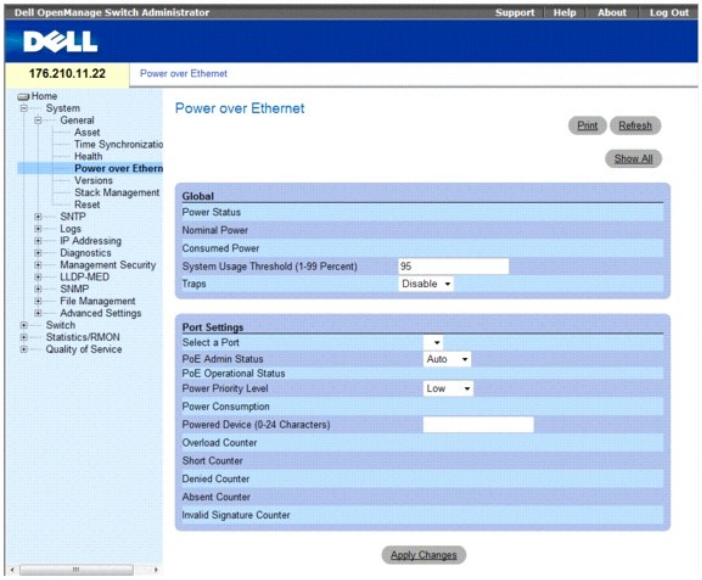
Управление питанием через Ethernet

Функция питания через сеть Ethernet (PoE) обеспечивает подключение устройств к источникам питания по существующим кабелям локальной без необходимости видоизменения или наращивания инфраструктуры сети. Это устраняет необходимость устанавливать устройства вблизи источников питания.

Потребителями называются устройства, которые получают питание от источников питания устройств PowerConnect (например, IP-телефоны). Потребители подключаются к устройству PowerConnect через порты Ethernet. Потребители подключаются либо через все 24 порта FE коммутатора PowerConnect 3524P или через все 48 FE портов коммутатора PowerConnect 3548P.

Чтобы открыть страницу **Power Over Ethernet** (Питание через Ethernet), выберите **System** (Система)→ **General** (Общее)→ **Power over Ethernet** (Питание через Ethernet) на панели дерева.

Рис. 6-5. Питание через Ethernet



На странице **Power Over Ethernet** (Питание через Ethernet) имеются следующие разделы:

- Global (Глобальные параметры)
- Port settings (Параметры порта)

Global

Глобальные параметры питания через Ethernet имеют следующие поля:

- **Power Status** (Состояние источника питания). показывает состояние источника питания, находящегося в сети.
  - **On** (Включен). источник питания работает.
  - **Off** (Выключен). источник питания не работает.
  - **Faulty** (Неисправность). обнаружена неполадка при работе источника питания. Пример неисправности - перегрузка или короткое замыкание.
- **Nominal Power** (Номинальная мощность). реальная электрическая мощность, которую может выдавать источник питания. Величина в поле отображается в ваттах.
- **Consumed Power** (Потребляемая мощность). мощность, потребляемая устройством. Величина в поле отображается в ваттах.
- **System Usage Threshold** (Порог использования ресурса системы) (1-99 %). указывает величину потребленного ресурса мощности в процентах до срабатывания сигнала тревоги. Величина в поле указывается в процентах от 1 до 99. Значение по умолчанию - 95%.
- **Traps** (Прерывания). включает или выключает получение сигналов прерывания от устройств PoE.
  - **Enable** (Включить). включает получение сигналов прерывания.
  - **Disable** (Выключить). выключает получение сигналов прерывания. Это значение по умолчанию.

Параметры порта

- **Select a Port** (Выбрать порт). указывает специфический интерфейс, для которого определяются и назначаются параметры PoE для запитанных интерфейсов, подключенных к выбранному порту.
- **PoE Admin Status** (Состояние администрирования PoE). указывает режим PoE. Возможные значения:
  - **Auto** (Автоматический). включает протокол обнаружения устройства и подает питание на устройство, используя модуль PoE. Протокол обнаружения устройства позволяет обнаруживать потребители, подключенные к интерфейсам устройства и определять их классификацию. Это значение установлено по умолчанию.
  - **Never** (Никогда). Отключает протокол обнаружения устройств и прекращает подачу энергии на устройство через модуль PoE.
- **PoE Operational Status** (Состояние работы PoE). указывает, задействован ли порт для работы в режиме PoE. Возможные значения:
  - **Disabled** (Отключен).
  - **Searching** (Поиск). в данный момент устройство PowerConnect осуществляет поиск потребителей. Это состояние является рабочим состоянием по умолчанию.
  - **Delevering Power** (Подача питания). устройство PowerConnect в настоящее время подает питание потребителям.
  - **Fault** (Неисправность). коммутатор PowerConnect обнаружил неисправность устройства-потребителя. Например, не удается произвести чтение памяти устройства - потребителя.

- **Test** (Тест). происходит тестовая проверка устройства-потребителя. Например, устройство-потребитель нуждается в проведении тестовой проверки для подтверждения того, что оно запитано от источника питания.
- **Other Fault** (Прочие неисправности).
- **Unknown** (Не определены).

- **Power Priority Level** (Уровень приоритета питания). определяет приоритет, в соответствии с которым питание подается на порты, в случае нехватки мощности. Приоритет подачи питания на порты используется в случае нехватки мощности. Значение поля по умолчанию - низкий приоритет. Например, если источник питания работает на пределе мощности (99%), и порт 1 имеет высокий приоритет, а порт 3 имеет низкий приоритет, питание будет в первую очередь подаваться на порт 1, а питание порта 3 может быть отключено.
  - **Critical** (Критический). определяет высший уровень приоритета.
  - **High** (Высокий). определяет второй по значимости уровень приоритета.
  - **Low** (Низкий). Самый низкий уровень приоритета.
- **Power Classification** (Классификация питания). классификация потребителей по следующему принципу:
  - **Класс 0: 0,44 – 12,95** — уровень энергопотребления порта в пределах от 0,44 до 12,95 Вт.
  - **Класс 1: 0,44 – 3,8** — уровень энергопотребления порта в пределах от 0,44 до 3,8 Вт.
  - **Класс 2: 3,84 – 6,49** — уровень энергопотребления порта в пределах от 3,84 до 6,49 Вт.
  - **Класс 3: 6,49 – 12,95** — уровень энергопотребления порта в пределах от 6,49 до 12,95 Вт.
- **Powered Device** (Потребитель) (0-24 символа). указывает установленное пользователем описание устройства-потребителя. Это поле может содержать до 24 символов.
- **Overload Counter** (Счетчик перегрузки). указывает количество случаев перегрузки источника питания.
- **Short Counter** (Счетчик коротких замыканий). указывает количество случаев короткого замыкания источника питания.
- **Denied Counter** (Счетчик отказов). указывает количество случаев, когда устройству было отказано в подаче энергии.
- **Absent Counter** (Счетчик отключений). указывает количество случаев, при которых подача питания на устройство-потребитель было приостановлено в связи с тем, что его не удалось обнаружить.
- **Invalid Signature Counter** (Счетчик недействительной подписи). указывает количество случаев, при которых была получена недействительная подпись. Подписью называется идентификатор устройства сети питания. Подписи генерируются в процессе обнаружения потребителей, их классификации или технического обслуживания.

Определение установок PoE

1. Откройте страницу **Power Over Ethernet** (Питание через Ethernet).
2. Определите поля.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

   Установки питания через Ethernet будут изменены, и произойдет обновление устройства.

Отображение установок PoE для всех портов

1. Откройте страницу **Power Over Ethernet** (Питание через Ethernet).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется таблица **Power Over Ethernet** (Питание через Ethernet).

Рис. 6-6. Таблица «Питание через Ethernet»

Управление питанием через Ethernet с помощью команд консоли

В таблице (см. ниже) показаны эквивалентные команды консоли, предназначенные для просмотра полей страницы **Power Over Ethernet** (Питание через Ethernet).

Команда консоли	Описание
power inline {*auto* | *never*}	Настраивает режим администрирования питания интерфейса.
power inline powered-device *pd-type*	Устанавливает описание типа устройства-потребителя.
power inline priority {critical | high | low}	Устанавливает приоритет интерфейса для подачи питания от линейного источника.
power inline usage-threshold	Устанавливает порог мощности до срабатывания сигнала тревоги.
power inline traps enable	Включает подачу сигналов прерывания PoE устройства.
show power inline [*интерфейс ethernet*]	Отображает информацию о конфигурации режима PoE.

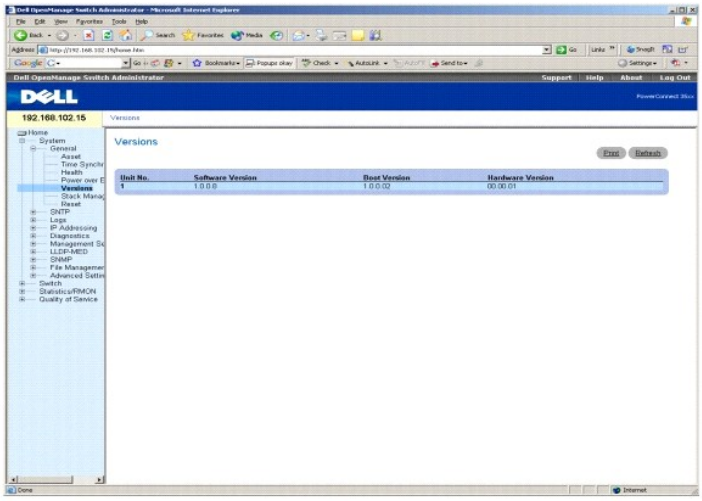
Ниже приведены примеры команд консоли для режима питания через Ethernet (PoE).

Console> enable (включить)					
Console# show power inline					
Unit (Устройство)	Power (Электропитание)	Nominal Power (Номинальная мощность)	Consumed Power (Потребляемая мощность)	Usage (Процент использования)	Threshold (Порог)
1	On (Вкл.)	370 Вт	0 Вт (0%)	95	Disable (Отключение)
2	Off (Выкл.)	1 Вт	0 Вт (0%)	95	Disable (Отключение)
3	Off (Выкл.)	1 Вт	0 Вт (0%)	95	Disable (Отключение)
4	Off (Выкл.)	1 Вт	0 Вт (0%)	95	Disable (Отключение)
5	Off (Выкл.)	1 Вт	0 Вт (0%)	95	Disable (Отключение)
6	Off (Выкл.)	1 Вт	0 Вт (0%)	95	Disable (Отключение)
7	Off (Выкл.)	1 Вт	0 Вт (0%)	95	Disable (Отключение)
8	Off (Выкл.)	1 Вт	0 Вт (0%)	95	Disable (Отключение)
Port (Порт)	Powered Device (Устройство-потребитель)	State (Состояние)	Status (Статус)	Priority (Приоритет)	Class (Класс)
1/e1		Auto (Авто)	Searching (Поиск)	low (низкий)	class0 (класс 0)
1/e2		Auto (Авто)	Searching (Поиск)	low (низкий)	class0 (класс 0)
1/e3		Auto (Авто)	Searching (Поиск)	low (низкий)	class0 (класс 0)
1/e4		Auto (Авто)	Searching (Поиск)	low (низкий)	class0 (класс 0)
1/e5		Auto (Авто)	Searching (Поиск)	low (низкий)	class0 (класс 0)
1/e6		Auto (Авто)	Searching (Поиск)	low (низкий)	class0 (класс 0)

Просмотр информации о версии

Страница **Versions** (Версии) содержит сведения об используемых устройствах и версиях программного обеспечения. Чтобы открыть страницу **Versions** (Версии), на панели дерева выберите **System** (Система)→ **General** (Общее)→ **Versions** (Версии).

Рис. 6-7. Версии



Страница **Versions** (Версии) содержит следующие поля.

- **Unit No.** (Номер устройства). указывает номер устройства, для которого отображается версия устройства.
- **Software Version** (Версия программы). текущая версия программного обеспечения, запущенного на устройстве.
- **Boot Version** (Версия загрузчика). текущая версия загрузчика, используемого на устройстве.
- **Hardware Version** (Версия аппаратного обеспечения). текущая версия аппаратного обеспечения устройства.

Отображение версий устройств с помощью команд консоли

В следующей таблице приведены команды консоли для просмотра полей, отображаемых на странице **Versions** (Версии).

Таблица 6-6. Команды консоли для отображения версий

Команда консоли	Описание
show version	Отображает сведения о версии системы.

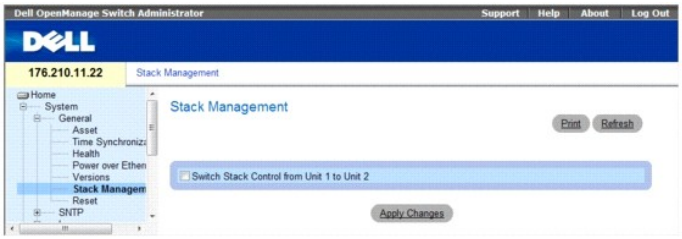
Далее приведен пример команд консоли.

```
console> show version

Unit SW version Boot version HW version

------------------- ------------------- ------------------- ----- 1
1.0.0.8 1.0.0.02 00.00.01
```

Управление устройствами стека

Страница **Stack Management** (Управление стеком) позволяет сетевому администратору переключать управление стеком с устройства 1 на устройства 2 и наоборот. Чтобы открыть страницу **Stack Management** (Управление стеком), нажмите **System** (Система)→ **General** (Общее)→ **Stack Management** (Управление стеком) на панели дерева.

Рис. 6-8. Управление стеком



- **Switch Stack Control from Unit 1 to Unit 2** (Переключение управления стеком с устройства 1 на устройство 2). переключает управление стеком с главного устройства стека на резервное.

Переключение между привилегированными устройствами стека

1. Откройте страницу **Stack Management** (Управление стеком).
2. Установите флажок в окне **Switch Stack Control from Unit 1 to Unit 2** (Переключение управления стеком с устройства 1 на устройство 2).
3. Нажмите кнопку **Apply Changes** (Применить изменения).

   Появится сообщение подтверждения.
4. Нажмите кнопку **OK**.

   Будут восстановлены заводские настройки устройства. После этого появится окно, в котором пользователь должен ввести имя пользователя и пароль.

Управление стеками с помощью команд консоли

В приведенной ниже таблице приведены эквивалентные команды для просмотра полей, отображаемых на странице **Stack Management** (Управление стеком).

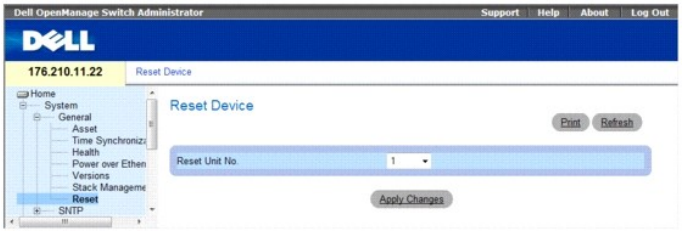
Таблица 6-7. Команды консоли для управления стеком

Команда консоли	Описание
stack reload	Производит перезагрузку устройств стека.
stack master	Осуществляет принудительный выбор главного устройства стека.

Восстановление заводских параметров устройства

Страница **Reset** (Сброс) позволяет удаленно произвести сброс установок устройства. Сохранить все изменения в файле настроек перед перезагрузкой устройства. Это позволит сохранить текущую конфигурацию устройства. Подробная информация по сохранению конфигурационных файлов дана в разделе Копирование файлов. Чтобы открыть страницу **Reset** (Сброс), на панели дерева выберите **System** (Система)→ **General** (Общее)→ **Reset** (Сброс).

Рис. 6-9. Сброс



Страница **Reset** (Сброс) содержит следующее поле:

Reset Unit No. (Номер устройства для сброса). Ввод номера устройства стека, подлежащего сбросу установок.

Восстановление заводских параметров устройства

1. Откройте страницу **Reset** (Сброс).
2. Выберите номер устройства, введя его в поле **Reset Unit Number** (Номер устройства для сброса).
3. Нажмите кнопку **Apply Changes** (Применить изменения).

   Появится сообщение подтверждения.
4. Нажмите кнопку **OK**.

   Будут восстановлены заводские настройки устройства. После сброса установок устройства будет выведено окно ввода имени пользователя и пароля.
5. Введите имя пользователя и пароль, чтобы снова подключиться к веб-интерфейсу.

Восстановление заводских параметров устройства с помощью команд консоли

В приведенной ниже таблице указаны эквивалентные команды консоли, предназначенные для сброса установок устройства:

Таблица 6-8. Команды консоли для сброса

Команда консоли	Описание
reload	Перезагрузка устройства.

Далее приведен пример команды консоли:

```
console# reload

You haven't saved your changes. (Изменения не были сохранены.) Are you sure you want to continue? (Вы уверены, что хотите продолжить?) (Y/N)
[N] Y

This command will reset the whole system and disconnect your current session. (По этой команде сеанс работы будет прерван и произойдет
перезагрузка системы) Do you want to continue? (Хотите продолжить?) (Y/N)[N] Y
```

Настройка параметров SNTP

Коммутатор поддерживает "Простой протокол сетевого управления" (SNTP). Протокол SNTP гарантирует точность синхронизации времени такта сетевого коммутатора до миллисекунды. Синхронизация по времени выполняется сетевым сервером SNTP. SNTP работает только как клиент и не предоставляет службу синхронизации времени для других систем.

Коммутатор может запрашивать настройку времени у следующих типов серверов.

- Сервер одноадресной рассылки
- Сервер любого типа рассылки
- Сервер широковещательной рассылки

Источники времени устанавливаются по уровням. Уровни определяют точность источника времени. Чем выше уровень (нуль - это самый высокий уровень), тем более точным является встроенный генератор синхроимпульсов (часы). Коммутатор получает время с уровня 1 и выше. *Далее приведен пример уровней:*

- **Уровень 0** — *в качестве источника времени используются часы реального времени, например система GPS.*
- **Уровень 1** — *Используется сервер, который напрямую связан с источником времени уровня. Серверы времени уровня 1 предоставляют основные стандарты времени в сети.*
- **Уровень 2** — *источник времени подключен к серверу уровня 1 по сети. Например, сервер уровня 2 получает настройку времени по сетевому соединению по протоколу NTP от сервера уровня 1.*

Получаемые от сервера SNTP данные оцениваются на основе уровня времени и типа сервера. Оценка и определение значений времени SNTP выполняется по следующим уровням времени:

- **T1** — *время, когда исходный запрос был послан клиентом.*
- **T2** — *время, когда исходный запрос был получен сервером.*
- **T3** — *время, когда сервер отправил ответ клиенту.*
- **T4** — *время, когда клиент получил ответ от сервера.*

Устройство может запрашивать настройку времени у следующих типов серверов: Unicast (сервер одноадресной передачи), Anycast (сервер передачи любого типа) и Broadcast (сервер широковещательной передачи).

Опрос данных одноадресной рассылки используется для опроса сервера, для которого известен IP-адрес. Для получения данных синхронизации опрашиваются только серверы SNTP, настроенные на устройстве. T1-T4 используются для определения времени сервера. Это предпочтительный метод для синхронизации времени устройства, т.к. он является наиболее безопасным. Если выбран данный метод, информация SNTP принимается только от серверов SNTP, определенных на устройстве с помощью страницы **SNTP Servers** (Серверы SNTP).

Опрос данных рассылки любого типа используется в том случае, если известен IP-адрес. Если выбран данный метод, все SNTP серверы сети могут отправлять данные синхронизации. Устройство считается синхронизированным, если оно заранее отправляет запросы о синхронизации данных. Для установки значения времени используется наиболее подходящий ответ (низший уровень) на запрос о данных синхронизации от первых трех серверов SNTP. Уровни времени T3 и T4 используются для определения времени сервера.

Опрос серверов для получения данных о времени по методу передачи любого типа является более предпочтительным, чем опрос по методу широковещательной передачи. Однако этот метод менее безопасен, чем метод широковещательной передачи, поскольку в данном случае принимаются пакеты SNTP от серверов SNTP, не настроенных на устройстве.

Данные серверов широковещательной рассылки используются в том случае, если IP-адрес сервера неизвестен. Если сообщение широковещательной передачи отправляется с сервера SNTP, то клиент SNTP ожидает это сообщение. Если включен опрос по методу широковещательной передачи, принимаются любые данные синхронизации, даже если они не запрашивались устройством. Это наименее безопасный метод.

Устройство осуществляет поиск данных синхронизации либо путем постоянных запросов, либо в каждый интервал опроса. Если включен опрос по методу одноадресной передачи, рассылки любого типа и широковещательной передачи, то поиск данных осуществляется в следующем порядке.

- Предпочтение отдается данным от серверов, определенных на устройстве. Если опрос по методу одноадресной рассылки отключен или ни один сервер не определен на устройстве, устройство принимает данные от любого отвечающего сервера SNTP.
- Если поступает ответ от нескольких устройств широковещательной рассылки, предпочтение отдается данным синхронизации от устройства с низшим уровнем.
- Если у серверов один и тот же уровень, данные синхронизации принимаются от сервера SNTP, ответившего первым.

Проверка подлинности MD5 (Message Digest 5) обеспечивает синхронизацию линий связи устройства с серверами SNTP. MD5 - это алгоритм, создающий 128-разрядную хеш-строку. MD5 является разновидностью алгоритма MD4, который обеспечивает большую безопасность по сравнению с MD4. MD5 проверяет целостность передаваемых данных, а также определяет источник передаваемых данных.

Чтобы открыть страницу SNTP, выберите **System** (Система)→ **SNTP** на панели дерева.

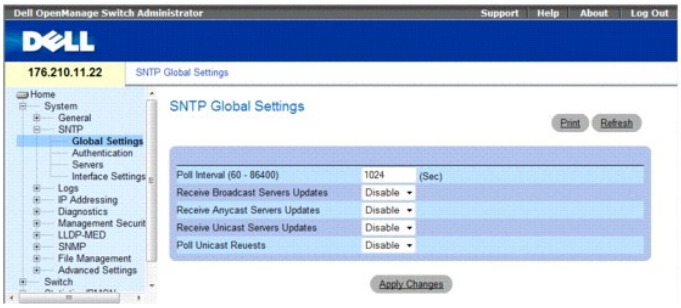
В этом разделе имеются следующие тематические подразделы:

- Определение общих параметров SNTP
- Определение методов проверки подлинности SNTP
- Определение серверов SNTP
- Определение интерфейсов SNTP

Определение общих параметров SNTP

Страница **SNTP Global Settings** (Общие параметры SNTP) содержит информацию для определения общих параметров SNTP. Чтобы открыть страницу **SNTP Global Settings** (Общие параметры SNTP), выберите **System** (Система)→ **SNTP**→ **Global Settings** (Общие параметры) на панели дерева.

Рис. 6-10. Общие параметры SNTP



Страница **SNTP Global Settings** (Общие параметры SNTP) содержит следующие поля.

- **Poll Interval (60-86400)** (Интервал опроса). определяет интервал (в секундах), с которым сервер SNTP запрашивает одноадресную информацию. По умолчанию интервал опроса составляет 1024 секунды.
- **Receive Broadcast Servers Updates** (Принимать обновления от серверов широковещательной рассылки). опрашивает серверы SNTP для получения данных о времени от сервера широковещательной рассылки для выбранных интерфейсов.
- **Receive Anycast Servers Updates** (Принимать обновления от серверов рассылки любого типа). опрашивает сервер SNTP для получения данных о времени от сервера рассылки любого типа для выбранных интерфейсов. Если включены оба поля (**Receive Anycast Servers Update** (Принимать обновления от серверов рассылки любого типа) и **Receive Broadcast Servers Update** (Принимать обновления от серверов широковещательной рассылки)), системное время устанавливается в соответствии с данными о времени, полученными от сервера рассылки любого типа.

- **Receive Unicast Servers Updates** (Принимать обновления от серверов одноадресной рассылки). опрашивает сервер SNTP для получения данных о времени от сервера одноадресной рассылки для выбранных интерфейсов. Если включены все три поля - **Receive Broadcast Servers Updates** (Принимать обновления от серверов широковещательной рассылки), **Receive Anycast Servers Updates** (Принимать обновления от серверов рассылки любого типа) и **Receive Unicast Servers Updates** (Принимать обновления от серверов одноадресной рассылки), - то системное время устанавливается в соответствии с данными времени, полученными от сервера одноадресной рассылки.
- **Poll Unicast Requests** (Опрашивать серверы одноадресной передачи). если этот параметр включен, отправляет запросы данных о времени сервера одноадресной рассылки SNTP на сервер SNTP.

Определение общих параметров SNTP

1. Откройте страницу **SNTP Global Settings** (Общие параметры SNTP).
2. Определите поля.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

   Изменения настроек SNTP будут применены.

Определение общих параметров SNTP с помощью команд консоли

В следующей таблице приведены команды консоли для настройки полей, отображаемых на странице **SNTP Global Settings** (Общие параметры SNTP)**.**

Команда консоли	Описание
sntp broadcast client enable	Включает клиентов широковещательной передачи SNTP
sntp anycast client enable	Включает клиентов рассылки любого типа SNTP
sntp unicast client enable	Включает клиентов одноадресной передачи SNTP

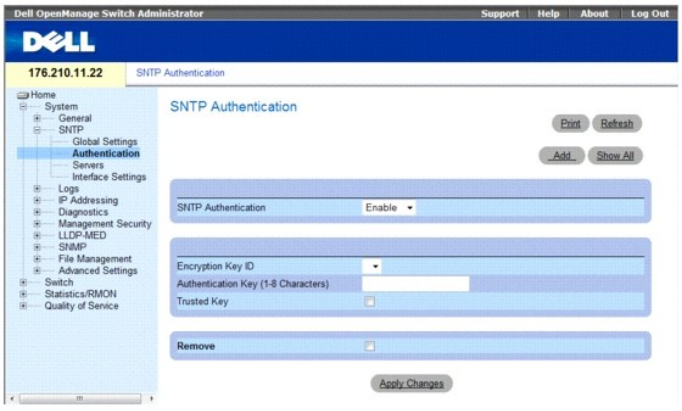
Далее приведен пример команд консоли.

```
console(config)# sntp anycast client enable
```

Определение методов проверки подлинности SNTP

Страница **SNTP Authentication** (Проверка подлинности SNTP) позволяет включить проверку подлинности SNTP между устройством и сервером SNTP. Это означает, что на странице **SNTP Authentication** (Проверка подлинности SNTP) также выбирается сервер, который выполняет проверку подлинности. Выберите **System** (Система)→ **SNTP**→ **Authentication** (Проверка подлинности), чтобы открыть страницу **SNTP Authentication** (Проверка подлинности SNTP).

Рис. 6-11. Проверка подлинности SNTP



Страница **SNTP Authentication** (Проверка подлинности SNTP) содержит следующие поля:

- **SNTP Authentication** (Проверка подлинности SNTP). включает или выключает проверку подлинности сеанса SNTP между устройством и сервером SNTP.
  - **Enable** (Включить). проводит проверку подлинности сеанса SNTP между устройством и сервером SNTP.

- **Disable** (Выключить). отключает проверку подлинности сеанса SNTP между устройством и сервером SNTP.

- **Encryption Key ID** (Идентификатор ключа шифрования). определяет идентификатор ключа, который используется для проверки подлинности сервера SNTP и устройства. Максимальная длина значения в этом поле составляет 4294967295 символов.
- **Authentication Key (8 Characters)** (Ключ проверки подлинности от 1 до 8 символов). определяет ключ, используемый для проверки подлинности.
- **Trusted Key** (Доверенный ключ). определяет ключ шифрования (одноадресный), используемый для проверки подлинности сервера SNTP.
  - **Флажок установлен**. ключ шифрования задействован.
  - **Флажок снят**. ключ шифрования не задействован.
- **Remove** (Удалить). удаление выбранных ключей проверки подлинности.
  - **Флажок установлен**. удаляет выбранный ключ шифрования.
  - **Флажок снят**. применяет выбранные ключи шифрования. Это значение по умолчанию.

Добавление ключа проверки подлинности SNTP

1. Откройте страницу **SNTP Authentication** (Проверка подлинности SNTP).
2. Нажмите кнопку **Add** (Добавить).

   Откроется страница **Add Authentication Key** (Добавление ключа проверки подлинности).

   Рис. 6-12. Добавление ключа проверки подлинности

3. Определите поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

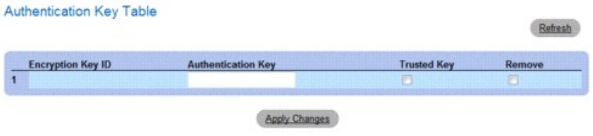
   Будет добавлен ключ проверки подлинности SNMP, а устройство будет обновлено.

Отображение таблицы ключей проверки подлинности

1. Откройте страницу **SNTP Authentication** (Проверка подлинности SNTP).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **Authentication Key Table** (Таблица ключей проверки подлинности).

   Рис. 6-13. Таблица ключей проверки подлинности



Удаление ключа проверки подлинности

1. Откройте страницу **SNTP Authentication** (Проверка подлинности SNTP).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **Authentication Key Table** (Таблица ключей проверки подлинности).

3. Выберите запись в **Authentication Key Table** (Таблица ключей проверки подлинности).

4. Установите флажок **Remove** (Удалить).
5. Нажмите кнопку **Apply Changes** (Применить изменения).

   Запись будет удалена, а устройство обновлено.

Определение параметров проверки подлинности SNTP с помощью команд консоли

В следующей таблице приведены команды консоли для настройки полей, отображаемых на странице **SNTP Authentication** (Проверка подлинности SNTP).

Команда консоли	Описание
sntp authenticate	Определяет проверку подлинности для трафика полученного от серверов простого сетевого протокола времени (SNTP).
sntp trusted-key	Проверяет подлинность системы, для которой производится синхронизация протокола SNTP.
sntp authentication-key *номер* **md5** *значение*	Определяет ключ проверки подлинности для SNTP.

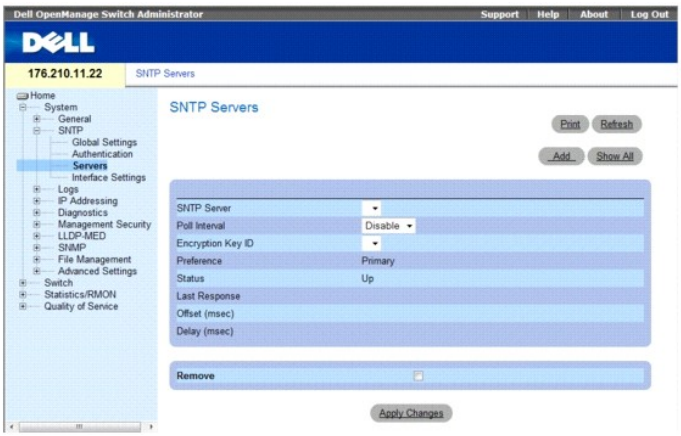
Далее приведен пример команд консоли.

```
console(config)# sntp authentication-key 8 md5 Calked

Console(config)# sntp trusted-key 8

Console(config)# sntp authenticate
```

Определение серверов SNTP

Страница **SNTP Servers** (Серверы SNTP) содержит информацию для выбора сервера SNTP, а также позволяет добавить новый сервер. *Чтобы открыть страницу* **SNTP Servers** (Серверы SNTP), на панели дерева выберите **System** (Система)→ **SNTP**→ **SNTP Servers** (Серверы SNTP).

Рис. 6-14. Серверы SNTP



Страница **SNTP Servers** (Серверы SNTP) содержит следующие поля.

- **SNTP Server** (Сервер SNTP). определяемый пользователем IP-адрес сервера SNTP. Можно определить до восьми серверов SNTP.
- **Poll Interval** (Интервал опроса). когда этот флажок установлен, включается опрос сервера SNTP для получения данных о времени.
- **Encryption Key ID** (Идентификатор ключа шифрования). отображает идентификатор ключа, который используется для обмена данными между сервером SNTP и устройством. Диапазон значений: 1 - 4294967295.
- **Preference** (Настройка). сервер SNTP, предоставляющий данные о системном времени SNTP. Возможные значения:
  - **Primary** (Основной). основной сервер, предоставляющий информацию SNTP.
  - **Secondary** (Дополнительный). резервный сервер, предоставляющий информацию SNTP.
- **Status** (Состояние). рабочее состояние сервера SNTP. Возможные значения:

- **Up** (Работает). сервер SNTP работает надлежащим образом.
- **Down** (Отключен). сервер SNTP в настоящее время недоступен. Например, сервер SNTP в настоящее время не подключен или отключен.
- **In progress** (Выполняется операция). сервер SNTP отправляет или принимает информацию SNTP.
- **Unknown** (Неизвестно). состояние процесса передачи информации SNTP в настоящее время неизвестно. Например, устройство в настоящее время выполняет поиск интерфейса.

- **Last Response** (Последний ответ). время, когда был получен последний ответ от сервера SNTP.
- **Offset** (Смещение). разница во времени между часами устройства и временем, полученным от сервера SNTP.
- **Delay (msec)** (Задержка, мс). время, необходимое для передачи пакета до сервера SNTP.
- **Remove** (Удалить). удаление указанного SNTP-сервера из списка **SNTP Servers**.
  - **Флажок установлен**. удаляет выбранный SNTP сервер.
  - **Флажок снят**. оставляет указанный сервер SNTP в настройке. Это значение по умолчанию.

При подключении дополнительного сервера SNTP, будут доступны следующие дополнительные параметры:

- **Supported IP Format** (Поддерживаемый формат IP-адресов). отображает формат IP-адресов, поддерживаемый сервером SNTP. Возможные значения:
  - **IPv6**. поддержка IP версии 6.
  - **IPv4**. поддержка IP версии 4.
- **IPv6 Address Type**. в случае, если сервер поддерживает систему IPv6 (см. предыдущий параметр), здесь указывается поддерживаемый тип статических адресов. Возможные значения:
  - **Link Local** (Локальная связь). адрес локальной связи, который не маршрутизируется, а используется только для связи в пределах той же сети.
  - **Global** (Глобальный). глобальный уникальный адрес IPv6 address; он является видимым и доступным для различных подсетей.
- **Link Local Interface** (Интерфейс локальной связи). если сервер поддерживает систему адресов локальной связи IPv6 (см. предыдущий параметр), здесь указывается интерфейс локальной связи. Возможные значения:
  - **VLAN1**. интерфейс IPv6 конфигурируется по сети VLAN1.
  - **ISATAP**. интерфейс IPv6 конфигурируется по туннелю ISATAP.

Добавление сервера SNTP

1. Откройте страницу **SNTP Servers** (Серверы SNTP).
2. Нажмите кнопку **Add** (Добавить).

   Откроется страница **Add SNTP Server** (Добавление сервера SNTP).

   Рис. 6-15. Добавление сервера SNTP

3. Определите поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

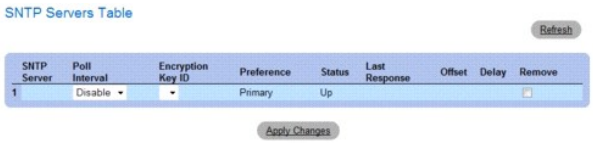
   Будет добавлен сервер SNTP, а устройство будет обновлено.

Отображение таблицы серверов SNTP

1. Откройте страницу **SNTP Servers** (Серверы SNTP).
2. Нажмите кнопку **Show All** (Показать все).

Откроется страница **SNTP Servers Table** (Таблица серверов SNTP).

Рис. 6-16. Таблица серверов SNTP



Изменение сервера SNTP

1. Откройте страницу **SNTP Servers** (Серверы SNTP).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **SNTP Servers Table** (Таблица серверов SNTP).
3. Выберите запись сервера SNTP.
4. Измените соответствующие поля.
5. Нажмите кнопку **Apply Changes** (Применить изменения).

   Информация сервера SNTP будет обновлена.

Удаление сервера SNTP

1. Откройте страницу **SNTP Servers** (Серверы SNTP).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **SNTP Servers Table** (Таблица серверов SNTP).
3. Выберите запись **SNTP Server** (Сервер SNTP).
4. Установите флажок **Remove** (Удалить).
5. Нажмите кнопку **Apply Changes** (Применить изменения).

   Запись будет удалена, а устройство обновлено.

Определение параметров серверов SNTP с помощью команд консоли

В следующей таблице приведены команды консоли для настройки полей, отображаемых на странице **SNTP Server** (Сервер SNTP).

Команда консоли	**Описание**
sntp server *ipv4-address*| *ipv6-address*|hostname [**poll**] [**key** *keyid*]	SNTP Настраивает устройство для использования SNTP при запросе и принятии трафика SNTP от сервера.

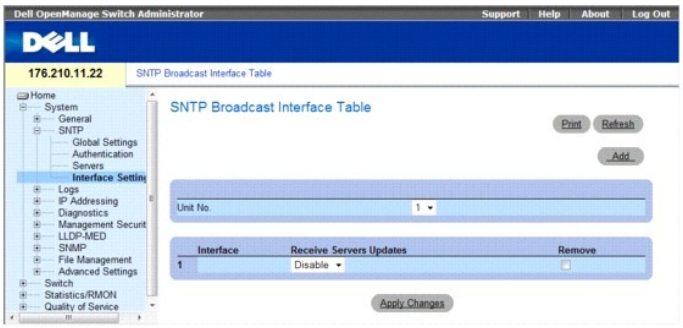
Далее приведен пример команд консоли.

```
Console(config)# sntp server 100.1.1.1 poll key 10
```

Определение интерфейсов SNTP

Страница **SNTP Broadcast Interface Table** (Таблица интерфейсов широковещательной передачи SNTP) содержит информацию об интерфейсе SNTP. Чтобы открыть страницу **SNTP Broadcast Interface Table**, выберите **System** (Система)→ **SNTP**→ **Interface Settings** (Параметры интерфейсов).

Рис. 6-17. SNTP Broadcast Interface Table (Таблица интерфейсов широковещательной передачи SNTP)



Страница **SNTP Broadcast Interface Table** (Таблица интерфейсов широковещательной передачи SNTP) содержит следующие поля:

- **Unit No.** (Номер устройства). указывает номер устройства, для которого включен интерфейс SNTP.

Interface (Интерфейс). содержит список интерфейсов, для которых можно включить протокол SNTP.

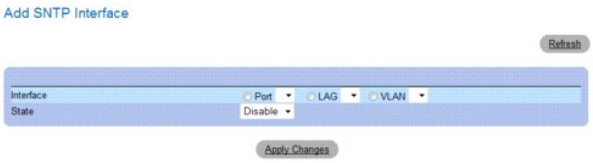
- **Receive Servers Updates** (Принимать обновления сервера). включает или отключает получение обновлений SNTP для определенного интерфейса.
  - **Enable** (Включить). включает получение обновлений SNTP для определенного интерфейса с сервера SNTP.
  - **Disable** (Выключить). интерфейс не будет получать обновление с сервера SNTP.
- **Remove** (Удалить). когда этот флажок установлен, протокол SNTP для указанного интерфейса будет отключен.
  - **Флажок установлен**. удаляет выбранный ввод интерфейса SNTP.
  - **Флажок снят**. оставляет выбранный ввод интерфейса SNTP.

Добавление интерфейса SNTP

1. Откройте страницу **SNTP Broadcast Interface Table** (Таблица интерфейсов широковещательной передачи SNTP).
2. Нажмите кнопку **Add** (Добавить).

   Откроется страница **Add SNTP Interface** (Добавление интерфейса SNTP).

   Рис. 6-18. Добавление интерфейса SNTP



3. Определите соответствующие поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Интерфейс SNTP будет добавлен, а устройство обновлено.

Определение параметров интерфейса SNTP с помощью команд консоли

В следующей таблице приведены команды консоли для настройки полей, отображаемых на странице **SNTP Broadcast Interface Table** (Таблица интерфейсов широковещательной передачи SNTP).

Команда консоли	Описание
sntp client enable	Включает клиента SNTP (Simple Network Time Protocol) для интерфейса.

show sntp configuration	Отображает настройку протокола SNTP (Simple Network Time Protocol).

Далее приведен пример команд консоли для отображения интерфейсов SNTP.

```
console# show sntp configuration
Polling interval (Интервал опроса): 7200 seconds (секунд).

MD5 Authentication keys (Ключи для проверки подлинности MD5): 8, 9
Authentication is required for synchronization (Для синхронизации требуется проверка подлинности).
Trusted Keys (Доверенные ключи): 8,9

Unicast Clients Polling (Опрос клиента одноадресной рассылки): Enabled (Включен).

Server (Сервер)                          Polling (Опрос)   Encryption Key (Ключ шифрования)
---------------------------------------- ----------------- --------------------------------
176.1.1.8                                Enabled (Включено) 9
176.1.8.179                              Disabled (Выключено) Disabled (Выключено)

Broadcast Clients (Клиенты широковещательной передачи): Enabled (Включено)
Broadcast Clients Poll (Опрос клиентов широковещательной передачи): Enabled (Включено)
Broadcast Interfaces (Интерфейсы широковещательной передачи):1/e1, 1/e3
```

Управление журналами

Страница Logs (Журналы) содержит ссылки на страницы разных журналов. Чтобы открыть страницу **Logs** (Журналы), на панели дерева выберите **System** (Система)→ **Logs** (Журналы).

В этом разделе имеются следующие тематические подразделы:

- Определение общих параметров журналов
- Просмотр таблицы RAM Log Table (Таблица журнала ОЗУ)
- Просмотр таблицы Log File Table (Таблица файла журнала)
- Просмотр журнала входов устройств
- Изменение определений удаленного сервера журналов

Определение общих параметров журналов

Системные журналы позволяют просматривать события устройства в реальном времени, а также записывать события для использования в дальнейшем. Журналы событий позволяют записывать и управлять событиями, а также отображать сообщения об ошибках и информационные сообщения.

Сообщения событий имеют уникальный формат в соответствии с рекомендациями протокола System Logs относительно формата сообщений для всех сообщений об ошибках. Например, для сообщений Syslog и сообщений локальных устройств назначается код уровня ошибки, а также добавляется мнемоника сообщения, которая определяет исходное приложение, создавшее сообщение. Это позволяет фильтровать сообщения на основе срочности или важности. Распределением сообщений журнала по различным адресам, например в буфер журнала, файл журнала или на сервер Syslog, управляют параметры настройки Syslog. Пользователи могут определить до восьми серверов Syslog.

Ниже указаны уровни важности журналов:

- **Emergency** (Аварийное). наивысший уровень предупреждения. Если устройство выключено или работает неправильно, сообщение аварийного журнала сохраняется в определенном местоположении журнала.
- **Alert** (Сигнал о сбое). второй уровень аварийного предупреждения. Журнал сохраняется при серьезных отклонениях в работе устройства, например, если все функции устройства отключены.
- **Critical** (Критическое). третий уровень аварийного предупреждения. Критический журнал сохраняется в том случае, если происходят критические отклонения в работе устройства, например, если не работают два порта устройства, в то время как остальные по-прежнему работают.

- **Error** (Ошибка). произошла ошибка устройства, например, если порт отключен.
- **Warning** (Предупреждение). самый низкий уровень предупреждения устройства. Устройство работает, но имеется ошибка в работе.
- **Notice** (Уведомление). предоставляет информацию об устройстве.
- **Informational** (Информационное). предоставляет информацию об устройстве.
- **Debug** (Отладка). предоставляет отладочные сообщения.

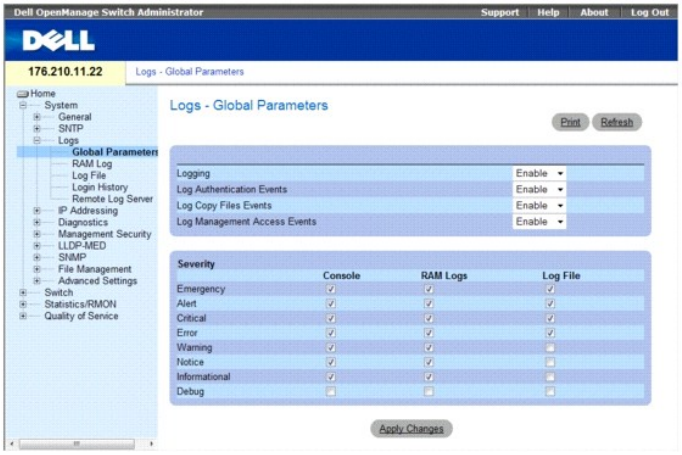
Таблица 6-13. Уровни важности журнала

Тип важности	Уровень важности	Описание
Аварийное	0	Система не работает.
Сигнал о сбое	1	Система требует немедленного вмешательства.
Критическое	2	Система находится в критическом состоянии.
Ошибка	3	Произошла ошибка системы.
Предупреждение	4	Появилось предупреждение системы.
Примечание	5	Система работает правильно, но появилось уведомление системы.
Информационное	6	Предоставляет сведения об устройстве.
Отладка	7	Предоставляет подробные сведения о журнале. При возникновении ошибки отладки обратитесь в интерактивную службу технической поддержки Dell.

Страница **Logs - Global Parameters** (Общие параметры журналов) содержит поля, позволяющие определить события и журналы, в которые они должны быть записаны. Она содержит поля для общего включения журналов и поля для определения параметров журналов. Сообщения журнала Severity (Важность) перечисляются в порядке от большей важности к меньшей.

Чтобы открыть страницу **Logs - Global Parameters** (Общие параметры журналов), на панели дерева выберите **System** (Система)→ **Logs** (Журналы)→ **Global Parameters** (Общие параметры).

Рис. 6-19. Общие параметры журналов



Страница **Logs - Global Parameters** (Общие параметры журналов) содержит следующие параметры:

- **Logging** (Регистрация). включает или выключает функции создания глобальных журналов для кэширования, файлов и серверов на устройстве. Вывод журнала на консоль по умолчанию включен.
- **Log Authentication Events** (Вести журнал событий проверки подлинности). включает или выключает генерирование журналов при проверке подлинности пользователей.
- **Log Copy Files Events** (Вести журнал копирования файлов). включает или выключает генерирование журналов при копировании файлов.
- **Log Management Access Events** (Вести журнал управления доступом). включает или выключает генерирование журналов при доступе к устройству через систему управления. Например, при каждом доступе к устройству через SSH, создается журнал устройства.
- **Severity** (Уровень важности). отображает журналы важности. Ниже показаны уровни важности журналов. Если выбирается уровень важности, автоматически выбираются все уровни важности выше указанного.
  - **Emergency** (Аварийное). наивысший уровень предупреждения. Если устройство выключено или работает неправильно, сообщение аварийного журнала сохраняется в определенном местоположении журнала.
  - **Alert** (Сигнал о сбое). второй уровень аварийного предупреждения. Журнал сохраняется при серьезных отклонениях в работе устройства, вызванных, например, попыткой загрузить несуществующий файл настройки.

- **Critical** (Критическое). третий уровень аварийного предупреждения. Критический журнал сохраняется в том случае, если происходят критические отклонения в работе устройства, например, если не работают два порта устройства, в то время как остальные по-прежнему работают.
- **Error** (Ошибка). произошла ошибка устройства, например сбой в операции копирования.
- **Warning** (Предупреждение). самый низкий уровень предупреждения устройства. Например, устройство работает, а соединение порта в настоящее время отключено.
- **Notice** (Уведомление). предоставляет важную информацию об устройстве.
- **Informational** (Информационное). предоставляет информацию об устройстве. Например, порт в настоящее время работает.
- **Debug** (Отладка). предоставляет отладочные сообщения.

Страница **Global Log Parameters** (Общие параметры журналов) также содержит флажки, которые соответствуют отдельной системе регистрации:

- **Console** (консоль). минимальный уровень важности, из которого журналы передаются на консоль.
- **RAM Logs** (Журналы ОЗУ). минимальный уровень важности, из которого журналы передаются в файл журнала, который хранится в ОЗУ (кэше).
- **Log File** (Файл журнала). минимальный уровень важности, из которого журналы передаются в файл журнала, который хранится во флэш-памяти.

Включение журналов

1. Откройте страницу **Global Log Parameters** (Общие параметры журналов).
2. Выберите значение **Enable** (Включить) в раскрывающемся списке **Logging** (Протоколирование).
3. Выберите тип журнала и важность журнала, установив флажки **Global Log Parameters** (Общие параметры журналов).
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Параметры журналов будут сохранены, а устройство обновлено.

Включение журналов с помощью команд консоли

В следующей таблице приведены команды консоли для настройки полей, отображаемых на странице **Global Log Parameters** (Общие параметры журналов).

Команда консоли	**Описание**
logging on	Включает регистрацию сообщений об ошибках.
logging {ipv4-address | ipv6-address | hostname} [**port** *port*] [**severity** *level*] [**facility** *facility*] [**description** *text*]	Регистрирует сообщения на сервере системных журналов. Список уровней важности см. в разделе Уровни важности журнала.
logging console *уровень*	Ограничивает сообщения, фиксируемые в журнале консоли, в зависимости от их важности.
logging buffered *уровень*	Ограничивает вывод системных сообщений из внутреннего буфера (ОЗУ) в зависимости от их важности.
logging file *уровень*	Ограничивает количество системных сообщений, посылаемых в файл журналов, в зависимости от их важности.
clear logging	Очищает журналы.
clear logging file	Удаляет сообщения из файла журнала.
show syslog servers	Отображает установки системных журналов.

Далее приведен пример команд консоли.

```
console(config)# logging on

console(config)# logging console errors

console(config)# logging buffered debugging

console(config)# logging file alerts

console(config)# end

console# clear logging file

Clear Logging File [y/n]y
```

```
Console# show syslog-servers

Device Configuration (Конфигурация устройства)

-----------------------------

IP address (IP - flhtc)     Port  facility (портовые устройства)  Severity (степень
«тяжести» ошибки)  Description (описание)

----------     ----  --------  --------  -----------

  1.1.1.1       514 local7    info

fe80::11%vlan1  514 local7    info

  3211::22      514 local7    info
```

Просмотр таблицы RAM Log Table (Таблица журнала ОЗУ)

Страница **RAM Log Table** (Таблица журнала ОЗУ) содержит сведения о записях журнала, хранящегося в ОЗУ, включая время, когда был записан журнал, важность журнала и описание журнала. Чтобы открыть **RAM Log Table** (Таблица журнала ОЗУ), на панели дерева выберите **System** (Система) → **Logs** (Журналы)→ **RAM Log** (Журнал ОЗУ).

Рис. 6-20. Страница RAM Log Table (Таблица журнала ОЗУ)

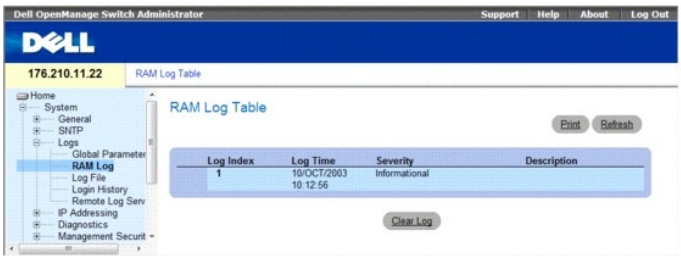


Таблица **RAM Log Table** (Таблица журнала ОЗУ) содержит следующие поля.

- **Log Index** (Индекс журнала). показывает номер журнала в **RAM Log Table** (Таблица журнала ОЗУ).
- **Log Time** (Время журнала). время, когда журнал был введен в **RAM Log Table** (Таблица журнала ОЗУ).
- **Severity** (Уровень важности). указывает важность журнала.
- **Description** (Описание). описывает запись в журнале.

Удаление данных журнала:

1. Откройте страницу **RAM Log Table** (Таблица журнала ОЗУ).
2. Нажмите кнопку **Clear Log** (Очистить журнал).

   Информация журнала будет удалена из **RAM Log Table** (Таблица журнала ОЗУ), а устройство обновлено.

Просмотр и очистка таблицы журнала ОЗУ с помощью команд консоли

В следующей таблице приведены команды консоли для просмотра и очистки полей, отображаемых на странице **RAM Log Table** (Таблица журнала ОЗУ).

Команда консоли	Описание
show logging	Отображает состояние журнала и системные сообщения, хранящиеся во внутреннем буфере.
clear logging	Очищает журналы.

Далее приведен пример команд консоли.

```
console# show logging
```

```
Logging is enabled.

Console Logging: Level info. Console Messages: 0 Dropped.

Buffer Logging: Level info. Buffer Messages: 124 Logged, 124 Displayed, 200 Max.

File Logging: Level error. File Messages: 164 Logged, 126 Dropped.

3 messages were not logged

Application filtering control

Application Event Status

AAA Login Enabled

File system Copy Enabled

File system Delete-Rename Enabled

Management ACL Deny Enabled



01-Jan-2000 09:23:34 :%Box-I-PS-STAT-CHNG: PS# 1 status is - operational.

01-Jan-2000 09:23:29 :%Box-W-PS-STAT-CHNG: PS# 1 status is - not operational.

01-Jan-2000 09:22:44 :%Box-I-PS-STAT-CHNG: PS# 1 status is - operational.

01-Jan-2000 09:22:39 :%Box-W-PS-STAT-CHNG: PS# 1 status is - not operational.

01-Jan-2000 09:10:34 :%Box-I-PS-STAT-CHNG: PS# 1 status is - operational.

01-Jan-2000 09:10:29 :%Box-W-PS-STAT-CHNG: PS# 1 status is - not operational.

01-Jan-2000 09:09:16 :%AAA-I-CONNECT: New http connection for user admin, source 192.168.102.5
destination 192.168.102.15 ACCEPTED

01-Jan-2000 08:39:49 :%Box-I-PS-STAT-CHNG: PS# 1 status is - operational.
```

Просмотр таблицы Log File Table (Таблица файла журнала)

Log **File Table** (Таблица файла журналов) содержит сведения о записях журнала, сохраненных в файле журналов во флэш-памяти, включая время, когда был записан журнал, важность журнала и описание сообщения журнала. Чтобы открыть **Log File Table**, на панели дерева выберите **System** (Система)→ **Logs** (Журналы)→ **Log File** (Файл журнала).

Рис. 6-21. Страница Log File Table (Таблица файла журналов)

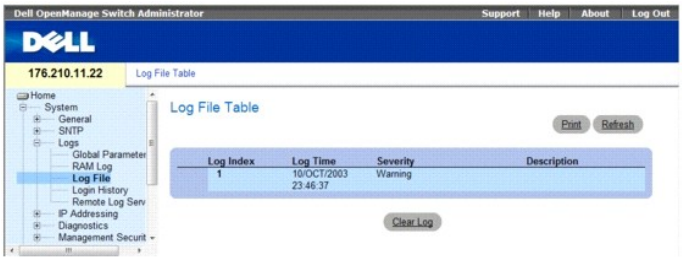


Таблица **Log File Table** (Таблица файла журналов) содержит следующие поля:

- **Log Index** (Индекс журнала). показывает номер журнала в **Log File Table** (Таблица файла журнала).
- **Log Time** (Время журнала). время, когда журнал был введен в **Таблицу файла журнала**.
- **Severity** (Уровень важности). указывает важность журнала.
- **Description** (Описание). текст сообщения журнала.

Отображение таблицы файла журналов с помощью команд консоли

В следующей таблице приведены команды консоли для просмотра и настройки полей, отображаемых на странице **Log File Table** (Таблица файла журнала).

Команда консоли	Описание
show logging file	Отображает состояние журнала и системные сообщения, хранящиеся в файле журналов.
clear logging file	Удаляет сообщения из файла журнала.

Далее приведен пример команд консоли.

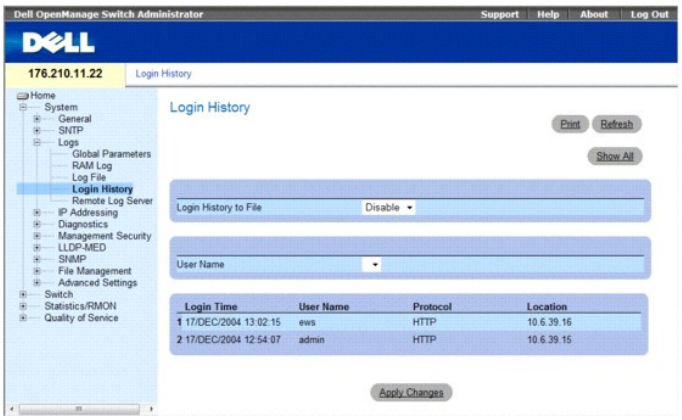
```
console# show logging file

Logging is enabled.

Console Logging: Level info. Console Messages: 0 Dropped.

Buffer Logging: Level info. Buffer Messages: 62 Logged, 62 Displayed, 200 Max.

File Logging: Level debug. File Messages: 11 Logged, 51 Dropped.

SysLog server 12.1.1.2 Logging: warning. Messages: 14 Dropped.

SysLog server 1.1.1.1 Logging: info. Messages: 0 Dropped.

01-Jan-2000 01:12:01 :%COPY-W-TRAP: The copy operation was completed successfully

01-Jan-2000 01:11:49 :%LINK-I-Up: 1/e11

01-Jan-2000 01:11:46 :%LINK-I-Up: 1/e12

01-Jan-2000 01:11:42 :%LINK-W-Down: 1/e13

01-Jan-2000 01:11:35 :%LINK-I-Up: 1/e14
```

Просмотр журнала входов устройств

На странице **Login History** (Журнал входов) содержатся сведения для просмотра и мониторинга использования устройств, включая время входа пользователя и использования протокола для доступа к устройству.

Чтобы открыть страницу **Login History** (Журнал входов), на панели дерева выберите **System** (Система)→ **Logs** (Журналы)→ **Login History** (Журнал входов).

Рис. 6-22. Журнал входов



На странице **Login History** (Журнал входов) находятся следующие поля:

- **User Name** (Имя пользователя). содержит список имен пользователя устройств, определенных пользователем.
- **Login History** (Журнал входов). показывает, что журналы входов включены.
- **Login Time** (Время входа). отображает время доступа выбранного пользователя к устройству.
- **User Name** (Имя пользователя). отображает имя пользователя, который произвел вход в устройство.
- **Protocol** (Протокол). отображает, каким способом пользователь получил доступ к устройству.
- **Location** (Местоположение). отображает IP-адрес точки, из которой был произведен вход в устройство.

Просмотр журнала входов

1. Откройте страницу **Login History** (Журнал входов).
2. Выберите пользователя в поле **User Name** (Имя пользователя).
3. Нажмите кнопку **Apply Changes** (Применить изменения).

   Отобразятся сведения о входе выбранного пользователя.

Отображение журнала входов в устройство с помощью команд консоли

В следующей таблице приведены команды консоли для просмотра и настройки полей, отображаемых на странице **Login History** (Журнал входов).

Команда консоли	**Описание**
show users login-history	Отображение информации о журнале управления паролями.

Далее приведен пример команд консоли.

console# **show users login-history**			
Login Time	Username	STP	Location
-----------	--------	--------	----------
01-Jan-2005 23:58:17	Anna	HTTP	172.16.1.8
01-Jan-2005 07:59:23	Errol	HTTP	172.16.0.8
01-Jan-2005 08:23:48	Amy	Последовательный порт	
01-Jan-2005 08:29:29	Alan	Страница SSH	172.16.0.8
01-Jan-2005 08:42:31	Bob	HTTP	172.16.0.1
01-Jan-2005 08:49:52	Cindy	Telnet	172.16.1.7

Изменение определений удаленного сервера журналов

Страница **Remote Log Server Settings** (Параметры удаленного сервера журналов) содержит поля для просмотра и настройки доступных серверов журналов. Кроме того, можно определить новые серверы журналов и важность журналов, отправляемых на каждый сервер.

Уровни важности событий перечислены на этой странице в убывающем порядке, начиная с самого высокого уровня важности, и заканчивая самым низким. Если выбирается какой-либо уровень важности для ввода в журнал, автоматически выбираются все уровни важности выше указанного. Если уровень важности не выбран, в журнале не будут отображаться события с более низким уровнем важности.

Например, если выбран уровень «Warning», то в журнале будут все события с уровнем важности «Warning» и выше. При этом события с уровнем важности ниже, чем «Warning», в журнале отображаться не будут.

Чтобы открыть страницу **Remote Log Server Settings** (Параметры удаленного сервера журналов), на панели дерева выберите **System** (Система)→ **Logs** (Журналы)→ **Remote Server Settings** (Установки удаленного сервера).

Рис. 6-23. Страница Remote Log Server Settings (Параметры удаленного сервера журналов)

Страница **Remote Log Server Settings** (Параметры удаленного сервера журналов OOB) содержит следующие поля.

- **Available Servers** (Доступные серверы). список серверов, на которые можно отправить журналы.
- **UDP Port (1-65535)** (Порт UDP). порт UDP, на который посылаются журналы для выбранного сервера. Возможные значения: от 1 до 65535. Значение по умолчанию: 514.
- **Facility** (Приложение). определяемое пользователем приложение, из которого отправляются журналы на удаленный сервер. Для одного сервера можно назначить только одно приложение. Если назначен второй уровень приложения, первый уровень приложения отменяется. Все приложения, определенные для устройства, используют одно и то же приложение на сервере. Значение поля по умолчанию - Local 7. Возможные значения поля:
  - **Local 0 - Local 7.**
- **Description (0-64 Characters)** (Описание (0-64 символов)). описание сервера, задаваемое пользователем.
- **Severity to Include** (Указываемая важность). далее приведены имеющиеся уровни важности:
  - **Emergency** (Аварийное). система не работает.
  - **Alert** (Сигнал о сбое). система требует немедленного вмешательства.
  - **Critical** (Критическое). система находится в критическом состоянии.
  - **Error** (Ошибка). произошла ошибка системы.
  - **Warning** (Предупреждение). появилось предупреждение системы.
  - **Notice** (Примечание). система работает правильно, но появилось уведомление системы.
  - **Informational** (Информационное). предоставляет информацию об устройстве.
  - **Debug** (Отладка) - предоставляет подробные сведения о журнале. При возникновении ошибки отладки обратитесь в службу технической поддержки клиентов.
- **Delete Server** (Удалить сервер). когда флажок установлен, выбранный сервер удаляется из списка *Available Servers* (Доступные серверы).

При подключении дополнительного сервера SNTP, будут доступны следующие дополнительные параметры:

- **Supported IP Format** (Поддерживаемый формат IP-адресов). Отображает формат IP-адресов, поддерживаемый сервером SNTP. Возможные значения:
  - **IPv6**. поддержка IP версии 6.
  - **IPv4**. поддержка IP версии 4.
- **IPv6 Address Type**. В случае, если сервер поддерживает систему IPv6 (см. предыдущий параметр), здесь указывается поддерживаемый тип статических адресов. Возможные значения:
  - **Link Local** (Локальная связь). Адрес локальной связи, который не маршрутизируется, а используется только для связи в пределах той же сети.
  - **Global** (Глобальный). Глобальный уникальный адрес IPv6 address; он является видимым и доступным для различных подсетей.
- **Link Local Interface** (Интерфейс локальной связи). Если сервер поддерживает систему адресов локальной связи IPv6 (см. предыдущий параметр), здесь указывается интерфейс локальной связи. Возможные значения:
  - **VLAN1**. Интерфейс IPv6 конфигурируется по сети VLAN1.
- **ISATAP**. Интерфейс IPv6 конфигурируется по туннелю ISATAP.

Отправка журналов на сервер

1. Откройте страницу **Remote Log Server Settings** (Параметры удаленного сервера журналов).
2. Выберите сервер в раскрывающемся списке **Available Servers** (Доступные серверы).
3. Определите поля.
4. Выберите уровень важности журнала, установив флажок **Severity to Include** (Указываемая важность).
5. Нажмите кнопку **Apply Changes** (Применить изменения).

   Параметры журналов будут сохранены, а устройство обновлено.

Определение нового сервера:

1. Откройте страницу **Remote Log Server Settings** (Параметры удаленного сервера журналов).
2. Нажмите кнопку **Add** (Добавить).

   Откроется страница **Add a Log Server** (Добавление сервера журналов) .

   Рис. 6-24. Добавление сервера журналов

Страница **Add a Log Server** (Добавление сервера журналов) содержит дополнительное поле.

- **New Log Server IP Address** (IP-адрес нового сервера журналов). определяет IP-адрес нового сервера журналов.

l Определите поля.

l Нажмите кнопку **Apply Changes** (Применить изменения).

Сервер будет определен и добавлен в список **Available Servers** (Доступные серверы).

Отображение таблицы удаленных серверов журналов:

1. Откройте страницу **Remote Log Server Settings** (Параметры удаленного сервера журналов).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **Log Servers Table** (Таблица серверов журналов):

   Рис. 6-25. Таблица серверов журналов.

Удаление сервера журналов со страницы Log Server Table (Таблица серверов журналов):

1. Откройте страницу **Remote Log Server Settings** (Параметры удаленного сервера журналов).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **Log Servers Table** (Таблица серверов журналов):
3. Выберите запись **Log Servers Table** (Таблица серверов журналов).
4. Установите флажок **Remove** (Удалить), чтобы удалить серверы.
5. Нажмите кнопку **Apply Changes** (Применить изменения).

   Запись **Log Servers Table** (Таблицы серверов журналов) будет удалена, а устройство обновлено.

Работа с удаленным сервером журналов с помощью команд консоли

В таблице перечислены эквивалентные команды консоли для работы с удаленными серверами журнала.

Команда консоли	**Описание**
logging *(ipv4-address|ipv6-addres* **|** *hostname}* [**port** *port*] [**severity** *level*] [**facility** *facility*] [**description** *text*]	Регистрирует сообщения на удаленном сервере.
no logging	Удаляет сервер syslog.
show logging	Отображает состояние журнала и системные сообщения.

Далее приведен пример команд консоли.

```
console> enable

console# configure

console (config) # logging 10.1.1.1 severity critical

console(config)# end

console# show logging

Logging is enabled.

Console Logging: Level debug. Console Messages: 5 Dropped.

Buffer Logging: Level debug. Buffer Messages: 16 Logged, 16 Displayed, 200 Max.

File Logging: Level error. File Messages: 0 Logged, 209 Dropped.

SysLog server 31.1.1.2 Logging: error. Messages: 22 Dropped.

SysLog server 5.2.2.2 Logging: info. Messages: 0 Dropped.

SysLog server 10.2.2.2 Logging: critical. Messages: 21 Dropped.

SysLog server 10.1.1.1 Logging: critical. Messages: 0 Dropped.

1 messages were not logged

03-Mar-2004 12:02:03 :%LINK-I-Up: 1/e11

03-Mar-2004 12:02:01 :%LINK-W-Down: 1/e12

03-Mar-2004 12:02:01 :%LINK-I-Up: 1/e13
```

Определение IP-адресации

Страница **IP Addressing** (IP-адресация) содержит ссылки для назначения IP-адресов интерфейса и шлюза по умолчанию, а также определения параметров ARP и DHCP для интерфейсов. Чтобы открыть страницу **IP Addressing** (IP-адресация), на панели дерева выберите **System** (Система)→ **IP Addressing** (IP-адресация).

В этом разделе имеются следующие тематические подразделы:

- Определение шлюзов по умолчанию для адресов IPv4
- Определение интерфейсов IPv4
- Определение параметров DHCP интерфейса IPv4
- Настройка системы имен доменов
- Определение доменов по умолчанию
- Отображение хоста домена
- Определение параметров ARP

Настройка интернет-протокола версии 6 (IPv6)

Устройство работает в качестве IPv6-совместимого хоста, и одновременно IPv4-совместимого хоста (режим, известный как режим обработки двойного стека). Это позволяет устройству работать как в полноценной сети IPv6, так и в комбинированной сети IPv4/IPv6.

Первоначальное различие между IPv4 и IPv6 состоит в длине сетевых адресов. Адреса системы IPv6 имеют длину 128 бит, в то время как адреса системы IPv4 имеют длину 32 бита; тем самым, предоставляется значительно большее пространство для ввода адреса.

Синтаксис системы IPv6

128-битный формат адресов IPv6 делится на восемь групп по четыре шестнадцатеричных числа знака. Допускаются сокращения путем замены группы нулей «двойным двоеточием» (::). Представление адресов системы IPv6 может в дальнейшем упрощаться путем пропуска нулей, стоящих в начале адреса.

Все различные форматы адресов IPv6 допускаются к вводу. Однако, в целях оптимизации экранного отображения, система будет отображать адреса в самой краткой форме, в которой группы нулей заменяются «двойным двоеточием» и удаляются нули, стоящие в начале адреса.

Префиксы системы IPv6

Несмотря на то, что допускается запись адресов одноадресной передачи системы IPv6 с префиксами, на практике длина этих префиксов будет всегда равна 64 знакам и, таким образом, устанавливать ее не требуется. Все префиксы, длина которых менее 64 бита, представляют собой диапазон маршрута или адреса, который сокращает часть адресного пространства адресов IPv6.

При каждом назначении IP-адреса интерфейсу, система запускает алгоритм обнаружения дублирующихся адресов (DAD), предназначенный для обеспечения уникальности адресов.

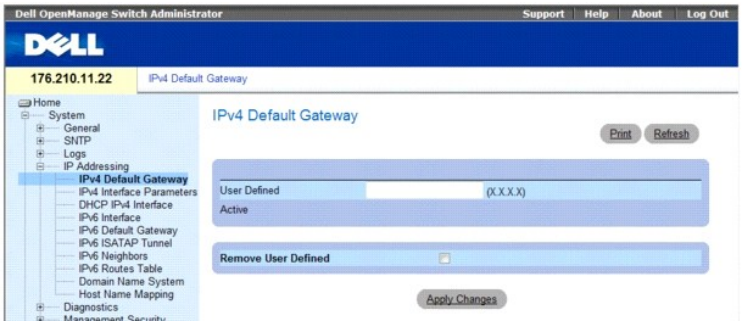
Промежуточный механизм переноса требуется для связи узлов, использующих только систему IPv6, с узлами системы IPv6 по инфраструктуре системы IPv4. Туннельный механизм использует туннельный протокол ISATAP. Этот протокол обрабатывает сеть IPv4 как виртуальную местную связь сети IPv6, при этом каждый адрес системы IPv4 сопоставляется с адресом IPv6 локальной связи.

Определение шлюзов по умолчанию для адресов IPv4

Страница **IPv4 Default Gateway** (Шлюз IPv4 по умолчанию) содержит поля для назначения шлюза устройствам. При отправке пакетов в удаленную сеть пакеты пересылаются на IP-адрес по умолчанию. Настроенный IP-адрес должен принадлежать той же подсети IP-адресов, что и один из IP интерфейсов.

Чтобы открыть страницу **IPv4 Default Gateway** (Шлюз адреса IPv4 по умолчанию), на панели дерева выберите **System** (Система)→ **IP Addressing** (IP-адресация)→ **IPv4 Default Gateway** (Шлюз по умолчанию).

Рис. 6-26. Шлюз адреса IPv4 по умолчанию



Страница **IPv4 Default Gateway** (Шлюз адреса IPv4 по умолчанию) содержит следующие поля:

- **User Defined** (Шлюз по умолчанию, определяемый пользователем). отображает IP-адрес шлюза устройства.
- **Active** (Активен). показывает, что шлюз активен.
- **Remove User Defined** (Удалить определенный пользователем шлюз). удаляет шлюз по умолчанию. Возможные значения:
  - **Флажок установлен**. удаляет выбранный шлюз по умолчанию.
  - **Флажок снят**. оставляет шлюз по умолчанию.

Выбор шлюза IPv4 устройства

1. Откройте страницу **IPv4 Default Gateway** (Шлюз адреса IPv4 по умолчанию).
2. Введите IP-адрес в поле **User Defined** (Определяемый пользователем).
3. Установите флажок **Active** (Активный).
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Будет выбран шлюз устройства по умолчанию, а устройство обновлено.

Удаление шлюза IPv4 устройства по умолчанию

1. Откройте страницу **IPv4 Default Gateway** (Шлюз адреса IPv4 по умолчанию).
2. Установите флажок в поле **Remove User Defined** (Удалить установленный пользователем) для удаления шлюзов по умолчанию.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

   Запись шлюза пол умолчанию будет удалена, а устройство обновлено.

Определение шлюза IPv4 устройства по умолчанию с помощью команд консоли

В следующей таблице приведены команды консоли для настройки полей, отображаемых на странице **Default Gateway** (Шлюз по умолчанию).

Команда консоли	**Описание**
ip default-gateway *ip-адрес*	Определяет шлюз по умолчанию.
no ip default-gateway	Удаляет шлюз по умолчанию.

Далее приведен пример команд консоли.

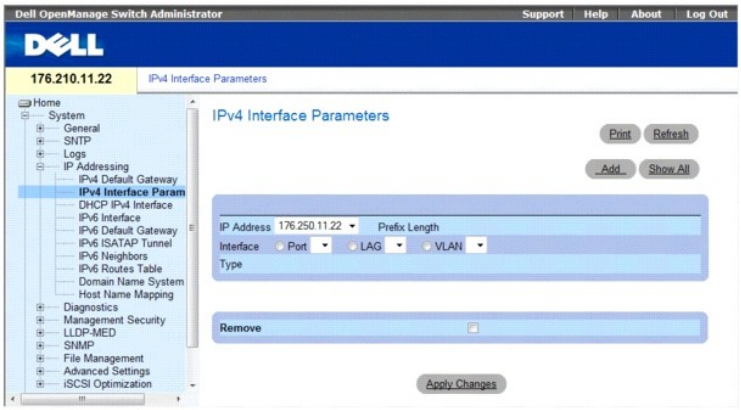
```
console(config)# ip default-gateway 196.210.10.1

console(config)# no ip default-gateway
```

Определение интерфейсов IPv4

Страница **IPv4 Interface Parameters** (Параметры интерфейса IPv4) содержит поля для назначения IP-параметров для интерфейсов.

Чтобы открыть страницу **IPv4 Interface Parameters** (Параметры интерфейса IPv4), выберите **System** (Система)→ **IP Addressing** (IP-адресация)→ **IPv4 Interface Parameters** (Параметры интерфейса IPv4). на панели дерева.

Рис. 6-27. Параметры интерфейса IPv4



Страница IP Interface Parameters (Параметры IP-интерфейса) содержит следующие параметры.

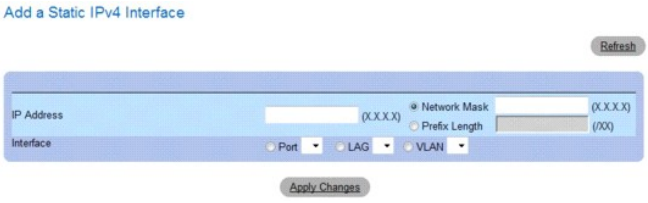
- **IP Address** (IP-адрес). IP-адрес интерфейса.
- **Prefix Length** (Длина префикса). число бит, образующих префикс IP-адреса назначения.
- **Interface** (Интерфейс). тип интерфейса, для которого определен IP-адрес. Выберите **Port** (Порт), **LAG** или **VLAN**.
- **Type** (Тип). показывает, был ли IP-адрес определен как статический.
- **Remove** (Удалить). удаляет интерфейс из падающего меню **IP Address** (IP-адрес).
  - **Флажок установлен**. удаляет выбранный интерфейс.
  - **Флажок снят**. оставляет выбранный интерфейс.

Добавление интерфейса IPv4

1. Откройте страницу **IPv4 Interface Parameters** (Параметры интерфейса IPv4).
2. Нажмите кнопку **Add** (Добавить).

   Откроется страница **Add a Static IPv4 Interface** (Добавление статического интерфейса IPv4):

   Рис. 6-28. Добавление статического интерфейса IPv4

   Помимо параметров, находящихся на странице **IP Interface Parameters** (Параметры IP-интерфейса), страница **Add a Static IP Interface** (Добавить статический IP-интерфейс) содержит следующий параметр:

   - **Network Mask** (Маска сети). определяет маску подсети IP-адреса.

3. Заполните поля на этой странице.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Новый IP-адрес будет добавлен в интерфейс, а устройство обновлено.

Изменение параметров адреса IPv4

1. Откройте страницу **IPv4 Interface Parameters** (Параметры интерфейса IPv4).
2. Выберите IP-адрес в раскрывающемся списке **IP Address** (IP-адрес).
3. Измените тип интерфейса.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Параметры будут изменены, а устройство обновлено.

Удаление адресов IPv4

1. Откройте страницу **IPv4 Interface Parameters** (Параметры интерфейса IPv4).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **Interface Parameters Table** (Таблица параметров интерфейса).

   Рис. 6-29. Таблица параметров интерфейса IPv4

3. Выберите IP-адрес и установите флажок **Remove** (Удалить).
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Выбранный IP-адрес будет удален, а устройство обновлено.

Определение интерфейсов IPv4 с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для установки полей, отображаемых на странице **IPv4 Interfaces Parameters** (Параметры интерфейса IPv4).

Команда консоли	**Описание**
ip address *ip-адрес* {*маска* | *длина_префикса*}	Задает IP-адрес.
no ip address [*ip-адрес*]	Удаляет IP-адрес.
show ip interface [**ethernet** *номер_интерфейса* | **vlan** *идентификатор_vlan* | **port-channel** номер]	Выводит состояние готовности настроенных IP-интерфейсов.

Далее приведен пример команд консоли.

```
Console(config)# interface vlan 1

console(config-if)# ip address 92.168.1.123 255.255.255.0

console(config-if)# no ip address 92.168.1.123

console(config-if)# end

console# show ip interface vlan 1

Gateway IP Address Activity status

--------------------- ------------------

192.168.1.1 Active
```

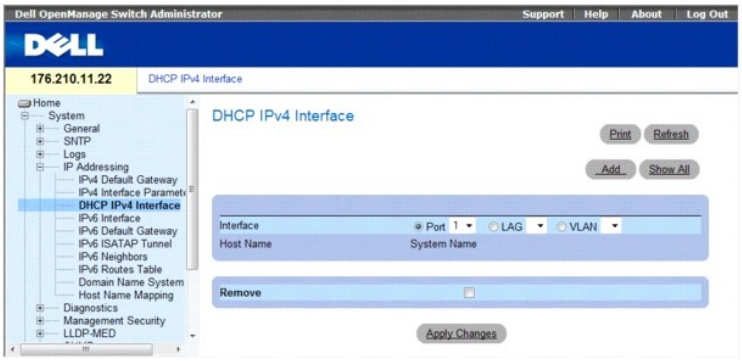
```
IP address Interface Type

------------------ ------------ ------------------

192.168.1.123/24 VLAN 1 Static
```

Определение параметров DHCP интерфейса IPv4

Страница **DHCP IPv4 Interface** (интерфейс IPv4 DHCP) содержит параметры для определения клиентов DHCP, подключенных к устройству.

Чтобы открыть страницу **DHCP IPv4 Interface Parameters** (Интерфейс DHCP IPv4), выберите **System** (Система)→ **IP Addressing** (IP-адресация)→ **DHCP IPv4 Interface** (Интерфейс IPv4). на панели дерева.

Рис. 6-30. IPv4 - интерфейс DHCP



Страница DHCP IP Interface (IP-интерфейс DHCP) содержит следующие поля.

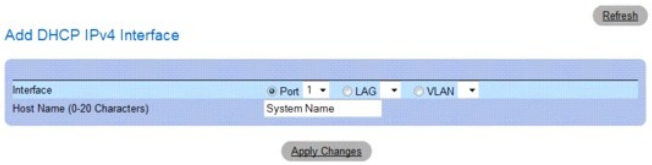
- **Interface** (Интерфейс). Интерфейс клиента DHCP. Нажмите кнопку возле опций **Port**, **LAG**, или **VLAN** и выберите интерфейс клиента DHCP.
- **Host Name** (Имя хоста). системное имя, в том виде, как оно написано в журнале сервера DHCP. Это поле может содержать до 20 символов.
- **Remove** (Удалить). когда установлен этот флажок, клиенты DHCP удаляются.
  - **Флажок установлен**. удаляет выбранный DHCP - клиент.
  - **Флажок снят**. оставляет выбранный DHCP - клиент.

Добавление клиента DHCP

1. Откройте страницу **DHCP IPv4 Interface** (IPv4 интерфейс DHCP).
2. Нажмите кнопку **Add** (Добавить).

   Откроется страница **Add DHCP IPv4 Interface** (Добавить IPv4 интерфейс DHCP).

   Рис. 6-31. Добавление интерфейса DHCP IPv4



3. Введите значения в поля на этой странице.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   IP-интерфейс DHCP будет добавлен, а устройство обновлено.

Изменение IPv4 интерфейса

1. Откройте страницу **DHCP IPv4 IP Interface** (IPv4 интерфейс DHCP).
2. Измените поля.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

   Запись будет изменена, а устройство обновлено.

Удаление IPv4 - интерфейса DHCP

1. Откройте страницу **DHCP IPv4 Interface** (IPv4 интерфейс DHCP).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница с таблицей **DHCP IPv4 Interface Table** (Параметры интерфейса IPv4)

   Рис. 6-32. Таблица DHCP IPv4 интерфейсов

3. Выберите запись клиента DHCP.
4. Установите флажок **Remove** (Удалить).
5. Нажмите кнопку **Apply Changes** (Применить изменения).

   Выбранная запись будет удалена, а устройство обновлено.

Определение IPv4-интерфейсов DHCP с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для определения клиентов DHCP.

Команда консоли	**Описание**
ip address dhcp [**hostname** *имя_хоста*]	Получение IP-адреса для интерфейса Ethernet по протоколу DHCP (Dynamic Host Configuration Protocol).

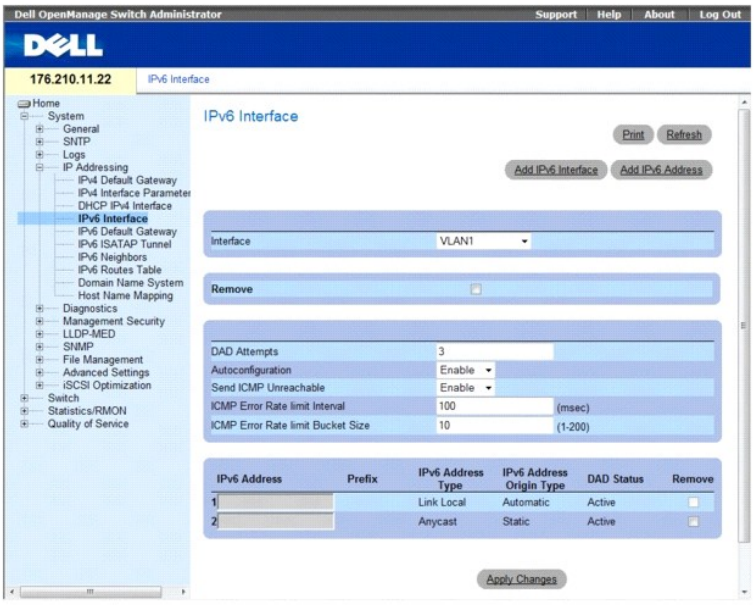
Далее приведен пример команды консоли:

```
console(config)# interface ethernet 1/e11

console(config-if)# ip address dhcp
```

Определение интерфейсов IPv6

Система поддерживает хосты IPv6. Страница **IPv6 Interface Parameters** (Параметры интерфейса IPv6) содержит поля для назначения интерфейсов IPv6. Чтобы открыть страницу **IPv6 Interface** (Интерфейс IPv6), выберите **System** (Система)→ **IP Addressing** (IP-адресация)→ **IPv6 Interface** (Интерфейс IPv6) на панели дерева.

Рис. 6-33. Интерфейс IPv6



- **Interface** (Интерфейс). Интерфейс IPv6, который выбран для настройки.
- **Remove** (Удалить). При выборе этого параметра, происходит удаление атрибутов IPv6 интерфейса.
- **DAD Attempts** (Количество попыток определения уникальности адресов). Определяет количество последовательных сообщений определения уникальности соседних адресов, которые были посланы на интерфейс при работе алгоритма обнаружения дублирующихся адресов (DAD) над адресами одноадресной передачи IPv6 данного интерфейса. Новые адреса остаются в промежуточном состоянии до окончания процесса обнаружения дублирующихся адресов. Если в поле введено значение 0, алгоритм обнаружения дублирующихся адресов на указанном интерфейсе будет отключен. Если в поле введено значение 1, произойдет однократная передача без последующих пересылок. Диапазон значений поля: 0-600, значение по умолчанию: 1.
- **Autoconfiguration** (Автоматическая конфигурация). Указывает, была ли проведена процедура назначения IPv6-адресов интерфейса с помощью автоматической конфигурации, не использующей информацию о состоянии. При включении этой функции, запускается процедура поиска соседних узлов маршрутизатора (предназначенная для определения маршрутизатора для назначения IP-адреса интерфейсу с использованием префиксов, полученных в сообщении автоконфигурации). Если автоконфигурация отключена, автоматическое назначение адресов IPv6 глобальной одноадресной пересылки выполняться не будет, и существующие автоматически назначенные адреса IPv6 глобальной одноадресной пересылки будут удалены из интерфейса. Состояние параметра по умолчанию - *Enabled* (Включено).
- **Send ICMP Unreachable** (Пересылка сообщения о недоступности адреса ICMP). Указывает, включена или выключена передача сообщения «ICMPv6 Address Unreachable». При включении, сообщения о недоступном адресе будут генерироваться для любого пакета, приходящего от интерфейса с неназначенным портом TCP/UDP. Значение по умолчанию - *Enabled* (Включено).
- **ICMP Error Rate Limit Interval** (Интервал ошибки скорости ICMP). Интервал скорости для подачи сообщения об ошибке ICMPv6 в миллисекундах. Значение этого параметра и параметра Bucket Size (см. ниже) определяет, сколько сообщений об ошибке ICMP может быть послано в течение установленного временного интервала. Например, если установлен интервал 100 мс и размер сегмента - 10 сообщений, то в течение 1 секунды может пересылаться до 100 сообщений об ошибке ICMP.
- **ICMP Error Rate Limit Bucket Size** (Размер сегмента сообщений об ошибке ICMP). Устанавливает размер сегмента для сообщений об ошибке ICMPv6. Значение этого параметра и параметра интервала (см. выше) определяет, сколько сообщений об ошибке ICMP может быть послано в течение установленного временного интервала. Например, если установлен интервал 100 мс и размер сегмента - 10 сообщений, то в течение 1 секунды может пересылаться до 100 сообщений об ошибке ICMP. Значение по умолчанию - 100 сообщений об ошибке ICMP в секунду, что соответствует интервалу по умолчанию 100 мс, умноженному на размер сегмента по умолчанию, равный 10.
- **IPv6 Address** (Адрес IPv6). Указывает адрес IPv6, назначенный данному интерфейсу. Адрес должен быть достоверным адресом IPv6, записанным в 16-ричной системе, состоящий из 16-битных величин, разделенных двоеточием. Пример адреса IPv6: 2031:0:130F:0:0:9C0:876A:130D, а в сжатом виде - 2031::0:9C0:876A:130D. Для одного интерфейса может быть установлено до пяти адресов IPv6 (не включая адресов локальной связи), с общим ограничением до 128 адресов на систему.
- **Prefix** (Префикс). Указывает длину префикса адреса IPv6. Длина префикса представляет собой десятичное число, указывающее количество старших смежных битов адреса составляют префикс (сетевой сегмент адреса). Поле префикса применяется только для статических адресов IPv6, определенных как глобальные адреса IPv6.
- **IPv6 Address Type** (Тип адреса IPv6). Указывает способ присоединения IP-адреса к интерфейсу. Возможные значения:
  - **Link Local** (Локальная связь). Адрес локальной связи, который не маршрутизируется, а используется только для связи в пределах той же сети. Адрес локальной связи имеет префикс 'FE80'.
  - **Global Unicast** (Глобальный адрес одноадресной передачи). Указывает, что IP-адрес является глобальным уникальным адресом одноадресной пересылки системы IPv6; он является видимым и доступным из других подсетей.
  - **Global Anycast** (Глобальный адрес произвольной адресации). Указывает, что IP-адрес является глобальным уникальным адресом для произвольной адресации в системе IPv6; он является видимым и доступным из других подсетей.
  - **Multicast** (Многоадресный). Указывает, что данный IP-адрес является многоадресным.
- **IPv6 Address Origin Type** (Тип происхождения адреса IPv6). Определяет тип конфигурируемого статического IPv6-адреса интерфейса. Возможные значения:
  - **Dynamic** (Динамический). Указывает, что адрес получен от системы автоматической конфигурации.
  - **Static** (Статический). Показывает, что конфигурация адреса произведена пользователем.
  - **System** (система). Показывает, что IP-адрес был генерирован системой.

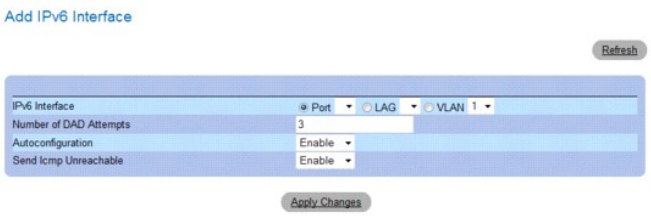
- **DAD Status** (состояние алгоритма DAD). Отображает статус системы автоматического обнаружения дублирующихся адресов (DAD), которая определяет уникальность введенных адресов IPv6. Этот параметр представляет собой параметр только для чтения, значения полей которого таковы:
  - **Tentative** (Временный). Указывает, что система находится в процессе определения дублирующихся адресов IPv6.
  - **Duplicate** (Дублирование). Указывает, что адрес IPv6 уже используется другим хостом сети. Дублирующийся адрес IPv6 блокируется и не используется в дальнейшем для пересылки и получения трафика.
  - **Active** (Работает). Указывает, что IPv6 находится в рабочем состоянии.
- **Remove** (Удаление). Если выбрана эта опция, происходит удаление адреса из таблицы.

Добавление интерфейса IPv6

1. Откройте страницу **IPv6 Interface** (Интерфейс IPv6).
2. Выберите **Add IPv6 Interface** (Добавить интерфейс IPv6).

   Откроется с траница **Add a Static IPv6 Interface** (Добавление статического интерфейса IPv6).

   Рис. 6-34. Добавление интерфейса IPv6



3. Заполните поля на этой странице.

   IPv6 Interface (Интерфейс IPv6) указывает, является ли данный интерфейс портом, LAG или VLAN.

4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Новый интерфейс будет добавлен, а устройство обновлено.

Добавление адреса IPv6 к текущему интерфейсу

1. Откройте страницу **IPv6 Interface** (Интерфейс IPv6).
2. Выберите **Add IPv6 Address** (Добавить интерфейс IPv6).

   Откроется страница **Add IPv6 Address** (Добавление адреса IPv6):

   Рис. 6-35. Добавление адреса IPv6

3. Заполните поля на этой странице.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Новый адрес будет добавлен и устройство обновлено.

Изменение параметров интерфейса IPv6

1. Откройте страницу **IPv6 Interface** (Интерфейс IPv6).
2. Выберите интерфейс в раскрывающемся меню **Interface** (Интерфейс).
3. Измените необходимые поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Параметры будут изменены, а устройство обновлено.

Определение интерфейсов IPv6 с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для настройки полей, отображаемых на странице **IPv6 Interface** (Интерфейс IPv6).

Команда консоли	Описание
ipv6 enable [**нет автоконфигурации**]	Включает обработку IPv6 интерфейса.
ipv6 address autoconfig	Включает автоматическую конфигурацию адресов IPv6 с использованием автоконфигурации, не учитывающей состояние интерфейса.
ipv6 icmp error-interval *миллисекунды* [*bucketsize*]	Конфигурирует параметры предельного интервала и размера сегмента для протокола управляющих интернет-сообщений (ICMP) для сообщений об ошибках IPv6.
show ipv6 icmp error-interval	Отображает интервал подачи сообщений об ошибках ipv6 icmp error interval.
ipv6 address *ipv6-address/prefix-length* [**eui-64**] [**anycast**]	Конфигурирует адрес IPv6 интерфейса.
ipv6 address *ipv6-address* **link-local**	Конфигурирует адрес локальной связи IPv6 интерфейса.
ipv6 unreachables	Включает генерирование сообщений протокола ICMP для IPv6 (ICMPv6) о недоступном адресе для пакетов, поступающих на указанный интерфейс.
show ipv6 interface [ethernet *номер_интерфейса* | **vlan** *идентификатор_vlan* | **port-channel** *номер*]	Выводит состояние готовности настроенных интерфейсов IPv6.
ipv6 nd dad attempts *кол-во_попыток*	Устанавливает количество последовательных сообщений определения уникальности соседних адресов, которые были посланы на интерфейс при работе алгоритма обнаружения дублирующихся адресов (DAD) над адресами одноадресной передачи IPv6 данного интерфейса.
ipv6 host *name ipv6-address1 [ipv6-address2...ipv6-address4]*	Определяет соответствие статических имен хостов адресам в кэше имен хоста.
ipv6 set mtu {**ethernet** *interface* | **port-channel** *port-channel-number} { bytes* | ***default***}	Устанавливает максимальный размер пакета (МРП) для пакетов данных IPv6, пересылаемых на интерфейс.
ping {*ipv4-address* | *hostname*} [**size** *packet_size*] [**count** *packet_count*] [**timeout** *time_out*]	Пересылает пакеты эхо-запросов IPv4 ICMP на другой узел сети.
ping ipv6 {*ipv6-address* | *hostname*} [**size** *packet_size*] [**count** *packet_count*] [**timeout** *time_out*]	Пересылает пакеты эхо-запросов IPv6 ICMP на другой узел сети.

Далее приведен пример команд консоли.

```
console# show ipv6 interface vlan 1

Number of ND DAD attempts (Количество попыток ND DAD): 1

MTU size (Размер пакета МРП): 1500

Stateless Address Autoconfiguration state (Состояние автоконфигурации адреса без учета состояния адреса): enabled

ICMP unreachable message state (Состояние сообщения о недоступности адреса): enabled

MLD version (Версия MLD): 2


IP addresses (IP-адреса)          Type (Тип)      DAD State (Наличие дублирующихся адресов)

------------------------ ------    -----------

fe80::232:87ff:fe08:1700 linklayer Active

ff02::1                  linklayer N/A

ff02::1:ff08:1700        linklayer N/A
```

```
console(config)# ipv6 icmp

Ограничение интервала пересылки сообщений об ошибке ICMP

console(config)# ipv6 icmp error-interval

<0-2147483647> Временной интервал между ярлыками, установленными в сегменте, в миллисекундах

console(config)# ipv6 icmp error-interval 100

<1-200>      Максимальное количество ярлыков, сохраненных в сегменте
```

Определение шлюзов по умолчанию для адресов IPv6

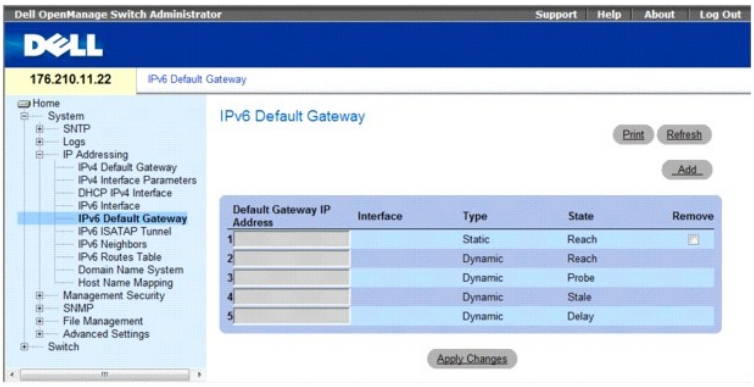
Страница **IPv6 Default Gateway** (Шлюзы IPv6 по умолчанию) позволяет произвести ручную настройку маршрутизатора для трафика по всем связям. Адрес шлюза по умолчанию - это интерфейс, который служит точкой доступа к другой сети. Для IPv6, конфигурация шлюза по умолчанию не является обязательной, поскольку хосты могут автоматически определять существование маршрутизатора локальной сети благодаря процедуре обнаружения маршрутизатора.

В отличие от системы IPv4, шлюз по умолчанию для системы IPv6 может иметь несколько адресов IPv6, которые могут включать один статический адрес, определяемый пользователем и несколько динамических адресов, определяемых при подаче сообщения определения маршрутизатора. Шлюз, определяемый пользователем, имеет более высокий приоритет над автоматически определяемым маршрутизатором.

- При удалении IP-интерфейса, все IP-адреса, определенные для него по умолчанию, также удаляются.
- Динамические IP-адреса удаляться не могут.
- Предупреждающее сообщение будет выводиться при попытке пользователя вставить более одного пользовательского адреса.
- При попытке вставить адрес другого типа, нежели адрес местной связи, будет выводится предупреждающее сообщение.

Чтобы открыть страницу **IPv6 Default Gateway** (Шлюз адреса IPv6 по умолчанию), выберите **System** (Система)→ **IP Addressing** (IP-адресация)→ **IPv6 Default Gateway** (Шлюз адреса IPv6 по умолчанию) на панели дерева.

Рис. 6-36. Шлюз адреса IPv6 по умолчанию



- **Default Gateway IP Address** (IP-адрес шлюза по умолчанию). Отображает IPv6 - адрес локальной связи для шлюза по умолчанию.
- **Interface** (Интерфейс). Указывает исходящий интерфейс, через который осуществляется доступ к шлюзу по умолчанию. К интерфейсу может относиться любой порт//LAG/VLAN и/или тоннель.
- **Type** (Тип). Указывает способ, которым конфигурируется шлюз по умолчанию. Возможные значения:
  - **Static** (статический). Показывает, что шлюз по умолчанию определяется пользователем.
  - **Dynamic** (динамический). Указывает, что шлюз был сконфигурирован динамически.
- **State** (Статус). Отображает статус шлюза по умолчанию. Возможные значения:
  - **Incomplete** (Не закончено). Указывает, что процесс определения адреса еще идет, и адрес канального уровня шлюза по умолчанию еще не был определен.
  - **Reachable** (Доступен). Указывает, что шлюз по умолчанию определен и доступен (по состоянию на несколько десятков секунд до настоящего момента).
  - **Stale** (Устаревший). Указывает, что шлюз по умолчанию больше не считается доступным, но, до тех пор, пока не будет пересылки трафика к шлюзу по умолчанию, не было предпринято попыток определить его доступность.
  - **Delay** (Задержка). Указывает, что шлюз по умолчанию более не рассматривается как доступный, и по шлюзу, установленному по умолчанию, был отправлен трафик. Имеется кратковременная задержка в отсылке тестовых импульсов для того, чтобы протоколы верхнего уровня смогли собрать информацию о доступности шлюза.

- **Probe** (Тестовый сигнал). Указывает, что шлюз по умолчанию более не рассматривается в качестве доступного, и для проверки его доступности посылаются тестовые сигналы одноадресной передачи определения соседних адресов.
- **Unreachable** (Недоступен). Указывает, что подтверждение доступности шлюза получено не было.

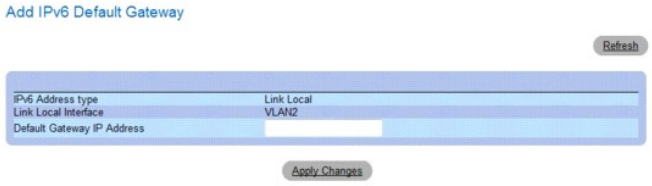
- **Remove** (Удаление). Если выбрана эта опция, происходит удаление адреса из списка.

Добавление шлюза по умолчанию для адресов IPv6

1. Откройте страницу **IPv6 Default Gateway** (Шлюз адреса IPv6 по умолчанию).
2. Нажмите кнопку **Add** (Добавить).

   Откроется страница **Add IPv6 Default Gateway** (Добавить шлюз адреса IPv6 по умолчанию):

   Рис. 6-37. Добавление шлюза адреса IPv6 по умолчанию



3. Заполните поля на этой странице.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Новый шлюз будет добавлен, а устройство обновлено.

Определение параметров шлюза IPv6 по умолчанию с помощью команд консоли

В следующей таблице приведены команды консоли для настройки полей, отображаемых на странице **IPv6 Default Gateway** (Шлюз адреса IPv6 по умолчанию).

Команда консоли	**Описание**
ipv6 default-gateway *ipv6-адрес*	Определяет шлюз IPv6 по умолчанию.

Определение туннелей IPv6 ISATAP

Страница **IPv6 ISATAP Tunnel** (Туннель IPv6 ISATAP) определяет процесс туннелирования устройства, которое формирует пакеты IPv6 и вставляет их в пакеты IPv4 для пересылки по сети IPv4.

Протокол внутрисайтовой автоматической туннельной адресации *(ISATAP)* представляет собой механизм переноса IPv6, который определяется как туннельный интерфейс IPv6 и предназначен для передачи пакетов IPv6 между двухстековыми узлами поверх сети IPv4.

При включении протокола ISATAP на туннельном интерфейсе, формируется конкретный IP-адрес, поскольку источник туннелирования или автоматический узел существует там, где IP-интерфейсу сопоставлен IPv4 - адрес с самым меньшим номером. Этот источник IPv4 используется для установки идентификатора туннельного интерфейса, в соответствии с правилами адресации протокола ISATAP. Если для протокола ISATAP включен туннельный интерфейс, для интерфейса необходимо указать источник туннелирования, чтобы этот интерфейс стал активным.

Адрес ISATAP представляется в следующем виде: [64-битный префикс]:0:5EFE:w.x.y.z, где 5EFE является идентификатором ISATAP, а w.x.y.z - публичные или частные адреса IPv4. Таким образом, адрес локальной связи Link Local может быть представлен в виде FE80::5EFE:w.x.y.z

После удаления последнего IPv4-адреса с интерфейса, интерфейс ISATAP IP принимает негативное состояние и отображается как «отключенный», однако, при этом администрирование остается включенным.

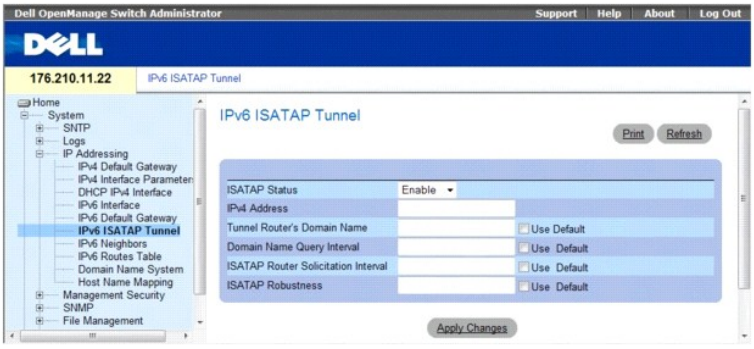
При определении туннелирования, необходимо принимать во внимание следующее:

- Адрес локальной связи IPv6 назначается интерфейсу ISATAP. Первоначальный IP-адрес назначается этому интерфейсу, и интерфейс принимает активное состояние.
- Если интерфейс ISATAP является активным, IPv4 - адрес маршрутизатора ISATAP определяется системой DNS путем использования преобразования данных ISATAP - IPv4. Если запись ISATAP DNS не обнаружена, то начнется поиск преобразования данных ISATAP-имя хоста-адрес в кэше имен хоста.
- Если при процессе DNS адрес IPv4 маршрутизатора ISATAP не был определен, состояние интерфейса ISATAP IP остается *Активным*. Система не получит шлюз по умолчанию для трафика ISATAP до тех пор, пока процедура определения DNS не будет закончена.

- Для того, чтобы туннелирование по протоколу ISATAP работало правильно по сети IPv4, необходимо произвести установку маршрутизатора ISATAP.

Чтобы открыть страницу **IPv6 ISATAP Tunnel** (Туннелирование IPv6 ISATAP), выберите **System** (Система)→ **IP Addressing** (IP-адресация)→ **IPv6 ISATAP Tunnel** (Туннелирование IPv6 ISATAP) на панели дерева.

Рис. 6-38. Туннелирование IPv6 ISATAP



- **ISATAP Status** (Состояние ISATAP). Определяет состояние работы протокола ISATAP устройства. Возможные значения:
  - **Enable** (Включено). Работа протокола ISATAP на устройстве включена.
  - **Disable** (Выключено). Работа протокола ISATAP на устройстве выключена. Это значение по умолчанию.
- **IPv4 Address** (адрес IPv4). Указывает локальный адрес (источник) IPv4 туннельного интерфейса.
- **Tunnel Router's Domain Name** (Имя домена туннельного маршрутизатора). Указывает глобальное текстовое значение, которое представляет собой конкретное имя домена маршрутизатора автоматического туннелирования. По умолчанию установлено имя ISATAP.
  - **Use Default** (Использовать стандартные установки). Установка флажка на этой опии возвращает стандартные значения параметров установок.
- **Domain Name Query Interval** (Интервал запроса доменного имени). Определяет интервал между запросами системы DNS (перед определением IP-адреса маршрутизатора ISATAP), посылаемыми для автоматического определения доменного имени маршрутизатора автоматического туннелирования. Диапазон значений: 10 - 3600 секунд. Значение по умолчанию: 10 секунд.
  - **Use Default** (Использовать стандартные установки). Установка флажка на этой опии возвращает стандартные значения параметров установок.
- **ISATAP Router Solicitation Interval** (Интервал запросов маршрутизатора ISATAP). Указывает интервал между посылкой сообщений-запросов маршрутизатора, в случае отсутствия активного маршрутизатора. Диапазон значений: 10 - 3600 секунд. Значение по умолчанию:10.
  - **Use Default** (Использовать стандартные установки). Установка флажка на этой опии возвращает стандартные значения параметров установок.
- **ISATAP Robustness** (Надежность ISATAP). Указывает количество обновлений запросов DNS/ запросов маршрутизатора, которые пересылает устройство. Диапазон значений: 1 - 20 секунд. Значение по умолчанию: 3.
  - **Use Default** (Использовать стандартные установки). Установка флажка на этой опии возвращает стандартные значения параметров установок.

Определение параметров туннельного протокола с помощью команд консоли

В следующей таблице приведены команды консоли для настройки полей, отображаемых на странице **IPv6 ISATAP Tunnel** (Туннелирование IPv6 ISATAP).

Команда консоли	**Описание**
interface tunnel (туннель интерфейса) *number (номер)*	Вход в режим конфигурирования туннельного интерфейса.
tunnel mode ipv6ip {isatap}	Конфигурирует глобальный режим механизма переноса данных IPv6.
tunnel isatap router *router_name*	Конфигурирует глобальную строку, которая содержит доменное имя конкретного автоматического туннельного маршрутизатора.
tunnel source { auto | ip-address *ipv4-address | interface }*	Указывает локальный адрес (источник) IPv4 туннельного интерфейса.
tunnel isatap query-interval (интервал запросов туннеля ISATAP) *seconds (секунды)*	Определяет интервал между запросами системы DNS (перед определением IP-адреса маршрутизатора ISATAP), посылаемыми для автоматического определения доменного имени маршрутизатора автоматического туннелирования.
tunnel isatap solicitation-interval (интервал ответных сообщений на запросы туннеля ISATAP) *seconds (ctreyls)*	Указывает интервал между посылкой ответных сообщений на запросы маршрутизатора, в случае отсутствия активного маршрутизатора.
tunnel isatap robustness (надежность туннеля) *number (число)*	Указывает количество обновлении запросов DNS/ запросов маршрутизатора, которые пересылает устройство.

show ipv6 tunnel (показать туннель ipv6)	Выводит информацию о туннеле ISATAP.

Далее приведен пример команд консоли.

```
Console> show ipv6 tunnel

Router DNS name (Имя DNS маршрутизатора): ISATAP

Router IPv4 address (Адрес IPv4 маршрутизатора): 172.16.1.1

DNS Query interval (интервал между запросами DNS): 10 секунд

Min DNS Query interval (Минимальный интервал между запросами DNS): 0 секунд

Router Solicitation interval (интервал ответов на запрос маршрутизатора): 10 секунд

Min Router Solicitation interval (Минимальный интервал ответов на запрос
маршрутизатора): 0 секунд

Robustness (Надежность): 3
```

Defining IPv6 Neighbors (Определение соседних узлов IPv6)

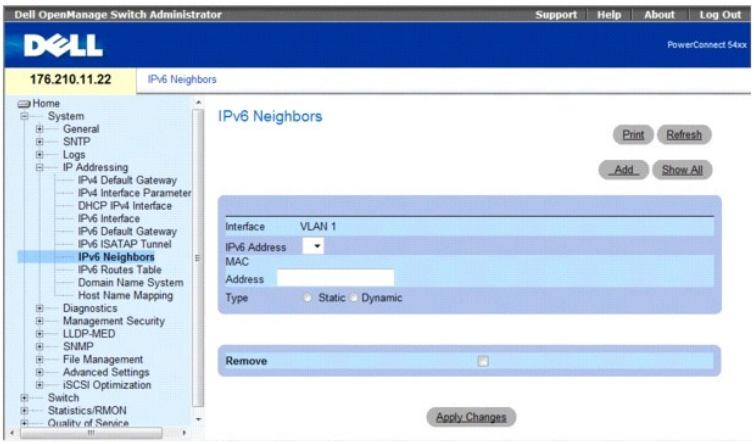
Страница **IPv6 Neighbors** (Соседние узлы IPv6) содержит информацию об определении соседних узлов IPv6, которая по своим функциональным свойствам аналогична странице *IPv4 Address Resolution Protocol (ARP)* (Протокол определения адреса IPv4). Функция поиска соседних узлов IPv6 позволяет определить адреса локальных связей в пределах одной подсети и содержит базу данных для регистрации и поддержки информации о доступности путей к активным соседним узлам.

Устройство поддерживает до 256 соседних узлов, полученных статически или динамически.

При удалении интерфейса, все соседние узлы, определенные статически и динамически, будут также удалены.

Чтобы открыть страницу **IPv6 Neighbors** (Соседние узлы IPv6), выберите **System** (система)→ **IP Addressing** (IP-адресация)→ **IPv6 Neighbors** (Соседние узлы IPv6) на панели дерева.

Рис. 6-39. Соседние узлы IPv6



- **Interface** (Интерфейс). Отображает интерфейс, на котором определен интерфейс IPv6. В качестве интерфейсов могут использоваться порты, LAG или VLAN.
- **IPv6 Address** (Адрес IPv6). Определяет IPv6-адрес соседнего узла, который конфигурируется в данный момент.
- **MAC Address** (MAC-адрес). Отображает MAC-адрес, назначенный данному интерфейсу.
- **Type** (Тип). Отображает тип записи кэша при определении соседнего узла. Возможные значения:
  - **Static** (Статический). Показывает записи кэша статических соседних адресов. Если запись для конкретного IPv6-адреса уже существует в кэше данных по определению соседних узлов — это определяется в процессе поиска соседних узлов IPv6, — то вы можете преобразовать эту запись в статическую.
  - **Dynamic** (динамический). Показывает записи кэша динамических соседних адресов.
- **Remove** (удаление). Если выбрана эта опция, происходит удаление соседнего адреса из списка.

В таблице соседних узлов IPv6, также имеются следующие параметры:

State (Состояние). Отображает состояние соседнего узла IPv6. Возможные значения этого поля:

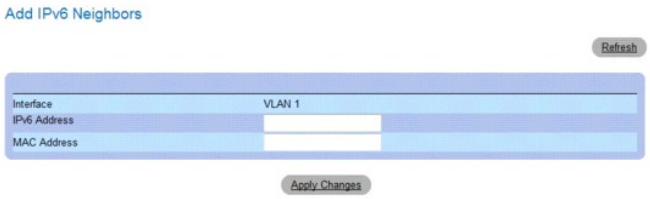
- **Incomplete** (Не закончено). Указывает, что процесс определения адреса еще идет, и адрес канального уровня соседнего узла по умолчанию еще не был определен.
- **Reachable** (Доступен). Указывает, что соседний узел определен и доступен (по состоянию на несколько десятков секунд до настоящего момента).
- **State** (Состояние). Указывает, что соседний узел больше не считается доступным, но до тех пор, пока не было пересылки трафика к соседнему узлу, не было предпринято попыток определить его доступность.
  - **Delay** (Задержка). Указывает, что соседний узел более не рассматривается как доступный, и к соседнему узлу был послан трафик. Имеется кратковременная задержка в отсылке тестовых импульсов для того, чтобы протоколы верхнего уровня смогли собрать информацию о доступности соседнего узла.
  - **Probe** (Тестовый сигнал). Указывает, что соседний узел более не рассматривается в качестве доступного, и для проверки его доступности посылаются тестовые сигналы-запросы одноадресной передачи определения соседних узлов.

Добавление соседнего узла IPv6

1. Откройте страницу **IPv6 Neighbors** (Соседние узлы IPv6).
2. Нажмите кнопку **Add** (Добавить).

   Откроется страница **Add IPv6 Neighbors** (добавить соседние узлы IPv6) .

   Рис. 6-40. Добавление соседних узлов IPv6



3. Заполните поля на этой странице.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Новый соседний узел будет добавлен, а устройство обновлено.

Изменение параметров соседнего узла

1. Откройте страницу **IPv6 Neighbors** (Соседние узлы IPv6).
2. Выберите IP-адрес в раскрывающемся списке **IPv6 Address** (Адрес IPv6).
3. Измените необходимые поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

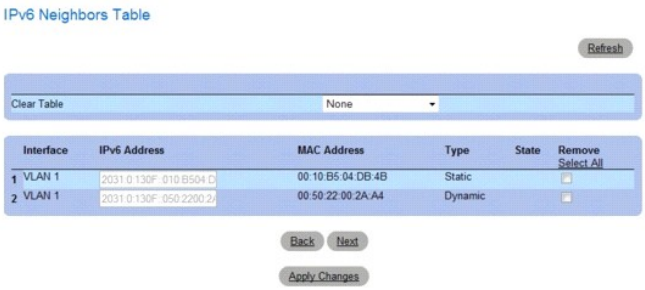
   Параметры будут изменены, а устройство обновлено.

Удаление соседних узлов

1. Откройте страницу **IPv6 Neighbors** (Соседние узлы IPv6).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **IPv6 Neighbors Table** (Таблица соседних узлов IPv6).

   Рис. 6-41. Таблица соседних узлов IPv6



3. Поставьте флажок на опии **Remove** (Удалить) возле нужного узла. Другой способ - выберите нужное значение в поле **Clear Table** (Очистить таблицу). Возможные значения:
   - Static Only (Только статические) — Удаляет записи для статических узлов таблицы соседних узлов IPv6.
   - Dynamic Only (Только динамические) — Удаляет записи для динамических узлов таблицы соседних узлов IPv6
   - All Dynamic and Static (Динамические и статические) — Удаляет все записи (статические и динамические) из таблицы соседних узлов IPv6.
   - None (Не удалять) — Отмена удаления записей.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Выбранные соседние узлы будут удалены, а устройство обновлено.

Определение соседних узлов IPv6 с помощью команд консоли

В следующей таблице приведены команды консоли для настройки полей, отображаемых на странице **IPv6 Neighbors** (Соседние узлы IPv6).

Команда консоли	**Описание**
ipv6 neighbor *ipv6_addr hw_addr* {**ethernet** *interface-number* | **vlan** *vlan-id* | **port-channel** *number* }	Конфигурирует статистические записи кэша обнаружения соседних узлов IPv6.
show ipv6 neighbors {static | dynamic}[**ipv6-address** *ipv6-address*] [**mac-address** *mac-address*] [**ethernet** *interface-number* | **vlan** *vlan-id* | **port-channel** *number*]	Отображает информацию из кэша обнаружения соседних узлов IPv6.
clear ipv6 neighbors	Удаляет все записи из кэша обнаружения соседних узлов.

Далее приведен пример команд консоли.

```
Console# show ipv6 neighbors dynamic

Interface (Интерфейс)  IPv6 address (Адрес IPv6)              HW address (Аппаратный
адрес)      State (состояние)

---------  ------------             ----------       -----

VLAN 1     2031:0:130F::010:B504:DBB4   00:10:B5:04:DB:4B  REACH

VLAN 1     2031:0:130F::050:2200:2AA4   00:50:22:00:2A:A4  REACH
```

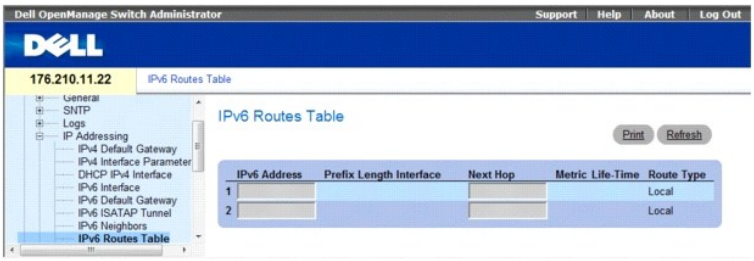
Просмотр таблицы маршрутов IPv6

Таблица маршрутов IPv6 (**IPv6 Routes Table**) хранит информацию о префиксах назначения адресов IPv6, и способе доступа к ним (прямом или косвенном). Таблица маршрутизации используется для определения адресов следующего скачка и интерфейса, используемого для переадресации.

Каждая динамическая запись имеет ассоциированное значение таймера недействительности (взятое из оповещения маршрутизатора), используемое для удаления записей, которые более не отображаются в оповещении.

Чтобы открыть страницу **IPv6 Routes Table** (Таблица маршрутов IPv6), выберите **System** (Система)→ **IP Addressing** (IP-адресация)→ **IPv6 Routes Table** (Таблица маршрутов IPv6) на панели дерева.

Рис. 6-42. Таблица маршрутов IPv6



- **IPv6 Address** (Адрес IPv6). Определяет IPv6-адрес назначения.
- **Prefix Length** (Длина префикса). Указывает длину префикса адреса IPv6. Поле префикса применяется только для статических адресов IPv6, определенных как глобальные адреса IPv6. Диапазон значений: 5 -128.
- **Interface** (Интерфейс). Отображает интерфейс, который используется для переадресации пакета. К интерфейсу может относиться любой порт/LAG/VLAN.
- **Next Hop** (Следующий скачок). Определяет адрес, к которому переадресуется пакет, направленный по маршруту к адресу назначения (обычно это адрес соседнего маршрутизатора). В качестве этого адреса могут использоваться адреса локальной связи или глобальные IPv6-адреса.
- **Metric** (Метрика). Указывает величину, используемую при сравнении этого маршрута с другими маршрутами с тем же местом назначения, находящимися в таблице маршрутизации IPv6. Это администрируемый параметр, с диапазоном изменения от 0 до 255. Значение по умолчанию - 1.
- **Life-Time** (Срок службы) — Указывает срок службы маршрута.
- **Route Type** (Тип маршрута). Указывает, напрямую ли указано место назначения и способ определения этой записи. Возможны следующие значения::
  - **Local** (Локальный). Указывает прямую связь с записью маршрута.
  - **Static** (Статический). Указывает, что маршрут определен при работе процесса определения соседних узлов. Эта запись автоматически преобразуется в статическую запись.
  - **ICMP**. Указывает, что маршрут получен из сообщений ICMP.
  - **ND**. Указывает, что маршрут получен из сообщений алгоритма автоконфигурации.

Просмотр таблицы параметров маршрутизации IPv6 с помощью команд консоли

В следующей таблице приведены команды консоли для настройки полей, отображаемых на странице **IPv6 Routes Table** (Таблица маршрутов IPv6).

Команда консоли	Описание
traceroute {*ipv4-address* | *hostname*} [size *packet_size*] [ttl *max-ttl*] [**count** *packet_count*] [**timeout** *time_out*] [**source** *ip-address*] [**tos** *tos*]	Определяет маршруты, которые действительно принимают пакеты IPv4 при движении к месту назначения.
traceroute ipv6 {*ipv6-address* | *hostname*} [**size** *packet_size*] [**ttl** *max-ttl*] [**count** *packet_count*] [**timeout** *time_out*] [**source** *ip-address*] [**tos** *tos*]	Определяет маршруты, которые действительно принимают пакеты IPv6 при движении к месту назначения.
show ipv6 route	Отображает текущее состояние таблицы маршрутов IPv6.

Далее приведен пример команд консоли.

```
Console> show ipv6 route

Коды: L - Локальный, S - Статический, I - ICMP, ND - Оповещение маршрутизатора

Число в скобках представляет метрику.

S ::/0 via fe80::77 [0] VLAN 1 Lifetime Infinite (Срок службы неограничен)

ND ::/0 via fe80::200:cff:fe4a:dfa8 [0] VLAN 1 Lifetime 1784 sec (срок службы 1784 с)

L 2001::/64 прямое соединение g2 Lifetime Infinite (Срок службы неограничен)

L 2002:1:1:1::/64 прямое соединение, VLAN 1 Lifetime (Срок службы) 2147467 с

L 3001::/64 прямое соединение, VLAN 1 Lifetime Infinite (Срок службы неограничен)

L 4004::/64 прямое соединение, VLAN 1 Lifetime Infinite (Срок службы неограничен)

L 6001::/64 прямое соединение, g2 Lifetime Infinite (Срок службы неограничен
```

Настройка системы имен доменов

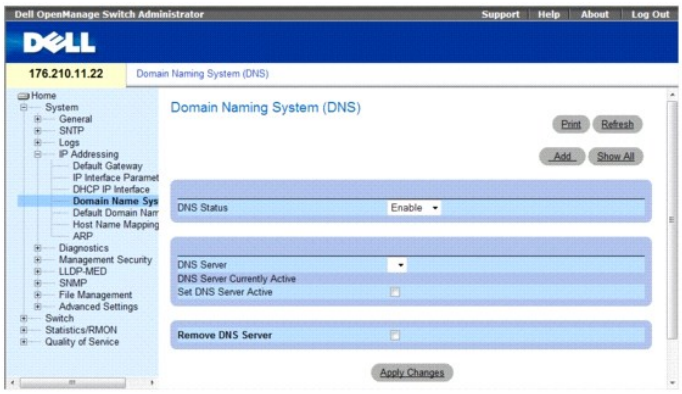
Система имен доменов (DNS) преобразует имена доменов, определенные пользователем, в IP-адреса. Каждый раз при назначении имени домена

служба DNS переводит имя в числовой IP-адрес. Например, **www.ipexample.com** переводится в 192.87.56.2. Серверы DNS ведут базы данных имен доменов и соответствующие им IP-адреса.

Страница **Domain Naming System (DNS)** (Система имен доменов) содержит поля для включения и активизации определенных серверов DNS.

Чтобы открыть страницу Domain Naming System (DNS) (Система имен доменов), выберите System (Система)→ IP Addressing (IP-адресация)→ Domain Name System (Система имен доменов) на панели дерева.

Рис. 6-43. Система имен доменов



Страница **Domain Naming System (DNS)** (Система имен доменов) содержит следующие поля.

- **DNS Status** (Состояние DNS). включает или отключает перевод имен DNS в IP-адреса.
- **DNS Server** (Сервер DNS). содержит список серверов DNS. Серверы DNS добавляются со страницы **Add DNS Server** (Добавление сервера DNS).
- **DNS Server Currently Active** (Сервер DNS в настоящее время активен). сервер DNS, который в настоящее время является активным сервером DNS.
- **Set DNS Server Active** (Сделать сервер DNS активным). активизирует выбранный сервер DNS.
- **Remove DNS Server** (Удалить сервер DNS). удаляет выбранный сервер DNS.
  - **Флажок установлен**. удаляет выбранный DNS сервер.
  - **Флажок снят** . оставляет выбранный сервер DNS.

При определении нового сервера DNS, будут доступны следующие дополнительные параметры:

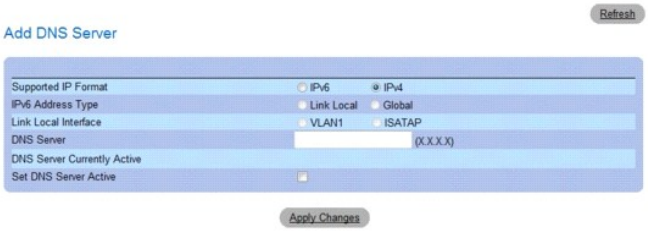
- **Supported IP Format** (Поддерживаемый формат IP-адресов). Отображает формат IP-адресов, поддерживаемый сервером SNTP. Возможные значения:
  - **IPv6**. поддержка IP версии 6.
  - **IPv4**. поддержка IP версии 4.
- **IPv6 Address Type**. В случае, если сервер поддерживает систему IPv6 (см. предыдущий параметр), здесь указывается поддерживаемый тип статических адресов. Возможные значения:
  - **Link Local** (Локальная связь). Адрес локальной связи, который не маршрутизируется, а используется только для связи в пределах той же сети.
  - **Global** (Глобальный). Глобальный уникальный адрес IPv6 address; он является видимым и доступным для различных подсетей.
- **Link Local Interface** (Интерфейс локальной связи). Если сервер поддерживает систему адресов локальной связи IPv6 (см. предыдущий параметр), здесь указывается интерфейс локальной связи. Возможные значения:
  - **VLAN1**. Интерфейс IPv6 конфигурируется по сети VLAN1.
  - **ISATAP**. Интерфейс IPv6 конфигурируется по туннелю ISATAP.

Добавление сервера DNS

1. Откройте страницу **Domain Naming System (DNS)** (Система имен доменов).
2. Нажмите кнопку **Add** (Добавить).

   Откроется страница **Add DNS Server** (Добавление сервера DNS).

   Рис. 6-44. Страница Add DNS Server (Добавление сервера DNS)



Помимо полей страницы **Domain Naming System (DNS)** (система доменных имен DNS), страница **Add DNS Server** (Добавить DNS - сервер) содержит следующее поле:

- **DNS Server** (Сервер DNS). IP-адрес сервера DNS.

3. Определите соответствующие поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Будет определен новый сервер DNS, а устройство обновлено.

Отображение таблицы серверов DNS

1. Откройте страницу **Domain Naming System (DNS)** (Система имен доменов).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **DNS Server Table** (Таблица серверов DNS).

   Рис. 6-45. Таблица DNS Server Table (Таблица серверов DNS)

Удаление серверов DNS

1. Откройте страницу **Domain Naming System (DNS)** (Система имен доменов).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **DNS Server Table** (Таблица серверов DNS).

3. Выберите запись **DNS Server Table** (Таблица серверов DNS).
4. Установите флажок **Remove** (Удалить).
5. Нажмите кнопку **Apply Changes** (Применить изменения).

Выбранный сервер DNS будет удален, а устройство обновлено.

Настройка серверов DNS с помощью команд консоли

В следующей таблице приведены команды консоли для настройки системной информации устройства.

Команда консоли	**Описание**
ip name-server *адрес_сервера*	Задает доступные имена серверов. Можно определить до восьми имен серверов.

no ip name-server *адрес_сервера*	Удаляет имя сервера.
ip domain-name *имя*	Определяет имя домена по умолчанию, которое используется программой, если имена хостов указаны неправильно.
clear host {имя | *}	Удаляет записи из кэша имя хоста-адрес.
show hosts [*имя*]	Отображает имя домена по умолчанию, список хостов сервера имен, статические имена и адреса, а также список имен и адресов из кэша.
ip domain-lookup	Включает систему DNS для преобразования имен хостов в IP-адреса.

Далее приведен пример команд консоли.

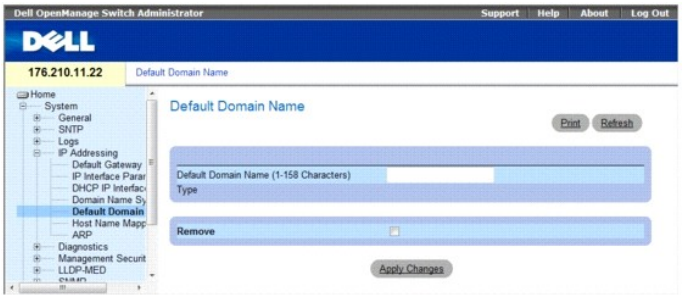
```
console (config)# ip name-server 176.16.1.18
```

Определение доменов по умолчанию

Страница **Default Domain Name** (Имя домена по умолчанию) содержит сведения для определения имен доменов DNS по умолчанию.

Чтобы открыть страницу **Default Domain Name** (Имя домена по умолчанию), выберите **System** (Система)→ **IP Addressing** (IP-адресация)→ **Default Domain Name** (Имя домена по умолчанию) на панели дерева.

Рис. 6-46. Имя домена по умолчанию



Страница **Default Domain Name** (Имя домена по умолчанию) содержит следующие поля.

- **Default Domain Name (1-158 characters)** (Имя домена по умолчанию, 1-158 символов). содержит имя сервера доменов DNS, определяемое пользователем. При настройке применяется имя домена по умолчанию, если имена хостов указаны неправильно.
- **Type** (Тип). тип IP-адреса. Возможные значения:
  - **Dynamic** (Динамический). IP-адрес, который создается динамически.
  - **Static** (Статический). статический IP-адрес.
  - **Remove** (Удалить). когда установлен этот флажок, удаляется имя домена по умолчанию.
  - **Флажок установлен**. удаляет выбранное имя домена по умолчанию.
  - **Флажок снят**. оставляет выбранное имя домена.

Определение имен доменов DNS с помощью команд консоли

В следующей таблице приведены команды консоли для настройки имен доменов DNS.

Команда консоли	**Описание**
ip domain-name ***имя***	Определяет имя домена по умолчанию, которое используется программой, если имена хостов указаны неправильно.
no ip domain-name	Отключает использованием системы имен доменов (DNS).
show hosts [*имя***]**	Отображает имя домена по умолчанию, список хостов сервера имен, статические имена и адреса, а также список имен и адресов из кэша.

Далее приведен пример команд консоли.

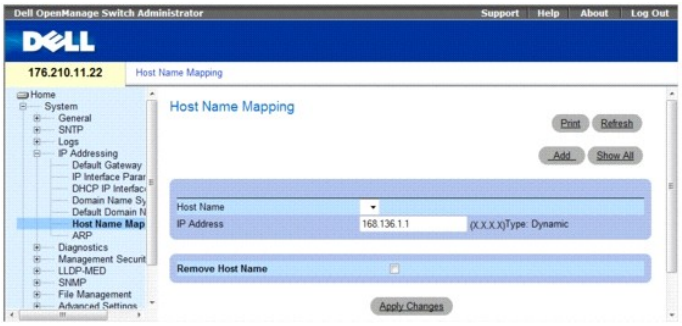
```
Console(config)# ip domain-name dell.com
```

Отображение хоста домена

Страница **Host Name Mapping** (Отображение имени хоста) содержит параметры назначения IP-адресов для статических имен хостов. На этой странице каждому хосту можно сопоставить один IP-адрес.

Чтобы открыть страницу **Host Name Mapping** (Отображение имени хоста), *выберите* **System** (Система)→ **IP Addressing** (IP-адресация)→ **Host Name Mapping** (Отображение имени хоста)на панели дерева.

Рис. 6-47. Отображение имени хоста



Страница Host Name Mapping (Отображение имени хоста) содержит следующие поля.

- **Host Name** (Имя хоста). содержит список имен хостов. Имена хоста определяются на странице **Add Host Name Mapping** (Добавление отображения имени хоста). Каждый хост предоставляет один IP-адрес.
- **IP Address (X.X.X.X)** (IP-адрес). предоставляет IP-адрес, который назначается для определенного имени хоста.
- **Type** (Тип). тип IP-адреса. Возможные значения:
  - **Dynamic** (Динамический). IP-адрес, который создается динамически.
  - **Static** (Статический). статический IP-адрес.
- **Remove Host Name** (Удалить имя хоста). когда этот флажок установлен, удаляется отображение хоста DNS.
  - **Флажок установлен**. удаляет отображение имени хоста DNS
  - **Флажок снят**. оставляет отображение имени хоста.

При определении нового имени хоста, будут доступны следующие дополнительные параметры:

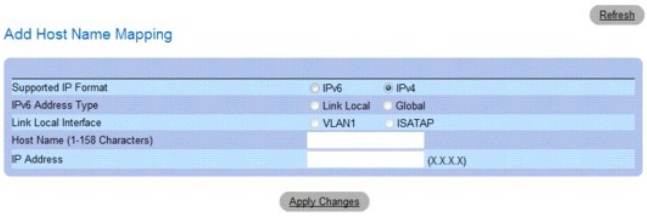
- **Supported IP Format** (Поддерживаемый формат IP-адресов). Отображает формат IP-адресов, поддерживаемый сервером SNTP. Возможные значения:
  - **IPv6**. поддержка IP версии 6.
  - **IPv4**. поддержка IP версии 4.
- **IPv6 Address Type** (Тип адреса IPv6). В случае, если хост поддерживает систему IPv6 (см. предыдущий параметр), здесь указывается поддерживаемый тип статических адресов. Возможные значения:
  - **Link Local** (Локальная связь). Адрес локальной связи, который не маршрутизируется, а используется только для связи в пределах той же сети.
  - **Global** (Глобальный). Глобальный уникальный адрес IPv6 address; он является видимым и доступным для различных подсетей.
- **Link Local Interface** (Интерфейс локальной связи). Если сервер поддерживает систему адресов локальной связи IPv6 (см. предыдущий параметр), здесь указывается интерфейс локальной связи. Возможные значения:
  - **VLAN1**. Интерфейс IPv6 конфигурируется по сети VLAN1.
  - **ISATAP**. Интерфейс IPv6 конфигурируется по туннелю ISATAP.

Добавление имен домена хоста

1. Откройте страницу **Host Name Mapping** (Отображение имени хоста).
2. Нажмите кнопку **Add** (Добавить).

   Откроется страница **Add Host Name Mapping** (Добавление отображения имени хоста).

   Рис. 6-48. Добавление отображения имени хоста



3. Определите соответствующие поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   IP-адрес будет сопоставлен с именем хоста, а устройство обновлено.

Отображение таблицы отображения имен хостов

1. Откройте страницу **Host Name Mapping** (Отображение имени хоста).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **Hosts Name Mapping Table** (Таблица отображения имен хостов).

   Рис. 6-49. Таблица отображения имен хостов

Удаление имени хоста из таблицы отображения IP-адресов

1. Откройте страницу **Host Name Mapping** (Отображение имени хоста).
2. Нажмите кнопку **Show All** (Показать все).
3. Откроется страница **Hosts Mapping Table** (Таблица отображения имен хостов).
4. Выберите запись **Host Name Mapping Table** (Таблица отображения имен хостов).
5. Установите флажок **Remove** (Удалить).
6. Нажмите кнопку **Apply Changes** (Применить изменения).

   Запись таблицы **Host Mapping Table** (Таблица отображения хостов) будет удалена, а устройство обновлено.

Сопоставление IP-адресов с именами хостов домена с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для сопоставления имен хостов домена с IP-адресами.

Команда консоли	**Описание**
ip host *name address*	Определяет соответствие статических имен хостов адресам в кэше хоста.
no ip host ***name***	Удаляет соответствие имен хостов адресам.
clear host {*имя* | *}	Удаляет записи из кэша имя хоста-адрес.

show hosts [имя]	Отображает имя домена по умолчанию, список хостов сервера имен, статические имена и адреса, а также список имен и адресов из кэша.

Далее приведен пример команд консоли.

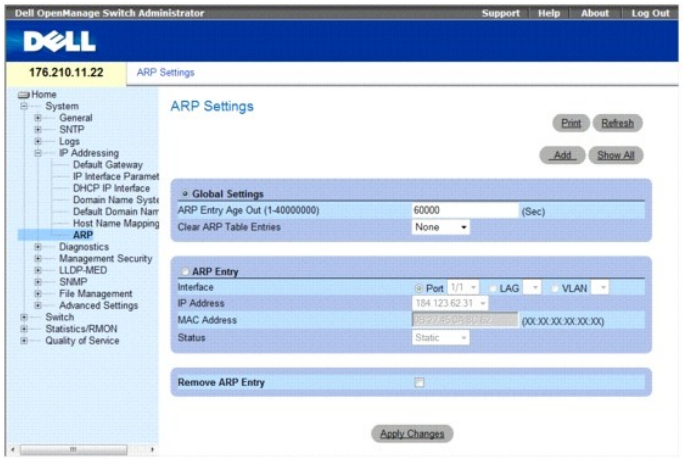
```
console (config)# ip host accounting.abc.com 176.10.23.1
```

Определение параметров ARP

Протокол разрешения адресов ARP (Address Resolution Protocol) преобразует IP-адреса в физические адреса и привязывает IP-адрес к MAC-адресу. Протокол ARP позволяет хосту установить связь с другими хостами, только если известны IP-адреса соседних хостов.

Чтобы открыть страницу **ARP Settings** (Параметры ARP), на панели дерева выберите **System** (Система)→**IP Addressing** (IP-адресация)→ **ARP**.

Рис. 6-50. Параметры ARP



Страница **ARP Settings** (Параметры APR) содержит следующие поля.

- **Global Settings** (Общие параметры). выберите этот параметр, чтобы активизировать поля общих параметров ARP.
  - **ARP Entry Age Out (1-40000000)** (Срок хранения записи ARP). время (в секундах) для всех устройств, которое проходит между запросами ARP по записям таблицы ARP. По истечении этого периода запись удаляется из таблицы. Диапазон значений: **1 - 40000000** секунд. Значение по умолчанию: 60000 секунд.
  - **Clear ARP Table Entries** (Удалить записи таблицы ARP). тип записей ARP, которые удаляются на всех устройствах. Возможные значения:
    - **None** (Нет). записи ARP не удаляются.
    - **All** (Все). все записи ARP удаляются.
    - **Dynamic** (Динамические). удаляются только динамические записи ARP.
    - **Static** (Статические). удаляются только статические записи ARP.
- **ARP Entry** (Запись ARP). выберите этот параметр, чтобы активизировать поля параметров ARP для одного устройства Ethernet.
  - **Interface** (Интерфейс). номер интерфейса порта, группы LAG или VLAN, которые подключены к устройству.
  - **IP Address** (IP-адрес). IP-адрес станции, который связан с MAC-адресом, указанным ниже.
  - **MAC Address** (MAC-адрес). MAC-адрес станции, который связан с IP-адресом в таблице ARP.
  - **Status** (Состояние). состояние записи таблицы ARP. Возможные значения этого поля:
    - **Dynamic** (Динамическая). запись ARP распознается динамически.
    - **Static** (Статическая). запись ARP - статическая.
- **Remove ARP Entry** (Удалить запись ARP). удаляет запись ARP.
  - **Флажок установлен**. удаляет запись ARP.
  - **Флажок снят**. оставляет запись ARP.

Добавление статической записи таблицы ARP:

1. Откройте страницу **ARP Settings** (Параметры ARP).

2. Нажмите кнопку **Add** (Добавить).

   Откроется страница **Add ARP Entry** (Добавление записи ARP).

3. Выберите интерфейс.

4. Определите поля.

5. Нажмите кнопку **Apply Changes** (Применить изменения).

   Запись **ARP Table** (Таблица ARP) будет добавлена, а устройство обновлено.

Отображение таблицы ARP

1. Откройте страницу **ARP Settings** (Параметры ARP).

2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **ARP Table** (Таблица ARP).

Удаление записи таблицы ARP

1. Откройте страницу **ARP Settings** (Параметры ARP)

2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **ARP Table** (Таблица ARP).

3. Выберите запись таблицы.

4. Установите флажок **Remove** (Удалить).

5. Нажмите кнопку **Apply Changes** (Применить изменения).

   Выбранная запись таблицы **ARP Table** будет удалена, а устройство обновлено.

Настройка ARP с помощью команд консоли

В следующей таблице приведены команды консоли для настройки полей, отображаемых на странице **ARP Settings** (Параметры ARP).

Команда консоли	**Описание**
arp *ip_адрес hw_адрес* {**ethernet** номер_интерфейса | **vlan** идентификатор_vlan| port-channel номер}	Добавляет постоянную запись в кэш ARP.
arp timeout *секунды*	Настраивает срок хранения записи в кэше ARP.
clear arp-cache	Удаляет все динамические записи из кэша ARP.
show arp	Выводит записи таблицы ARP.
no arp	Удаляет запись ARP из таблицы ARP Table.

Далее приведен пример команд консоли.

```
Console(config)# arp 198.133.219.232 00-00-0c-40-0f-bc

console(config)# arp timeout 12000

console(config)# exit

console# show arp

ARP timeout: 12000 Seconds
```

Interface	IP address	HW address	Status
---------	----------	----------	------
1/e11	10.7.1.102	00:10:B5:04:DB:4B	Dynamic
1/e12	10.7.1.135	00:50:22:00:2A:A4	Static

Запуск диагностики кабелей

Страница **Diagnostics** (Диагностика) содержит ссылки на страницы, которые используются для виртуального тестирования медных и оптоволоконных кабелей. Чтобы открыть страницу **Diagnostics** (Диагностика), на панели дерева выберите **System** (Система)→ **Diagnostics** (Диагностика).

В этом разделе имеются следующие тематические подразделы:

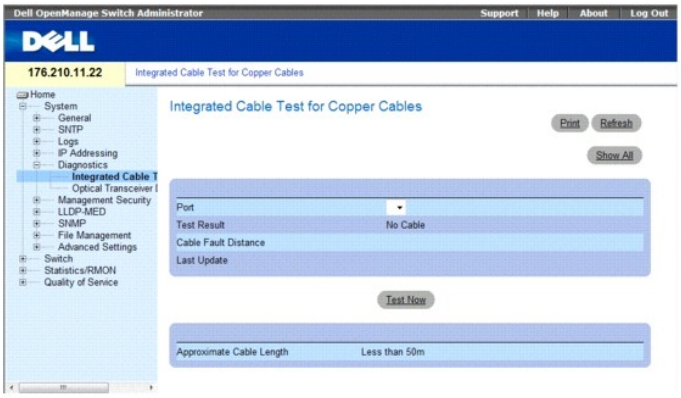
- Просмотр диагностики медных кабелей
- Просмотр диагностики оптического трансивера

Просмотр диагностики медных кабелей

Страница **Integrated Cable Test for Copper Cables** (Интегрированное тестирование медных кабелей) содержит поля для выполнения тестирования медных кабелей. В ходе тестирования кабеля отображается информация о неисправностях кабеля, времени выполнения последнего теста кабеля и типе неисправности кабеля. В тестах используется технология TDR (Time Domain Reflectometry) для проверки качества и характеристик медного кабеля, подключенного к порту. Можно тестировать кабели длиной до 120 метров. Проверка кабелей выполняются при отключенных портах. Исключение составляет тест примерной длины кабеля (Approximated Cable Length).

Чтобы открыть страницу **Integrated Cable Test for Copper Cables** (Интегрированное тестирование медных кабелей), на панели дерева выберите **System** (Система)→ **Diagnostics** (Диагностика)→ **Integrated Cable Test** (Интегрированное тестирование кабеля).

Рис. 6-51. Интегрированное тестирование медных кабелей



Страница **Integrated Cable Test for Copper Cables** (Интегрированное тестирование медных кабелей) содержит следующие поля:

- **Port** (Порт). порт, к которому подключен кабель.
- **Test Result** (Результат теста). результаты теста кабеля. Возможные значения:
  - **No Cable** (Нет кабеля). кабель не подключен к порту.
  - **Open Cable** (Оборванный кабель). кабель подключен только с одной стороны.
  - **Short Cable** (Короткозамкнутый кабель). короткое замыкание в кабеле.
  - **OK**. кабель прошел тестирование.
- **Cable Fault Distance** (Расстояние до повреждения). расстояние от порта до точки повреждения кабеля.
- **Last Update** (Последнее обновление). время последнего тестирования порта.
- **Approximate Cable Length** (Примерная длина кабеля). примерная длина кабеля. Тест можно выполнить, если порт включен и работает на скорости 1 Гбит/с.

Выполнение теста кабеля

1. Убедитесь, что оба конца медного кабеля подключены к устройству.
2. Откройте страницу **Integrated Cable Test for Copper Cables** (Интегрированное тестирование медных кабелей).
3. Выберите интерфейс, который необходимо протестировать.

4. Щелкните **Test Now** (Тестировать).

   Будет выполнен тест медного кабеля и результаты будут отображены на странице **Integrated Cable Test for Copper Cables** (Интегрированное тестирование медных кабелей).

Отображение таблицы результатов виртуального тестирования кабелей

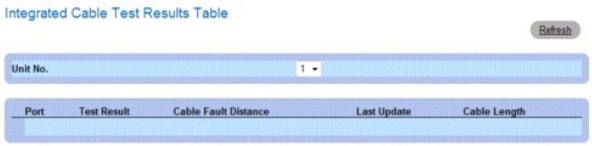
В этом окне отображаются результаты теста, который проводился ранее, но не запускает новую проверку всех портов. Длина кабеля, возвращаемая процедурой интегрированного тестирования (VCT), усредняется до следующих величин: до 50 метров, от 50 до 80 метров, от 80 до 110 метров, от 110 до 120 метров или более 120 метров. Отклонение может составлять до 20 метров, и измерение длины кабеля невозможно для каналов связи со скоростью 10 Мбит/с.

1. Откройте страницу **Integrated Cable Test for Copper Cables** (Интегрированное тестирование медных кабелей).

2. Нажмите кнопку **Show All** (Показать все).

   Откроется таблица **Integrated Cable Test Results Table** (Интегрированное тестирование медных кабелей).

Рис. 6-52. Интегрированное тестирование медных кабелей



Помимо полей, имеющихся на странице **Integrated Cable Test for Copper Cables** (Интегрированное тестирование медных кабелей), таблица **Integrated Cable Test Results Table** (Интегрированное тестирование медных кабелей) содержит следующее поле:

- **Unit No**. (Номер устройства). Указывает номер устройства стека, для которого отображается результат проверки.

Выполнение тестирования медных кабелей с помощью команд консоли

В следующей таблице приведены команды консоли для выполнения тестирования медных кабелей.

Команда консоли	**Описание**
test copper-port tdr интерфейс	Выполняет виртуальное тестирование кабеля.
show copper-port tdr **интерфейс**	Отображает результаты последнего виртуального тестирования кабеля для порта.
show copper-port cable-length **интерфейс**	Отображает предположительную длину кабеля, подключенного к порту.

Далее приведен пример команд консоли.

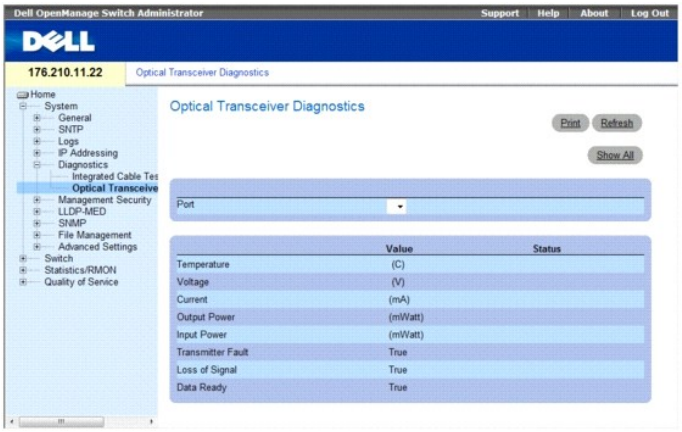
```
console> enable
Console# test copper-port tdr 1/e3
Cable is open at 100 meters.

Console# show copper-port cable-length
Port        Length (meters)
----        ---------------
1/e3        110-140
1/e4        Fiber
```

Просмотр диагностики оптического трансивера

С помощью страницы **Optical Transceiver Diagnostics** (Диагностика оптоволоконного трансивера) можно выполнить тестирование оптоволоконных кабелей. Диагностика оптического трансивера может быть выполнена только в том случае, если установлено соединение. Трансиверы Finisar не поддерживают диагностическую проверку неисправности. Функция анализа оптоволоконной сети работает только на трансиверах SFP, которые поддерживают стандарт диагностики SFF-872.

Чтобы открыть страницу **Optical Transceiver Diagnostics** (Диагностика оптического трансивера), на панели дерева выберите **System** (Система)→ **Diagnostics** (Диагностика)→ **Optical Transceiver Diagnostics** (Диагностика оптического трансивера).

Рис. 6-53. Диагностика оптического трансивера



Страница **Optical Transceiver Diagnostics** (Диагностика оптического трансивера) содержит следующие поля.

- **Port** (Порт). номер порта, кабель которого подвергается тестированию.
- **Temperature** (Температура). рабочая температура (C) кабеля.
- **Voltage** (Напряжение). рабочее напряжение кабеля.
- **Current** (Ток). рабочий ток кабеля.
- **Output Power** (Выходная мощность). значение выходной мощности.
- **Input Power** (Входная мощность). значение входной мощности.
- **Transmitter Fault** (Сбой передатчика). указывает, что произошла ошибка во время передачи.
- **Loss of Signal** (Потеря сигнала). указывает, возникла ли потеря сигнала.
- **Data Ready** (Готовность к передаче данных). на трансивер подается питание и он готов к передаче данных.

Отображение таблицы тестов диагностики оптического трансивера

1. Откройте страницу **Optical Transceiver Diagnostics** (Диагностика оптического трансивера).
2. Нажмите кнопку **Show All** (Показать все).

   Начнется тестирование и откроется таблица **Optical Transceiver Diagnostics Table** (Диагностика оптоволоконного трансивера).

Рис. 6-54. Диагностика оптического трансивера

Помимо полей, имеющихся на странице **Optical Transceiver Diagnostics** (Диагностика оптоволоконного трансивера), таблица **Optical Transceiver Diagnostics Table** (Диагностика оптоволоконного трансивера) содержит следующее поле:

- **Unit No**. (Номер устройства). номер устройства, для которого производится диагностика кабеля.
- **N/A**. недоступно, N/S - не поддерживается, W - предупреждение, E - ошибка

Выполнение тестирования оптоволоконных кабелей с помощью команд консоли

В следующей таблице приведены команды консоли для выполнения тестирования оптических кабелей.

Команда консоли	Описание
show fiber-ports optical-transceiver [[интерфейс]detailed] []	Отображает данные диагностики оптического трансивера.

Далее приведен пример команды консоли:

```
Console# show fiber-ports optical-transceiver detailed

Port  Temp[C]  Voltage  Current [Volt]  Output[mA]  Input [mWatt]  POWER TX [mWatt]  LOS Fault
----  -------  -------  --------------  ----------  -------------  ----------------  ---------
1/g1  48       5.15     50              1.789       1.789          No                No
1/g2  43       5.15     10              1.789       1.789          No                No
```

Управление безопасностью

Страница **Management Security** (Безопасность управления) предоставляет доступ на страницы, содержащие поля для настройки параметров безопасности для методов управления устройством, проверки подлинности пользователя, баз данных проверки подлинности пользователя и их серверов. Чтобы открыть страницу **Management Security** (Безопасность управления), на панели дерева выберите **System** (Система)→ **Management Security** (Безопасность управления).

В этом разделе имеются следующие тематические подразделы:

- Определение профилей доступа
- Определение профилей проверки подлинности
- Выбор профиля проверки подлинности
- Управление паролями
- Отображение активных пользователей
- Определение локальных баз данных пользователей
- Определения паролей линии
- Определение паролей включения
- Определение параметров TACACS+
- Настройка параметров RADIUS

Defining Access Profiles (Определение профилей доступа)

Страница **Access Profiles** (Профили доступа) содержит поля для определения профилей и правил для доступа к устройству. Можно ограничить доступ к функциям управления группам пользователей, которые определены входящими интерфейсами и исходными IP-адресами или маской исходной подсети.

Доступ к управлению может быть отдельно определен для каждого метода доступа для управления, включая Web (HTTP), безопасный web (HTTPS), Telnet и Secure Telnet.

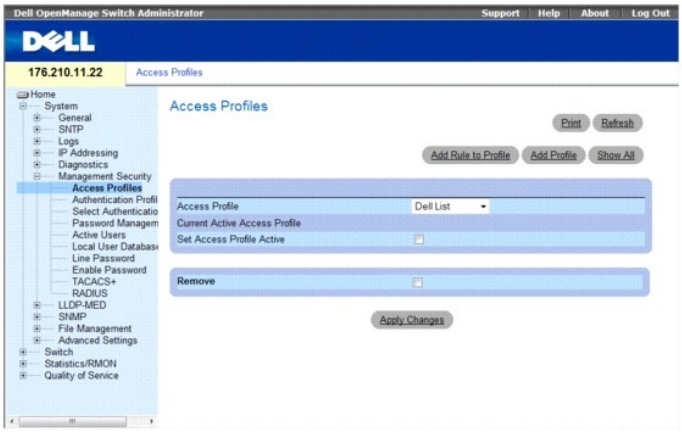
Доступ к различным методам управления может быть различным для разных групп пользователей. Например, «Группа пользователей 1» может получать доступ к устройству только через сеанс HTTP, а «Группа пользователей 2» может получать доступ к устройству через сеансы HTTP и Telnet.

Management Access Lists (Списки управления доступом) содержат до 256 правил, определяющих, какие пользователи могут управлять устройством и каким способом осуществляется это управление. Пользователям может быть запрещен доступ к устройству.

Страница **Access Profiles** (Профили доступа) содержит поля для настройки списков управления и назначения их для определенных интерфейсов.

Чтобы открыть страницу **Access Profiles** (Профили доступа), на панели дерева выберите **System** (Система)→ **Management Security** (Безопасность управления)→ **Access Profiles** (Профили доступа).

Рис. 6-55. Профили доступа



Страница **Access Profiles** (Профили доступа) содержит следующие поля:

- **Access Profile** (Профиль доступа). список определенных пользователем профилей. Список Access Profile (Профиль доступа) содержит значение по умолчанию **Console Only** (Только консоль). Если выбран этот профиль, активное управление устройством производится только с помощью подключенной консоли.
- **Current Active Access Profile** (Текущий активный профиль доступа). активный в настоящий момент профиль доступа.
- **Set Access Profile Active** (Сделать профиль доступа активным). активизирует профиль доступа.
- **Remove** (Удалить). удаляет профиль доступа из списка имен профилей доступа **(Access Profile Name)**.
  - **Флажок установлен**. удаляет профиль доступа.
  - **Флажок снят**. оставляет профиль доступа.

Активизация профиля

1. Откройте страницу **Access Profiles** (Профили доступа).
2. Выберите профиль доступа в поле **Access Profile** (Профиль доступа).
3. Установите флажок **Set Access Profile Active** (Активизировать профиль доступа).
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Профиль доступа будет активирован.

Добавление профиля доступа

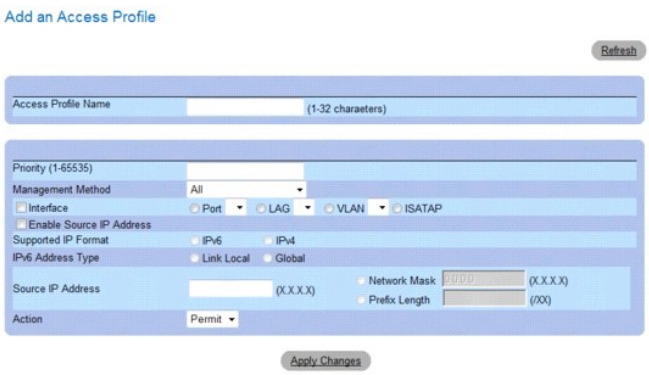
Правила служат фильтрами для определения приоритетов правил, метода управления устройством, типа интерфейса, IP-адреса источника и сетевой маски, а также действия при доступе для управления устройством. Доступ пользователей для управления может быть разрешен или заблокирован. Приоритет правила устанавливает порядок, в котором применяются правила. Назначение профиля доступа интерфейсу закрывает доступ через другие интерфейсы. Если профиль доступа не назначен ни для одного интерфейса, устройство будет доступно для всех интерфейсов.

Определение правил для профиля доступа:

1. Откройте страницу **Access Profiles** (Профили доступа).
2. Щелкните **Add Profile** (Добавить профиль).

   Откроется страница **Add An Access Profile** (Добавление профиля доступа).

   Рис. 6-56. Add an Access Profile (Добавление профиля доступа)



Страница **Add an Access Profile** (Добавление профиля доступа) содержит следующие дополнительные поля.

- **Access Profile Name (1-32 Characters)** (Имя профиля доступа). определенное пользователем имя профиля доступа. Имя профиля доступа может содержать до 32 символов.
- **Rule Priority (1-65535)** (Приоритет правила). приоритет правила. Если пакет соответствует правилу, группам пользователей либо предоставляется, либо запрещается доступ для управления устройством. Порядок применения правил устанавливается приоритетом правила в этом поле. Номер правила является важным для сопоставления пакетов правилам, поскольку сопоставление пакетов выполняется на основе схемы первого совпадения. Приоритеты правил можно просмотреть в таблице **Profile Rules Table** (Таблица правил профиля).
- **Management Method** (Метод управления). метод управления, для которого определен профиль доступа. Пользователям с этим профилем доступа предоставляется или запрещается доступ к устройству, в соответствии с выбранным методом управления (канал). Возможные значения:
  - **All** (Все). Назначает правилу все методы управления.
  - **Telnet**. Правилу назначается доступ по Telnet. Если выбран этот параметр, пользователи, имеющие доступ к устройству по Telnet и соответствующие критерию доступа, получают или не получают доступ к устройству.
  - **Secure Telnet (SSH)**. Назначает правилу доступ по SSH. Если выбран этот параметр, пользователи, имеющие доступ к устройству по Telnet и соответствующие критерию доступа, получают или не получают доступ к устройству.
  - **HTTP**. Назначает правилу доступ по HTTP. Если выбран этот параметр, пользователи, имеющие доступ к устройству по HTTP и соответствующие критерию доступа, получают или не получают доступ к устройству.
  - **Secure HTTP (HTTPS)** (Безопасный HTTP(HTTPS)). Назначает правилу доступ по HTTPS. Если выбран этот параметр, пользователи, имеющие доступ к устройству по HTTPS и соответствующие критерию доступа, получают или не получают доступ к устройству.
  - **SNMP**. Назначает правилу доступ по SNMP. Если выбран этот параметр, пользователи, имеющие доступ к устройству по SNMP и соответствующие критерию доступа, получают или не получают доступ к устройству.
- **Interface** (Интерфейс). тип интерфейса, к которому относится правило. Это необязательное поле. Это правило можно применять для выбранного порта, LAG или VLAN путем установки флажка и выбора соответствующей кнопки и интерфейса.
- **Enable Source IP Address** (Включить IP-адрес источника). Установите флажок на этом параметре для того, чтобы сузить условия, основанные на IP-адресе источника. Если флажок снят, IP-адрес источника не может быть введен в сконфигурированное правило.
- **Supported IP Format** (Поддерживаемый формат IP-адресов). Отображает формат IP-адресов. Возможные значения:
  - **IPv6**. поддержка IP версии 6.
  - **IPv4**. поддержка IP версии 4.
- **IPv6 Address Type** (Тип адреса IPv6). В случае, если сервер поддерживает систему IPv6 (см. предыдущий параметр), здесь указывается поддерживаемый тип статических адресов. Возможные значения:
  - **Link Local** (Локальная связь). Адрес локальной связи, который не маршрутизируется, а используется только для связи в пределах той же сети.
- **Global** (Глобальный). Глобальный уникальный адрес IPv6 address; он является видимым и доступным для различных подсетей.
- **Source IP Address (X.X.X.X)** (IP-адрес источника (X.X.X.X)). указывает IP-адрес источника, для которого применяется правило. Это дополнительное поле, показывающее, что правило действительно для этой подсети.
- **Network Mask (X.X.X.X)** (Маска сети (X.X.X.X)). указывает маску подсети IP-адреса.
- **Prefix Length (/XX)** (Длина префикса (/XX)). указывает число бит, образующих префикс исходного IP-адреса или сетевую маску исходного IP-адреса.
- **Action** (Действие). определяет, разрешен или запрещен доступ для управления для определенного интерфейса.
  - **Permit** (Разрешить). Разрешает доступ к устройству.
  - **Deny** (Запретить). Запрещает доступ к устройству. Это значение по умолчанию.

3. Определите поле **Access Profile Name** (Имя профиля доступа).
4. Определите соответствующие поля.
5. Нажмите кнопку **Apply Changes** (Применить изменения).

Новый профиль доступа будет добавлен, а устройство обновлено.

Добавление правил для профиля доступа

Первое правило необходимо определить для запуска соответствующего трафика на профили доступа.

1. Откройте страницу **Access Profile** (Профили доступа).
2. Щелкните **Add Profile to Rule** (Добавить профиль для правила).

   Откроется страница **Add An Access Profile Rule**.

   Рис. 6-57. Страница Add An Access Profile Rule (Добавление правила профиля доступа)

3. Заполните поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Правило будет добавлено в профиль доступа, а устройство обновлено.

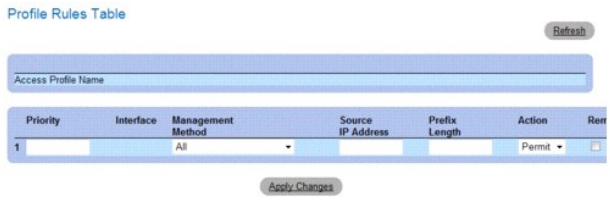
Просмотр таблицы правил профиля:

Порядок, в котором правила отображаются в таблице Profile Rules Table (Таблица правил профиля), имеет значение. Пакеты сравниваются с первым правилом, которое отвечает критериям правила.

1. Откройте страницу **Access Profiles** (Профили доступа).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **Profile Rules Table** (Таблица правил профиля).

   Рис. 6-58. Таблица правил профиля



Удаление правила

1. Откройте страницу **Access Profiles** (Профили доступа).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **Profile Rules Table Page** (Таблица правил профиля).

3. Выберите правило.
4. Установите флажок **Remove** (Удалить).
5. Нажмите кнопку **Apply Changes** (Применить изменения).

   Выбранное правило будет удалено, а устройство обновлено.

Определение профилей доступа с помощью команд консоли

В следующей таблице приведены команды консоли для настройки полей, отображаемых на странице **Access Profiles** (Профили доступа).

Команда консоли	**Описание**
management access-list *имя*	Определяет список доступа для управления и вводит контекст списка доступа для конфигурации.
permit [**ethernet** *номер_интерфейса* | **vlan** *идентификатор_vlan* **| port-channel** *номер*] [**service** *служба*]	Задает разрешающие условия для списка доступа для управления для порта.
permit ip-source {*ipv4-address* | *ipv6-address / prefix-length}* [**mask** *mask* | *prefix-length*] [**ethernet** *interface-number* | **vlan** *vlan-id* **| port-channel** *number*] [**service** *service*]	Задает для порта разрешающие условия списка доступа для управления и выбранный метод управления.
deny [**ethernet** *номер_интерфейса* | **vlan** *идентификатор_vlan* **| port-channel** *номер*] [**service** *служба*]	Задает для порта запрещающие условия списка доступа для управления и выбранный метод управления.
deny ip-source {*ipv4-address* | *ipv6-address / prefix-length}* [**mask** *mask* | *prefix-length*] [**ethernet** *interface-number* | **vlan** *vlan-id* **| port-channel** *number*] [**service** *service*]	Задает для порта запрещающие условия списка доступа для управления и выбранный метод управления.
management access-class {**console-only** | *имя*}	Определяет, какой список доступа используются в качестве активных соединений для управления.
show management access-list [*имя*]	Отображает активные списки доступа для управления.
show management access-class	Отображает информацию о классе доступа для управления.

Далее приведен пример команд консоли.

```
console(config)# management access-list mlist

console(config-macl)# permit ethernet 1/e1

console(config-macl)# permit ethernet 1/e2

console(config-macl)# deny ethernet 1/e3

console(config-macl)# deny ethernet 1/e4

console(config-macl)# exit

console(config)# management access-class mlist

console(config)# exit

console# show management access-list

mlist

-----

permit ethernet 1/e1

permit ethernet 1/e2

deny ethernet 1/e3

deny ethernet 1/e4

! (Note: all other access implicitly denied)

Console# show management access-class

Management access-class is enabled, using access list mlist
```

Определение профилей проверки подлинности

Страница **Authentication Profiles** (Профили проверки подлинности) содержит поля для выбора метода проверки подлинности пользователя на

устройстве. Идентификация пользователя происходит:

- Локально
- Через внешний сервер

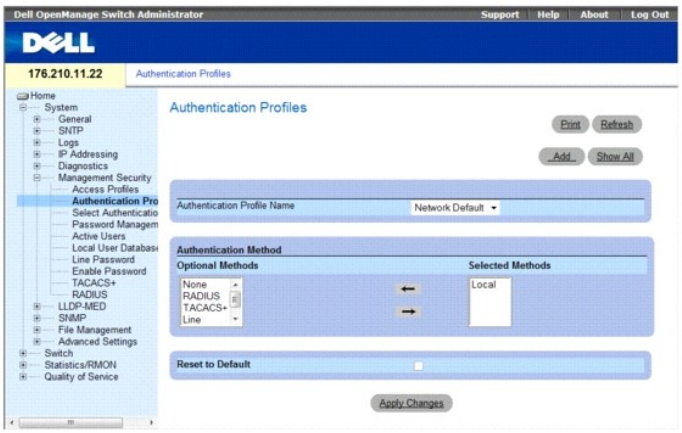
Для идентификации пользователя также можно задать значение *None* (Нет).

Проверка подлинности пользователя происходит в том порядке, в каком выбраны методы. Например, если выделены и параметр *Local* (Локально), и параметр *RADIUS*, пользователи сначала идентифицируются локально. Если локальная пользовательская база данных пуста, то пользователь идентифицируется через сервер RADIUS. При отрицательном результате проверки подлинности с использованием первого метода, процесс проверки подлинности прекращается.

Если при проверке подлинности происходит ошибка, используется следующий выбранный метод.

Чтобы открыть страницу Authentication Profiles (Профили проверки подлинности), выберите **System** (Система)→ **Management Security** (Безопасность управления)→ **Authentication Profiles** (Профили проверки подлинности) на панели дерева.

Рис. 6-59. Профили проверки подлинности



Страница **Authentication Profiles** (Профили проверки подлинности) содержит следующие поля.

- **Authentication Profile Name** (Имя профиля проверки подлинности). списки определяемых пользователем профилей проверки подлинности, в которые добавляются определяемые пользователем профили проверки подлинности. Возможные опции: **Network Default** (Сеть по умолчанию) и **Console Default** (Консоль по умолчанию). Имена профилей не могут содержать пробелы.
- **Optional Methods** (Дополнительные методы). определяемые пользователем методы проверки подлинности. Возможные опции таковы:
  - **None** (Нет). проверка подлинности пользователя не выполняется.
  - **Local** (Локально). проверка подлинности пользователя выполняется на уровне устройства. Для проверки подлинности устройство проверяет имя пользователя и пароль.
  - **RADIUS**. проверка подлинности выполняется на сервере RADIUS. Дополнительную информацию см. в разделе «Настройка параметров сервера RADIUS».
  - **TACACS+**. проверка подлинности выполняется на сервере TACACS+.
  - **Line** (Канал). для проверки подлинности пользователя используется пароль канала связи.
  - **Enable** (Включение). для проверки подлинности используется пароль включения.
- **Reset to Default** (Возврат к предустановкам). Восстанавливает метод определения подлинности пользователей, который был установлен для устройства по умолчанию. Пригодно только для профиля по умолчанию.

Выбор профиля проверки подлинности:

1. Откройте страницу **Authentication Profiles** (Профили идентификации).
2. Выберите профиль в поле **Authentication Profile Name** (Имя профиля проверки подлинности).
3. С помощью клавиш со стрелками выберите метод проверки подлинности. Проверка подлинности пользователя происходит в том порядке, в каком перечислены методы.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

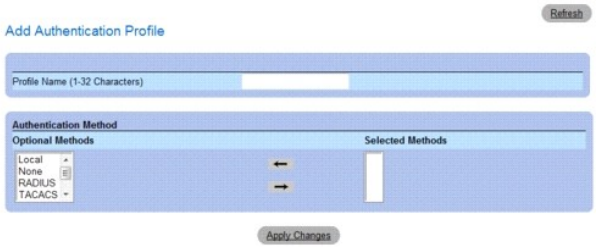
   Профиль проверки подлинности для этого устройства будет изменен.

Добавление профиля проверки подлинности:

1. Откройте страницу **Authentication Profiles** (Профили идентификации).
2. Нажмите кнопку **Add** (Добавить).

   Откроется страница **Add Authentication Profile** (Добавление профиля проверки подлинности).

   Рис. 6-60. Добавление профиля проверки подлинности



3. Настройте профиль.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

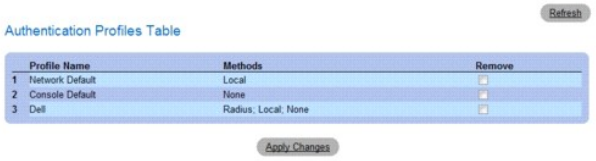
   Профиль проверки подлинности для этого устройства будет изменен.

Отображение таблицы проверки подлинности

1. Откройте страницу **Authentication Profiles** (Профили проверки подлинности).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **Authentication Profiles Table** (Таблица профилей проверки подлинности).

   Рис. 6-61. Authentication Profiles Table (Таблица профилей проверки подлинности)



Удаление профиля проверки подлинности

1. Откройте страницу **Authentication Profiles** (Профили идентификации).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **Authentication Profiles Table** Таблица профилей проверки подлинности.

3. Выберите профиль проверки подлинности.
4. Установите флажок **Remove** (Удалить).
5. Нажмите кнопку **Apply Changes** (Применить изменения).

   Выбранный профиль проверки подлинности будет удален.

Настройка профиля проверки подлинности с помощью команд консоли

В следующей таблице приведены команды консоли для настройки полей, отображаемых на странице **Authentication Profiles** (Профили проверки подлинности).

Команда консоли	**Описание**
aaa authentication login {**default** | *имя_списка*} *метод1* [*метод2*.]	Настраивает проверку подлинности при входе в систему.
no aaa authentication login {**default** | *имя_списка*}	Удаляет профиль проверки подлинности при входе в систему.

Далее приведен пример команд консоли.

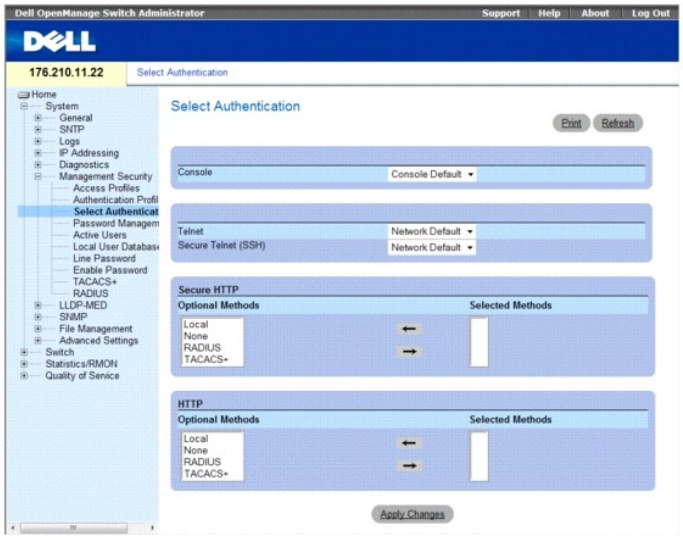
```
console(config)# aaa authentication login default radius local enable none

console(config)# no aaa authentication login default
```

Выбор профиля проверки подлинности

После того как профили проверки подлинности определены, их можно применить к методам доступа для управления. Например, проверка подлинности пользователей консоли может выполняться по списку профилей проверки подлинности 1, в то время как проверка подлинности пользователей Telnet выполняется по списку методов проверки подлинности 2.

Чтобы открыть страницу **Select Authentication** (Выбор проверки подлинности), выберите **System** (Система)→ **Management Security** (Безопасность управления)→ **Select Authentication** (Выбор проверки подлинности) на панели дерева.

Рис. 6-62. Страница Select Authentication (Выбор проверки подлинности)



Страница **Select Authentication** (Выбор проверки подлинности) содержит следующие поля.

- **Console** (Консоль). профили проверки подлинности, используемые для проверки подлинности пользователей консоли.
- **Telnet**. профили проверки подлинности, используемые для проверки подлинности пользователей Telnet.
- **Secure Telnet (SSH)**. профили проверки подлинности, используемые для проверки подлинности пользователей Secure Shell (SSH).Протокол SSH предоставляет клиентам безопасные и шифрованные удаленные соединения с устройством.
- **Secure HTTP** и **HTTP**. метод проверки подлинности, используемый для доступа через HTTP и Secure HTTP, соответственно. Возможные значения этого поля:
  - **Local** (Локально). проверка подлинности выполняется локально.
  - **None** (Нет). для доступа не используется никакой метод проверки подлинности пользователя.
  - **RADIUS**. проверка подлинности выполняется на сервере RADIUS.
  - **TACACS+**. проверка подлинности выполняется на сервере TACACS+.

Применение списка методов проверки подлинности к сеансам консоли

1. Откройте страницу **Select Authentication** (Выбор проверки подлинности).
2. Выберите профиль проверки подлинности в поле **Console** (Консоль).
3. Нажмите кнопку **Apply Changes** (Применить изменения).

   Сеансам консоли будет назначен список проверки подлинности.

Применение списка проверки подлинности к сеансам Telnet

1. Откройте страницу **Select Authentication** (Выбор проверки подлинности).
2. Выберите профиль проверки подлинности в поле **Telnet**.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

   Сеансам Telnet будет назначен список проверки подлинности.

Применение профилей проверки подлинности к сеансам Secure Telnet (SSH)

1. Откройте страницу **Select Authentication** (Выбор проверки подлинности).
2. Выберите профиль проверки подлинности в поле **Secure Telnet (SSH)**.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

   Сеансам Secure Telnet (SSH) будет назначен профиль проверки подлинности.

Назначение сеансам HTTP последовательности проверки подлинности

1. Откройте страницу **Select Authentication** (Выбор проверки подлинности).
2. Выберите последовательность проверки подлинности в поле **HTTP**.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

   Сеансам HTTP будет назначена последовательность проверки подлинности.

Назначение сеансам Secure HTTP последовательности проверки подлинности

1. Откройте страницу **Select Authentication** (Выбор проверки подлинности).
2. Выберите последовательность идентификации в поле **Secure HTTP**.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

   Сеансам Secure HTTP будет назначена последовательность проверки подлинности.

Назначение профилей или последовательностей проверки подлинности доступа с помощью команд консоли

В следующей таблице приведены команды консоли для настройки полей, отображаемых на странице **Select Authentication** (Выбор проверки подлинности).

Команда консоли	**Описание**
enable authentication [**default** | *имя_списка*]	Указывает список методов проверки подлинности при доступе на уровень с более высокими привилегиями в сеансе удаленного доступа Telnet, консоли или SSH.
login authentication [**default** | *имя_списка*]	Указывает список методов проверки подлинности для входа в систему с удаленного подключения Telnet, консоли или SSH.
ip http authentication *метод1* [*метод2*.]	Определяет методы проверки подлинности для серверов HTTP.

ip https authentication *метод1* [*метод2*.]	Определяет методы проверки подлинности для серверов HTTPS.
show authentication methods	Отображает информацию о методах проверки подлинности.

Далее приведен пример команд консоли.

```
console(config-line)# enable authentication default
console(config-line)# login authentication default
console(config-line)# exit
console(config)# ip http authentication radius local
console(config)# ip https authentication radius local
console(config)# exit

console# show authentication methods
Login Authentication Method Lists

---------------------------------
Console_Default     : None
Network_Default     : Local

Enable Authentication Method Lists

---------------------------------
Console_Default     : Enable   None
Network_Default     : Enable
Line                Login Method List       Enable Method List
----                -----------------       ------------------
Console             Значение по умолчанию   Значение по умолчанию
Telnet              Значение по умолчанию   Значение по умолчанию
Страница SSH        Значение по умолчанию   Значение по умолчанию

HTTP                : Local
https               : Local
dot1x               :
```

Управление паролями

Управление паролями повышает безопасность сети и улучшает контроль паролей. Паролям для доступа SSH, Telnet, HTTP, HTTPS и SNMP назначаются следующие функции безопасности.

- Определение минимальной длины пароля
- Истечение срока пароля
- Предотвращение частого повторного использования паролей
- Блокировка входа пользователей после неудачных попыток ввода пароля

Отсчет срока действия пароля начинается сразу после включения функции управления паролями. Сроки действия паролей определяются временем/датой, установленными пользователем. За десять дней до окончания действия пароля на устройстве отобразится соответствующее предупреждение.

После истечения срока действия пароля пользователи могут входить в систему еще несколько раз (количество доступных входов настраивается отдельно). Во время последних входов в систему будут отображаться дополнительные сообщения, информирующие пользователя о необходимости немедленной смены пароля. Если пароль не будет изменен, вход пользователя в систему будет заблокирован. Пользователь сможет войти в систему только через консоль. Предупреждения относительно паролей записываются в файле Syslog.

При переопределении уровня привилегий необходимо также переопределить пользователя. Однако срок действия пароля истекает на основе начального определения пользователя.

Перед истечением срока действия пароля пользователи получают соответствующее предупреждение и запрос на смену пароля. Однако это предупреждение не отображается для веб-пользователей.

Чтобы открыть страницу **Password Management** (Управление паролями), выберите **System** (Система)→ **Management Security** (Безопасность управления)→ **Password Management** (Управление паролями) на панели дерева.

Рис. 6-63. Страница Password Management (Управление паролями)

Страница **Password Management**(Управление паролями) содержит следующие поля.

- **Password Minimum Length (8-64)** (Минимальная длина пароля (8-64 символов)). когда установлен этот флажок, указывает минимальную длину пароля. Например, администратор может определить, что минимальное количество символов для всех паролей канала - 10.
- **Consecutive Passwords Before Re-use** (Последовательные пароли перед повторным использованием). указывает количество изменений пароля перед тем, как использовать его повторно. Возможные значения этого поля: 1-10**.**
- **Enable Login Attempts (1-5)** (Включить контроль попыток ввода пароля (1-5)). При установке флажка на этой опции, опция позволяет отключить пользователя от устройства при вводе неправильного пароля определенное число раз, которое устанавливается пользователем. Например, если это поле отмечено, и определено, что число попыток ввода пароля равно пяти, когда пользователь неправильно введет пароль пять раз, при шестой попытке устройство заблокирует пользователя. Возможные значения этого поля: 1-5.

Определение параметров управления паролями

1. Откройте страницу **Password Management** (Управление паролями)
2. Определите поля.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

   Параметры управления паролями будут определены, а устройство обновлено.

Управление паролями с помощью команд консоли

В следующей таблице приведены эквивалентные команды интерфейса командной строки для настройки полей, отображаемых на странице **Password Management** (Управление паролями).

Команда консоли	**Описание**
minimal length *пароль*	Определение минимальной длины пароля.
history *пароль*	Определение количества изменений пароля перед тем, как его можно использовать повторно.
history hold time *пароля*	Определение числа неправильных попыток ввода пароля до блокировки входа пользователя в систему.
show passwords configuration	Отображение информации об управлении паролями.
show users accounts	Отображает профиль пользователя.

Далее приведен пример команд консоли.

console # **show passwords configuration**				
Minimal length: 0 History: Disabled History hold time: no limit Lockout control: disabled				
Enable Passwords (Задействовать защиту паролем)				
Level	Password Aging	Password Expiry date	Lockout	
-----	--------	----------	-------	

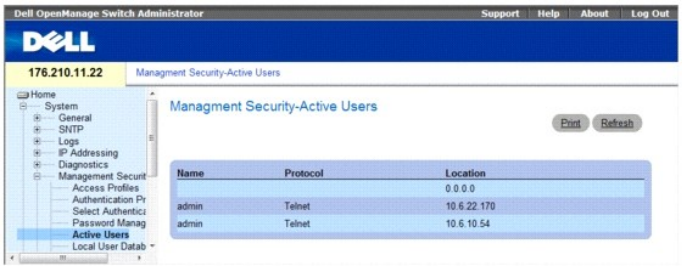
1	-	-	-	
15	-	-	-	
Line Passwords (Пароли каналов)				
Line	Password Aging	Password Expiry date	Lockout	
-------	--------	----------	-------	
Telnet	-	-	-	
Страница SSH	-	-	-	
Console	-	-	-	
console # **show users accounts**				
Username	Privilege	Password Aging	Password Expiry Date	Lockout
--------	---------	--------	----------	-------
nim	15	39	18-Feb-2005	

Отображение активных пользователей

Страница **Active Users** (Активные пользователи) отображает информацию об активных пользователях устройства.

Чтобы открыть страницу **Active Users** (Активные пользователи), выберите **System** (Система)→ **Management Security** (Безопасность управления)→ **Active Users** (Активные пользователи) на панели дерева.

Рис. 6-64. Active Users (Активные пользователи)



Страница Active Users (Активные пользователи) содержит следующие поля:

- **Name** (Имя). Список имен пользователей, которые осуществили вход в систему устройства.
- **Protocol** (Протокол). Способ управления, при помощи которого пользователь подключается к устройству.
- **Location** (Место расположения). IP-адрес пользователя.

Отображение активных пользователей с помощью команд консоли

В приведенной ниже таблице указаны эквивалентные команды консоли, предназначенные для отображения активных пользователей, подключенных к устройству.

Таблица 6-37. Команды консоли для отображения активных пользователей

Команда консоли	Описание
show users	Отображает информацию об активных пользователях.

Ниже приведен пример команды консоли:

```
console> show users


Имя
```

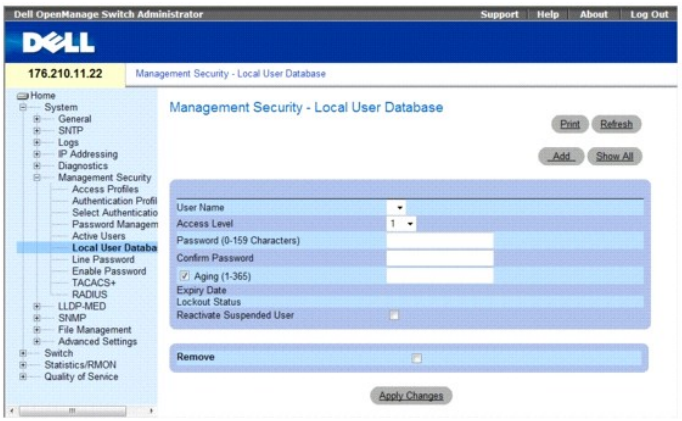
пользователя	Протокол	Расположение
Bob	Serial	
John	SSH	172.16.0.1
Robert	HTTP	172.16.0.8
Betty	Telnet	172.16.1.7

Определение локальных баз данных пользователей

Страница **Local User Database** (Локальная база данных пользователей) содержит поля, позволяющие определить пользователей, пароли и уровни доступа.

Чтобы открыть страницу **Local User Database** (Локальная база данных пользователей), выберите **System** (Система)→ **Management Security** (Безопасность управления)→ **Local User Database** (Локальная база данных пользователей) на панели дерева.

Рис. 6-65. Страница Local User Database (Локальная база данных пользователей)



Страница **Local User Database** (Локальная база данных пользователей) содержит следующие поля.

- **User Name** (Имя пользователя). список пользователей.
- **Access Level** (Уровень доступа). уровень доступа пользователя. Самый низкий уровень доступа пользователя - **1**, а самый высокий -**15**. Пользователи с уровнем доступа 15 являются привилегированными. Только эти пользователи имеют доступ к странице Dell OpenManage Switch Administrator.
- **Password (0-159 Characters)** (Пароль от 0 до 159 символов). задаваемый пользователем пароль.
- **Confirm Password** (Подтверждение пароля). подтверждение задаваемого пользователем пароля.
- **Aging (1-365)** (Срок действия пароля (1-365)). указывает срок действия пароля в днях.
  - **Флажок установлен**. срок действия пароля истекает после указанного количества дней.
  - **Флажок снят**. срок действия пароля не истек.
- **Expiry Date** (Дата окончания действия). указывает дату окончания действия определенного пользователем пароля.
- **Lockout Status** (Состояние блокировки пароля). Указывает, имеет ли пользователь в настоящее время доступ (статус *Usable (Доступ открыт)*), или пользователь лишен доступа вследствие большого числа неудачных попыток авторизации с момента последнего успешного входя в систему (статус *Locked (Доступ закрыт)*).
- **Reactivated Suspended User** (Возобновление приостановленных пользователей). возобновление права доступа указанного пользователя. Права доступа могут быть приостановлены после неудачной попытки входа в систему.
  - **Флажок установлен**. восстановить права доступа пользователя.
  - **Флажок снят**. пользователь отказано в доступе.
- **Remove** (Удалить). удаляет пользователя из списка имен пользователей (**User Name** list).
  - **Флажок установлен**. удаляет выбранного пользователя.
  - **Флажок снят**. оставляет выбранного пользователя.

Назначение прав доступа пользователю:

1. Откройте страницу **Local User Database** (Локальная база данных пользователей).
2. Выберите пользователя в поле **User Name** (Имя пользователя).
3. Определите поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

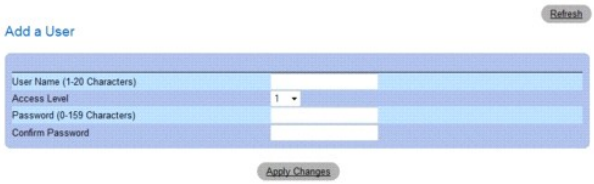
   Права доступа пользователя и пароли будут определены, а устройство обновлено.

Определение нового пользователя:

1. Откройте страницу **Local User Database** (Локальная база данных пользователей).
2. Нажмите кнопку **Add** (Добавить).

   Откроется страница **Add User** (Добавить пользователя).

   Рис. 6-66. Добавление пользователя



3. Определите поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Новый пользователь будет определен, а устройство обновлено.

Отображение локальной пользовательской таблицы:

1. Откройте страницу **Local User Database** (Локальная база данных пользователей).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **Local User Table** (Таблица локальных пользователей).

   Рис. 6-67. Local User Table (Таблица локальных пользователей).

Возобновление приостановленных прав пользователя:

1. Откройте страницу **Local User Database** (Локальная база данных пользователей).
2. Выберите запись **User Name** (Имя пользователя).
3. Установите флажок **Reactivate Suspended User** (Возобновить приостановленные права пользователя).
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Права доступа пользователя будут восстановлены, а устройство обновлено. Вы также можете восстановить доступ пользователей, которым был

закрыт доступ, пользуясь таблицей локальных пользователей.

Удаление пользователей:

1. Откройте страницу **Local User Database** (Локальная база данных пользователей).
2. Выберите **User Name** (Имя пользователя).
3. Установите флажок **Remove** (Удалить).
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Выбранный пользователь будет удален, а устройство обновлено.

Назначение пользователей с помощью команд консоли

В следующей таблице приведены команды консоли для настройки полей, отображаемых на странице **Local User Database** (Локальная база данных пользователей).

Команда консоли	**Описание**
username *имя* [**password** *пароль*] [**level** *уровень*] [**encrypted**]	Устанавливает проверку подлинности по имени пользователя.
set username *имя* **active**	Восстановление прав доступа пользователя.

Далее приведен пример команд консоли.

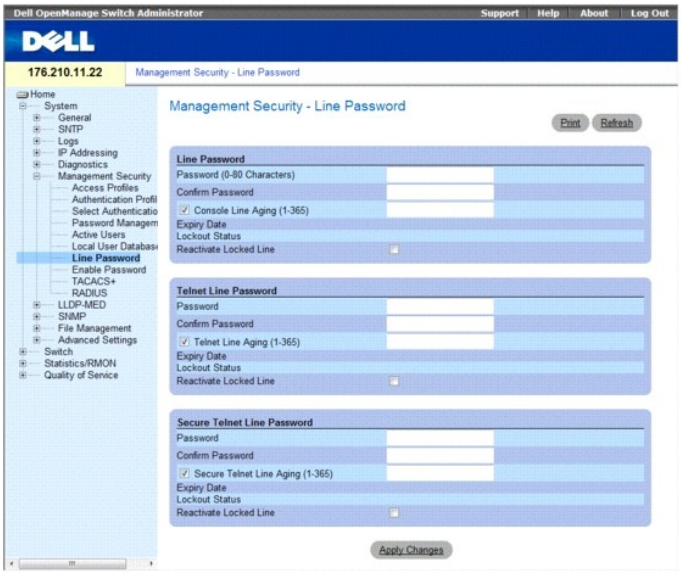
```
console(config)# username bob password lee level 15

console# set username bob active
```

Определение паролей каналов связи

Страница **Line Password** (Пароль канала связи) содержит поля для определения паролей каналов для методов управления.

Чтобы открыть страницу **Line Password** (Пароль канала), выберите **System** (Система)→ **Management Security** (Безопасность управления)→ **Line Passwords** (Пароли каналов) на панели дерева.

Рис. 6-68. Страница Line Password (Пароль канала)



Страница Line Password (Пароль канала) содержит следующие поля.

- **Line Password/Telnet Line Password/Secure Telnet Line Password** (Пароль канала для консоли/Telnet/Secure Telnet). пароли для доступа к устройству через консоль, Telnet или Secure Telnet соответственно.
- **Password** (Пароль). пароль канала для доступа к устройству.
- **Confirm Password** (Подтвердить пароль). подтверждение нового пароля канала. В целях безопасности пароль выводится в формате *****.
- **Console/Telnet/Secure Telnet Line Aging (1-365)** (Срок действия (1-365) пароля канала для консоли/Telnet/Secure Telnet). указывает срок действия пароля канала в днях.
  - **Флажок установлен**. срок действия пароля истекает после указанного количества дней.
  - **Флажок снят**. срок действия пароля не истек.
- **Expiry Date** (Дата окончания действия). указывает дату окончания действия пароля канала.
- **Lockout Status** (Состояние блокировки пароля). Указывает, имеет ли пользователь в настоящее время доступ (статус *Usable* (Доступ открыт)), или пользователь лишен доступа вследствие большого числа неудачных попыток авторизации с момента последнего успешного входя в систему (статус *Locked (Доступ закрыт)*).
- **Reactivate Locked Line** (Восстановить пароль канала). восстанавливает пароль канала для сеанса консоли/Telnet/Secure Telnet. Права доступа могут быть приостановлены после неудачной попытки входа в систему.
  - **Флажок установлен**. восстановление пароля
  - **Флажок снят**. пароль остается недействительным.

Определение паролей каналов связи для сеансов консоли

1. Откройте страницу **Line Password** (Пароль канала)
2. Введите значение в поле **Console Line Password** (Пароль канала для консоли).
3. Нажмите кнопку **Apply Changes** (Применить изменения).

   Пароль линии для сеансов консоли будет определен, а устройство обновлено.

Определение паролей каналов связи для сеансов Telnet

1. Откройте страницу **Line Password** (Пароль канала).
2. Введите значение в поля **Telnet Line Password** (Пароль канала для Telnet).
3. Нажмите кнопку **Apply Changes** (Применить изменения).

   Пароль линии для сеансов Telnet будет определен, а устройство обновлено.

Определение паролей каналов связи для сеансов безопасной связи Telnet

1. Откройте страницу **Line Password** (Пароль канала).
2. Введите значение в поля **Secure Telnet Line Password** (Пароль канала для Secure Telnet).
3. Нажмите кнопку **Apply Changes** (Применить изменения).

   Пароль линии для сеансов Secure Telnet будет определен, а устройство обновлено.

Назначение паролей каналов с помощью команд консоли

В следующей таблице приведены команды консоли для настройки полей, отображаемых на странице **Line Password** (Пароль канала).

Команда консоли	**Описание**
password *пароль* [**encrypted**]	Указывает пароль для канала.

Далее приведен пример команд консоли.

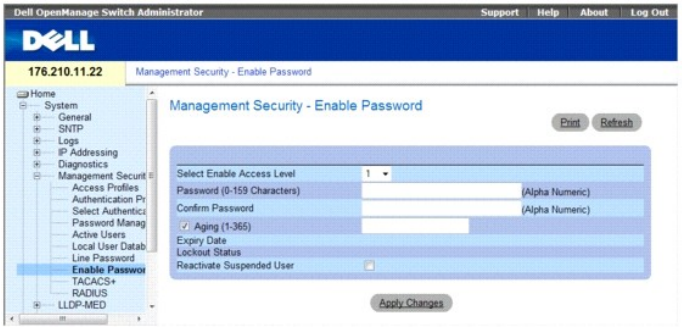
```
console(config-line)# password dell
```

Определение паролей включения

Страница **Enable Password** (Пароль включения) задает локальный пароль для управления доступом для конфигураций Normal (Обычная) и Privilege (С привилегиями).

Чтобы открыть страницу **Enable Password** (Пароль включения), выберите **System** (Система)→ **Management Security** (Безопасность управления)→ **Enable Passwords** (Пароли включения) на панели дерева.

Рис. 6-69. Страница Enable Password (Пароль включения)



Страница **Enable Password** (Пароль включения) содержит следующие поля.

- **Select Enable Access Level** (Выбор уровня доступа для включения). уровень доступа, связанный с паролем включения. Самый низкий уровень доступа пользователя - **1**, а самый высокий -**15**. Пользователи с уровнем доступа 15 являются привилегированными. Только эти пользователи имеют доступ к странице Dell OpenManage Switch Administrator.
- **Password (0-159 characters)** (Пароль (0-159 символов)). текущий пароль включения.
- **Confirm Password** (Подтвердить пароль). Подтверждения пароля. В целях безопасности пароль выводится в формате *****.
- **Aging (1-365)** (Срок действия пароля (1-365)). указывает срок действия пароля в днях.
  - **Флажок установлен**. срок действия пароля истекает после указанного количества дней.
  - **Флажок снят**. срок действия пароля не истек.
- **Expiry Date** (Дата окончания действия). указывает дату окончания действия пароля включения.
- **Lockout Status** (Состояние блокировки). указывает число неправильных попыток ввода пароля с момента последнего успешного входа в систему, если установлен флажок **Enable Login Attempts** (Включить контроль попыток ввода пароля) на странице **Password Management** (Управление паролями). Если вход в систему для пользователя заблокирован, отображается состояние **LOCKOUT** (Блокировка).
- **Reactivated Suspended User** (Возобновление приостановленных пользователей). возобновление права доступа указанного пользователя. Права доступа могут быть приостановлены после неудачной попытки входа в систему.
  - **Флажок установлен**. восстановить права доступа пользователя.
  - **Флажок снят**. пользователю отказано в доступе.

Определение нового пароля включения:

1. Откройте страницу **Enable Password** (Пароль включения).
2. Определите поля.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

   Новый пароль включения будет определен, а устройство обновлено.

Назначение паролей включения с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для настройки полей, отображаемых на странице **Enable Password** (Пароль включения).

Команда консоли	Описание
enable password [**level** *уровень*] *пароль* [**encrypted**]	Задает локальный пароль для управления доступом для уровней пользователей и привилегий.

Далее приведен пример команд консоли.

```
console(config)# enable password level 15 secret
```

Определение параметров TACACS+

Устройство предоставляет поддержку для клиентов TACACS+ (Terminal Access Controller Access Control System). TACACS+ обеспечивает централизованную систему безопасности для проверки пользователей, получающих доступ к устройству.

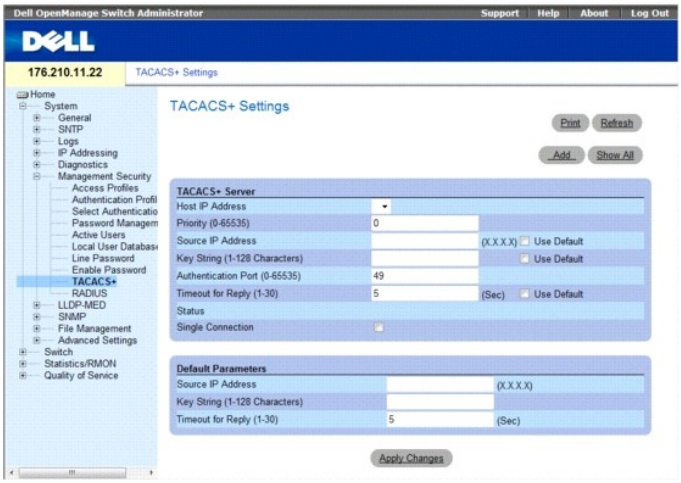
TACACS+ обеспечивает централизованную систему управления пользователями, при сохранении совместимости с сервером RADIUSи другими процедурами аутентификации. TACACS+ предоставляет следующие службы:

- **Authentication** (Проверка подлинности). обеспечивает проверку подлинности во время входа, а также по именам пользователей и определенным пользователями паролям.
- **Authorization** (Авторизация). выполняется при входе. После завершения сеанса проверки подлинности запускается сеанс авторизации с использованием проверенного имени пользователя. Сервер TACACS+ проверяет привилегии пользователя.

Протокол TACACS+ обеспечивает целостность сети благодаря обмену шифрованными данными протокола между устройством и сервером TACACS+.

Чтобы открыть страницу **TACACS+ Settings** (Параметры TACACS+), выберите **System** (Система)→ **Management Security** (Безопасность управления)→ **TACACS+** на панели дерева.

Рис. 6-70. Страница TACACS+ Settings (Параметры TACACS+)



Страница параметры **TACACS+** содержит следующие поля.

- **Host IP Address** (IP-адрес хоста). указывает IP-адрес сервера TACACS+.
- **Priority (0-65535)** (Приоритет). определяет порядок, в котором используются серверы TACACS+. Значение по умолчанию: 0.
- **Source IP Address** (IP-адрес источника). IP-адрес устройства источника, используемый для сеанса TACACS+ между устройством и сервером TACACS+.
- **Key String (1-128 Characters)** (Строка ключа (1-128 символов)). определяет проверку подлинности и ключ шифрования обмена данными TACACS+ между устройством и сервером TACACS+. Этот ключ должен соответствовать ключу шифрования, используемому для сервера TACACS+. Этот ключ закодирован.
- **Authentication Port (0-65535)** (Порт проверки подлинности). порт проверки подлинности, через который осуществляется обмен данными во время сеансов TACACS+. По умолчанию это порт 49.
- **Timeout for Reply (1-30)** (Время для ответа). время ожидания ответа при обмене данными между устройством и сервером TACACS+. Диапазон значений: 1-30 секунд.
- **Status** (Состояние). состояние соединения между устройством и сервером TACACS+. Возможные значения:
  - **Connected** (Соединение установлено). между устройством и сервером TACACS+ установлено соединение.
  - **Not Connected** (Соединение не установлено). отсутствует соединение между устройством и сервером TACACS+.
- **Single Connection** (Одно соединение). Если выбран этот параметр, поддерживается одно открытое соединение между устройством и сервером TACACS+.
- **Use Default** (Использовать стандартные установки). Использует стандартное значение этого параметра.

В качестве параметров TACACS+ по умолчанию используются параметры по умолчанию, определенные пользователем. Параметры по умолчанию

применяются для вновь определенных серверов TACACS+. Если значения по умолчанию не определены, для новых серверов TACACS+ используются системные настройки по умолчанию.

Далее показаны настройки TACACS+ по умолчанию:

- **Source IP Address** (IP-адрес источника). IP-адрес устройства источника, используемый по умолчанию для сеанса TACACS+ между устройством и сервером TACACS+. IP-адрес источника по умолчанию 0.0.0.0.
- **Key String (1-128 Characters)** (Строка ключа (1-128 символов)). строка ключа по умолчанию, используемая для проверки подлинности и шифрования всех связей между устройством и сервером TACACS+. Этот ключ закодирован.
- **Timeout for Reply (1-30)** (Время для ответа (1-30)). время ожидания ответа при обмене данным между устройством и сервером TACACS+ до окончания действия связи. Значение по умолчанию: 5 секунд.

Добавление сервера TACACS+

1. Откройте страницу **TACACS+ Settings** (Параметры TACACS+).
2. Нажмите кнопку **Add** (Добавить).

   Откроется страница **Add TACACS+ Host** (Добавление хоста TACACS+) .

   Рис. 6-71. Страница Add TACACS+ Host (Добавление хоста TACACS+)

3. Определите поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

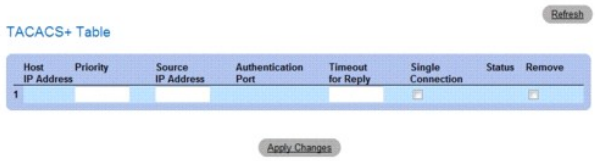
   Будет добавлен сервер TACACS+, а устройство будет обновлено.

Отображение таблицы TACACS+

1. Откройте страницу **TACACS+ Settings** (Параметры TACACS+).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **TACACS+ Table** (Таблица TACACS+).

   Рис. 6-72. TACACS+ Table (Таблица TACACS+)



Удаление сервера TACACS+

1. Откройте страницу **TACACS+ Table** (Таблица TACACS+).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **TACACS+ Table** (Таблица TACACS+).

3. Выберите запись таблицы **TACACS+ Table**.
4. Установите флажок **Remove** (Удалить).
5. Нажмите кнопку **Apply Changes** (Применить изменения).

   Будет удален сервер TACACS+, а устройство будет обновлено.

Определение параметров TACACS+ с помощью команд консоли

В следующей таблице приведены команды консоли для настройки полей, отображаемых на странице **TACACS+ Settings** (Параметры TACACS+).

Команда консоли	**Описание**
tacacs-server host {*ip-адрес* |*имя_хоста*} [**single-connection**] [**port** *номер_порта*] [**timeout** *тайм-аут*] [**key** *строка_ключа*] [**source** *источник*] [**priority** *приоритет*]	Указывает хост TACACS+.
tacacs-server key *строка ключа*	Отображает проверку подлинности и ключ шифрования для всех обменов данными TACACS+ между устройством и сервером TACACS+. Этот ключ должен соответствовать шифрованию, используемому для демона TACACS+. (Диапазон: 0 - 128 символов.)
tacacs-server timeout *время ожидания*	Отображает значение времени ожидания в секундах. (Диапазон: 1 - 30.)
tacacs-server source-ip *источник*	Отображает IP-адрес источника. (Диапазон: допустимый IP-адрес.)
show TACACS [*ip-адрес*]	Отображает настройку и статистику для сервера TACACS+.

Далее приведен пример команд консоли.

```
console# show tacacs

Device Configuration (Конфигурация устройства)

IP address      Status          Port  Single Connection  TimeOut  Source IP     Priority
-----------     ---------       ----  -----------------  -------  ---------     --------
12.1.1.2        Not Connected   49    Yes                1        12.1.1.1      1

Global values
-----------------
TimeOut : 5

Device Configuration (Конфигурация устройства)
--------------------
Source IP : 0.0.0.0
console#
```

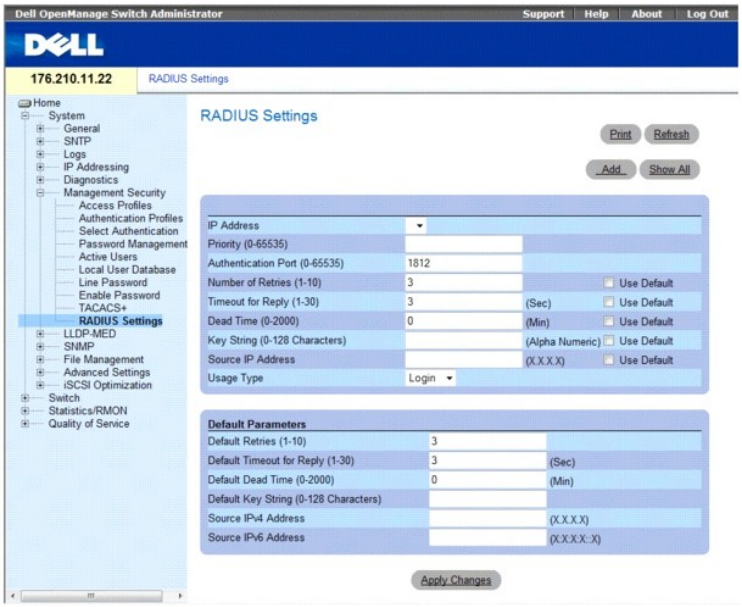
Настройка параметров RADIUS

Серверы RADIUS (RADIUS - Remote Authorization Dial-In User Service) обеспечивают дополнительную защиту сетей. Можно определить до 4 серверов RADIUS. Серверы RADIUS обеспечивают централизованный метод проверки подлинности:

- для доступа Telnet
- для доступа через безопасный командный процессор
- для доступа по Интернету
- для доступа через консоль

Чтобы открыть страницу **RADIUS Settings** (Параметры RADIUS), выберите **System** (Система)→ **Management Security** (Безопасность управления)→ **RADIUS** на панели дерева.

Рис. 6-73. Страница RADIUS Settings (Параметры RADIUS)



Страница **RADIUS Settings** (Параметры RADIUS) содержит следующие страницы:

- **IP Address** (IP-адрес). список IP-адресов серверов для проверки подлинности.
- **Priority (0-65535)** (Приоритет). приоритет сервера. Возможные значения: от 0до 65535, где 0 - наибольшее значение. Используется для настройки порядка, в котором серверы выстраиваются в очередь.
- **Authentication Port (0-65535)** (Порт авторизации). Определяет порт проверки подлинности. Порт проверки подлинности используется для проверки подлинности сервера RADIUS.
- **Number of Retries (1-10)** (Число повторных попыток). число запросов, переданных серверу RADIUS, прежде чем произошла ошибка. Возможные значения: 1 - -10.
- **Timeout for Reply (1-30**) (Время для ответа). отображает время в секундах, в течение которого устройство ожидает ответа от сервера RADIUS перед повторным запросом или переключением на следующий сервер. Возможные значения поля: 1- 30.
- **Dead Time (0-2000)** (Время отключения). отображает время (в секундах), в течение которого сервер RADIUS не принимает запросы на обработку. Диапазон значений: 0-2000.
- **Key String (0-128 Characters)** (Строка ключа (0-128 символов)). строка ключа, используемая для проверки подлинности и шифрования всех данных RADIUS, передаваемых между устройством и сервером RADIUS. Этот ключ закодирован.
- **Source IP Address** (IP-адрес источника). определяет исходный IP-адрес, который используется для связи с серверами RADIUS.
- **Usage Type** (Тип использования). Отображает тип использования сервера. Может быть задано одно из следующих значений: **login** (вход), **802.1x** или **all** (все). Если значение не указано, по умолчанию используется значение all (все).
- **Use Default** (Использовать стандартные установки). Использует стандартное значение этого параметра.

Если не указаны значения времени ожидания, числа попыток или времени отключения для конкретного хоста, для каждого хоста используются общие значения (по умолчанию). Следующие поля задают значения по умолчанию для RADIUS:

- **Default Retries (1-10)** (Число повторных попыток по умолчанию). число запросов по умолчанию, передаваемых серверу RADIUS, прежде чем отображается ошибка.
- **Default Timeout for Reply (1-30)** (Время для ответа по умолчанию). время по умолчанию (в секундах), в течение которого устройство ожидает ответа от сервера RADIUS. Значение по умолчанию: 5 секунд.
- **Default Dead Time (0-2000)** (Время отключения по умолчанию). время по умолчанию, в течение которого сервер RADIUS не принимает запросы на обработку. Диапазон значений: 0-2000.
- **Default Key String (0-128 Characters)** (Строка ключа по умолчанию (1-128 символов)). строка ключа по умолчанию, используемая для проверки подлинности и шифрования всех данных RADIUS, передаваемых между устройством и сервером RADIUS. Этот ключ закодирован.
- **Source IPv4 ddress** (IPv4-адрес источника). определяет исходный адрес IP версии 4, который используется для связи с серверами RADIUS.
- **Source IPv6 Address** (IPv6-адрес источника). определяет исходный адрес IP версии 6, который используется для связи с серверами RADIUS.

При определении нового сервера RADIUS server, будет доступен следующий дополнительный параметр:

- **Supported IP Format** (Поддерживаемый формат IP-адресов). Отображает формат IP-адресов, поддерживаемый сервером SNTP. Возможные значения:
  - **IPv6** Global (Глобальный адрес IPv6) — поддержка IP версии 6.
  - **IPv4**. поддержка IP версии 4.

Определение параметров RADIUS:

1. Откройте страницу **RADIUS Settings** (Параметры RADIUS).
2. Определите поля.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

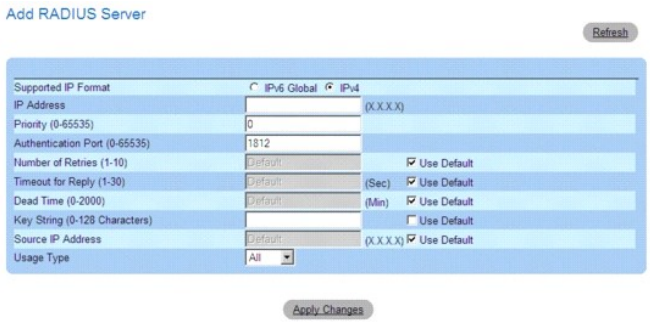
   Параметры RADIUS для данного устройства будут изменены.

Добавление сервера RADIUS:

1. Откройте страницу **RADIUS Settings** (Параметры RADIUS).
2. Нажмите кнопку **Add** (Добавить).

   Откроется страница **Add RADIUS Server** (Добавление сервера RADIUS).

   Рис. 6-74. Add RADIUS Server (Добавление сервера RADIUS)



3. Определите поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

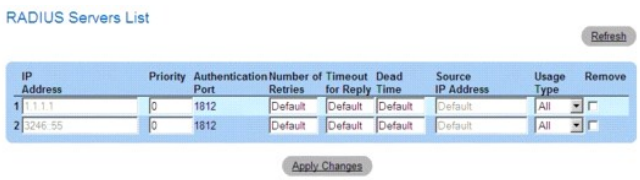
   Новый сервер RADIUS будет добавлен, а устройство обновлено.

Отображение списка серверов RADIUS:

1. Откройте страницу **RADIUS Settings** (Параметры RADIUS).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется список **RADIUS Servers List** (Список серверов RADIUS).

   Рис. 6-75. RADIUS Servers List (Список серверов RADIUS)



Удаление сервера RADIUS:

1. Откройте страницу **RADIUS Settings** (Параметры RADIUS).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется список **RADIUS Servers List** (Список серверов RADIUS).
3. Выберите запись списка **RADIUS Servers List** (Список серверов RADIUS).
4. Установите флажок **Remove** (Удалить).
5. Нажмите кнопку **Apply Changes** (Применить изменения).

   Будет удален сервер RADIUS, а устройство будет обновлено.

Определение серверов RADIUS с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для определения полей, отображаемых на странице **RADIUS Settings** (Параметры RADIUS).

Команда консоли	**Описание**
radius-server timeout количество_секунд *timeout*	Задает интервал для каждого устройства, ожидающего ответа хоста сервера.
radius-server source-ip источник	Определяет IPv4-адрес источника, который будет использоваться для связи с сервером RADIUS по протоколу IPv4.
radius-server source-ipv6 источник	Определяет IPv6-адрес источника, который будет использоваться для связи с сервером RADIUS по протоколу IPv6.
radius-server retransmit количество_попыток	Определяет, сколько раз программа выполняется поиск списка хостов с серверами RADIUS.
radius-server deadtime количество_секунд	Настраивает недоступные серверы так, чтобы они пропускались.
radius-server key строка_ключа	Задает проверку подлинности и ключ кодирования для всех связей RADIUS между маршрутизатором и сервером RADIUS.
radius-server host ip-адрес [**auth-port** номер_порта_идентификации] [**timeout** количество_секунд]] [**retransmit** количество_попыток] [**deadtime** количество_секунд] [**key** строка_ключа] [**source** источник] [**priority** приоритет]	Определяет хост сервера RADIUS.
show radius-servers	Отображает параметры сервера RADIUS.

Далее приведен пример команд консоли:

```
Console(config)# radius-server timeout 5

Console(config)# radius-server retransmit 5

Console(config)# radius-server deadtime 10

Console(config)# Console (config)# radius-server key dell-server dell-server

Console(config)# radius-server host 196.210.100.1 auth-port 127 timeout 20

Console# show radius-servers

IP address Auth Acct TimeOut Retransmit Deadtime Source IP Priority

-------- ---- ---- ------ --------- ------- ------- ------

172.16.1.1 164 51646 3 3 0 01 172.16.1.2 164 51646 3 3 0 02
```

Настройка LLDP и MED

Протокол LLDP позволяет сетевым администраторам выполнять поиск и устранение неисправностей и совершенствовать управление сетью путем выявления и сохранения топологии сети в средах, включающих оборудование самых разных поставщиков. С помощью протокола LLDP, используя стандартные методы, можно обнаружить сетевое окружение сетевых устройств, чтобы сообщить о них другим системам и сохранить обнаруженную информацию. Информация об устройствах включает следующее.

- Device Identification (Идентификатор устройства)
- Device Capabilities (Возможности устройства)
- Device Configuration (Конфигурация устройства)

Устройство рассылки запросов передает несколько наборов сообщений в одном пакете ЛВС. Для отправки нескольких наборов сообщений используется поле пакета Type Length Value (TLV) (Ввод значения длины). Устройства LLDP должны поддерживать сообщения о корпусе и идентификаторе порта, а также имя системы, идентификатор системы, описание системы и сообщения о возможностях системы.

В этом разделе рассмотрены следующие темы:

- Определение общих свойств LLDP
- Определение параметров порта для передачи пакетов LLDP
- Определение сетевой политики выявления конечной медиа-точки
- Определение параметров LLDP MED для порта
- Просмотр информации об окружении LLDP

Протокол LLDP Media Endpoint Discovery (LLDP-MED) повышает гибкость сети, обеспечивая различным системам IP возможность использовать один протокол LLDP.

Обеспечивает детальную информацию о топологии сети, включая сведения об устройствах сети и их местоположении: какой IP-телефон к какому порту подключен, какая программа работает на каком коммутаторе и какой порт к какому компьютеру подключен. Автоматически развертывает политики для сети для

- политик QoS;
- голосовых сетей VLAN

Обеспечивает службу экстренных вызовов (E-911), для которой используется информация о расположении IP-телефонов.

Предоставляет уведомления администраторам сети с информацией о поиске и устранении неисправностей при отправке данных по протоколу LLDP MED:

- Конфликты скорости порта и дуплексного режима
- Неправильная конфигурация политики QoS

В этом разделе имеются следующие тематические подразделы:

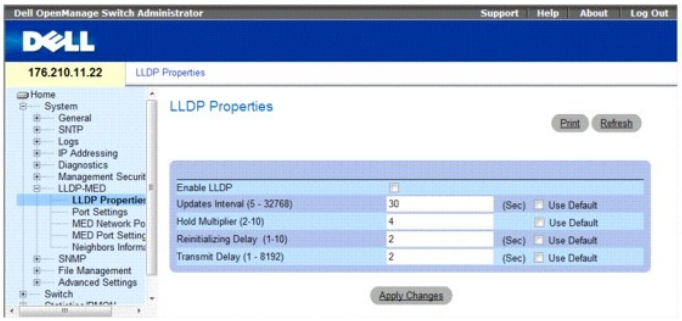
- Определение свойств LLDP
- Конфигурация LLDP с помощью команд консоли
- Определение параметров порта для передачи пакетов LLDP
- Определение сетевой политики для протокола LLDP MED
- Определение параметров LLDP MED для порта
- Просмотр информации об окружении LLDP

Определение свойств LLDP

Страница **LLDP Properties** (Свойства LLDP) содержит поля для конфигурации LLDP.

Чтобы открыть страницу **LLDP Properties** (Свойства LLDP), выберите **System** (Система)→ **LLDP-MED**→ **LLDP Properties** (Свойства LLDP) на панели дерева.

Рис. 6-76. LLDP Properties (Свойства LLDP)



- **Enable LLDP** (Включить LLDP). указывает, включен ли LLDP на устройстве. Возможные значения:
  - **Отмечен**. LLDP включен на устройстве.
  - **Не отмечен**. LLDP отключен на устройстве. Это значение по умолчанию.
- **Updates Interval (5-32768)** (Обновление интервала (5-32768)). указывает частоту отправки обновлении объявлений через протокол LLDP. Возможные значения поля: 5 - 32768 секунд. Значение по умолчанию: 30 секунд.

- **Hold Multiplier (2-10)** (Коэффициент удержания). Указывает время удержания, которое пересылается в пакетах обновления LLDP, в виде множителя времени таймера. Возможные значения поля: 2-10. Значение по умолчанию: 4.
- **Reinitializing Delay (1-10)** (Задержка повторной инициализации). Указывает минимальное время в секундах, которое выжидает порт LLDP до передачи повторной инициализации. Возможные значения поля: 1 - 10 секунд. Значение по умолчанию: 2 секунды.
- **Transmit Delay (1-8192)** (Задержка передачи). указывает период времени между последовательными передачами кадров LLDP в соответствии с изменениями в базе локальных систем LLDP MIB. Возможные значения поля: 1 - 8192 секунд. Значение по умолчанию: 2 секунды.

Конфигурация LLDP с помощью команд консоли

Таблица 6-43. Команды консоли для свойств LLDP

Команда консоли	Описание
`lldp enable (global)`	Включает протокол обнаружения каналов передачи данных.
`lldp hold-multiplier` `число`	Указывает время, в течение которого получающее устройство должно хранить пакет протокола обнаружения каналов передачи данных (LLDP) до его удаления.
`lldp reinit-delay` `Секунды`	Указывает минимальный период времени ожидания повторной инициализации для порта LLDP.
`lldp tx-delay Секунды`	Указывает время между последовательными передачами кадров LLDP.

Далее приведен пример команд консоли.

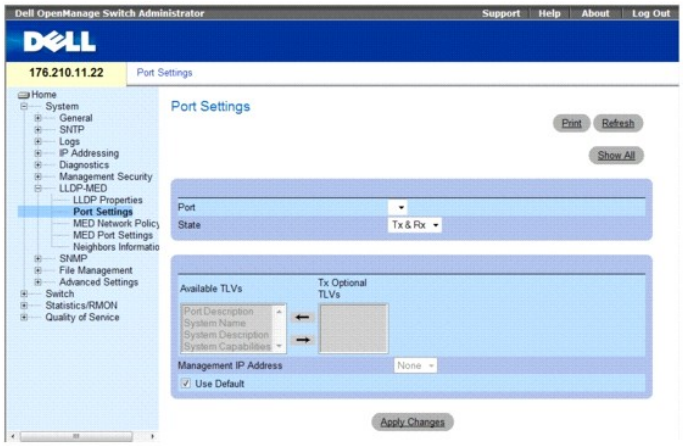
```
Console (config)# interface ethernet g1

Console(config-if)# lldp enable
```

Определение параметров порта для передачи пакетов LLDP

Страница **LLDP Port Settings** (Параметры порта для передачи пакетов LLDP) позволяет сетевым администраторам определять параметры порта для передачи пакетов LLDP, включая номер порта, номер порта для передачи пакетов LLDP и тип передаваемой через порт информации.

Страница **Port Settings** (Параметры порта) содержит поля для конфигурации LLDP. Чтобы открыть страницу **Port Settings** (Параметры порта), выберите **System** (Система)→ **LLDP-MED**→ **Port Settings** (Параметры порта) на панели дерева**.**

Рис. 6-77. Параметры порта



- **Port** (Порт). список портов, для которых включен протокол LLDP.
- **State** (Состояние). тип порта, для которого включен протокол LLDP. Возможные значения:
  - **Tx Only** (Только передача). возможна только передача пакетов LLDP.
  - **Rx Only** (Только прием). возможен только прием пакетов LLDP.
  - **Tx & Rx** (Передача и прием). возможны передача и прием пакетов LLDP packets. Это значение по умолчанию.
  - **Disable** (Отключить). протокол LLDP отключен для порта.
- **Available TLVs** (Доступные поля TLV). список доступных полей TLV, которые могут использоваться портом для объявлений. Возможные значения:
  - **Port Description** (Описание порта). объявляет описание порта.

- **System Name** (Имя системы). объявляет имя системы.
- **System Description** (Описание системы). объявляет описание системы.
- **System Capabilities** (Возможности системы). объявляет возможности системы.

- **Tx Optional TLVs** (Дополнительные TLV для передачи). список дополнительных TLV, объявленых портом. Полный список см. в поле **Available TLVs** (Доступные TLV).
- **Management IP Address** (IP-адрес управления). указывает IP-адрес управления, объявленный с интерфейса.
  - **Use Default** (Использовать стандартную установку). указывает способ включения TLV:
  - **Флажок установлен**. по умолчанию используются только обязательные TLV, они определяются типом аппаратного обеспечения (MAC-адресом), подтипом порта (номером порта), и временем до выхода TTL (оно равно120 с).
  - **Флажок снят**. TLV, определяемые пользователем, состоящие из 3 вышеописанных обязательных типов TLV и дополнительных TLV, которые перемещаются пользователем из доступного набора TLV.

На странице **LLDP Port Table** (Таблица портов LLDP) отображается конфигурация порта для передачи пакетов LLDP. Чтобы открыть страницу **LLDP Port Table** (Таблица портов LLDP), выберите **Security** (Безопасность)→ **LLDP**→ **Port Settings** (Параметры порта)→ **Show All** (Показать все) на панели дерева**.**

Рис. 6-78. Таблица портов LLDP

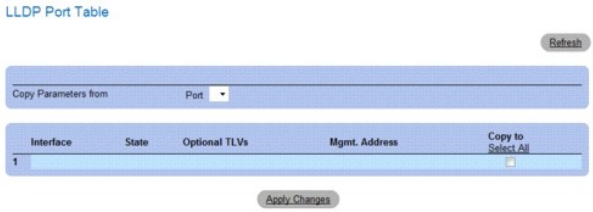


Таблица 6-44. Команды консоли для параметров портов LLDP

Команда консоли	**Описание**
clear lldp rx interface	Перезапускает устройство получения пакетов LLDP и выполняет очистку таблицы окружения.
lldp optional-tlv *tlv1 [tlv2 ... tlv5]*	Указывает, передачу каких дополнительных TLV из базового набора необходимо выполнить.
lldp enable [rx | tx | both]	Включает протокол обнаружения каналов передачи данных (LLDP) для интерфейса.

Далее приведен пример команд консоли.

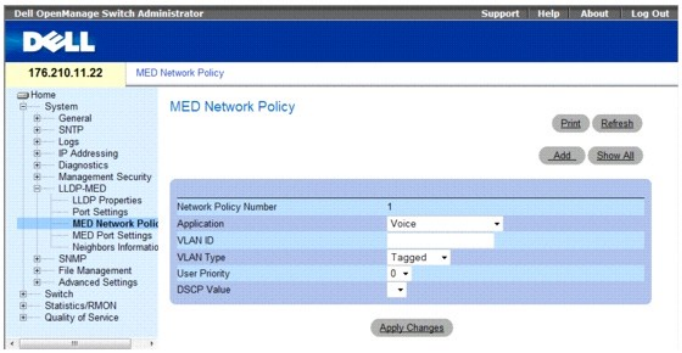
```
Console (config)# interface ethernet g1

Console(config-if)# lldp enable
```

Определение сетевой политики для протокола LLDP MED

Страница **MED Network Policy** (Сетевая политика MED) содержит поля для конфигурации LLDP.

Чтобы открыть страницу **MED Network Policy** (Сетевая политика MED), выберите **System** (Система)→ **LLDP-MED**→ **MED Network Policy** (Сетевая политика MED) на панели дерева**.**

Рис. 6-79. Сетевая политика MED



Страница *MED Network Policy (Сетевая политика MED)* содержит следующие поля:

- **Network Policy Number** (Номер сетевой политики). отображается номер сетевой политики.
- **Application** (Приложение). отображается приложение, для которого определяется сетевая политика. Возможные значения:
  - ***Voice*** (Голос). указывает, что сетевая политика определяется для голосового приложения.
  - ***Voice Signaling*** (Голосовые сигналы). указывает, что сетевая политика определяется для приложения голосовых сигналов.
  - ***Guest Voice*** (Голос с подключенного устройства). указывает, что сетевая политика определяется для приложения приема голоса с подключенного устройства.
  - ***Guest Voice Signaling*** (Голосовые сигналы с подключенного устройства). указывает, что сетевая политика определяется для приложения приема голосовых сигналов с подключенного устройства.
  - ***Softphone Voice*** (Голос с программного телефона). указывает, что сетевая политика определяется для приложения приема голоса с программного телефона.
  - ***Video Conferencing*** (Видео конференции). указывает, что сетевая политика определяется для приложения видео-конференций.
  - ***Streaming Video*** (Потоковое видео). указывает, что сетевая политика определяется для приложения потокового видео.
  - ***Video Signaling*** (Видеосигналы). указывает, что сетевая политика определяется для приложения приема видеосигналов.
- **VLAN ID** (ID VLAN). отображает ID VLAN, для которой определяется сетевая политика.
- **VLAN Type** (Тип VLAN). отображает тип VLAN, для которой определяется сетевая политика. Возможные значения:
  - ***Отмечен***. указывает, что сетевая политика определена для отмеченных VLAN.
  - ***Не отмечен***. указывает, что сетевая политика определена для неотмеченных VLAN.
- **User Priority** (Приоритет пользователя). определяет приоритет, назначенный для сетевого приложения. Диапазон значений: 0-7.
- **DSCP Value** (Значение DSCP). определяет значение DSCP, назначенное для сетевой политики. Диапазон значений: 0-63.

Добавление сетевой политики MED

1. Откройте страницу **MED Network Policy** (Сетевая политика MED).
2. Нажмите кнопку **Add** (Добавить).

   Отобразится страница *Add Network Policy* (Добавление сетевой политики).

   Рис. 6-80. Добавление сетевой политики

3. Определите поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Новая сетевая политика будет добавлена, а устройство - обновлено.

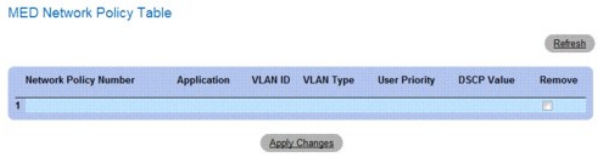
Отображение таблицы сетевой политики MED:

1. Откройте страницу **MED Network Policy** (Сетевая политика MED).

2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **MED Network Policy Table** (Таблица сетевой политики MED).

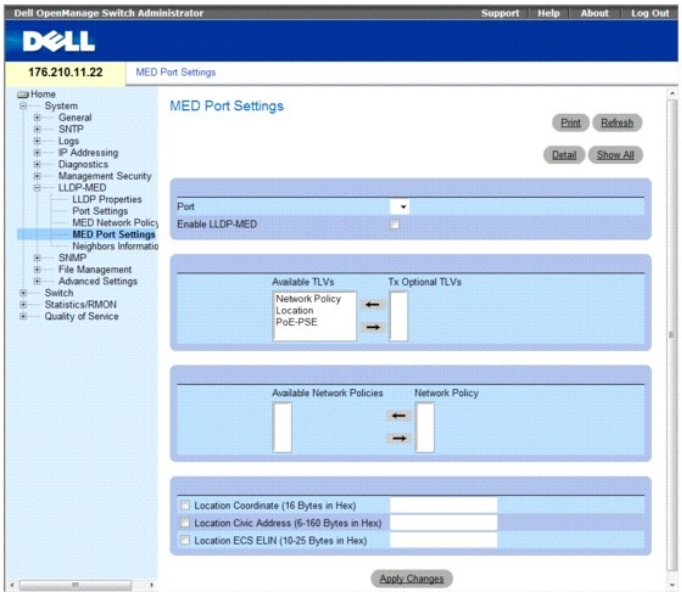
Рис. 6-81. MED Network Policy Table (Таблица сетевой политики MED)



Определение параметров LLDP MED для порта

Страница **MED Port Settings** (Параметры порта MED) содержит параметры для назначения сетевых политик LLDP определенным портам. Чтобы открыть страницу **Port Settings** (Параметры MED для порта), выберите **System** (Система)→ **LLDP-MED** → **Port Settings** (Параметры порта) на панели дерева. Откроется страница **MED Port Settings** (Параметры MED для порта).

Рис. 6-82. MED Port Settings (Параметры MED для порта)



На странице MED Port Settings (Параметры MED для порта) содержатся следующие поля:

- **Port** (Порт). отображает порт, для которого включен или выключен протокол LLDP-MED.
- **Enable LLDP-MED** (Включить LLDP-MED). обозначает, включен ли протокол LLDP-MED для выбранного порта. Возможные значения:
  - **Флажок установлен**. включает протокол LLDP-MED для порта.
  - **Флажок снят**. выключает протокол LLDP-MED для порта. Это значение по умолчанию.
- **Tx Optional TLVs / Available TLVs** (Дополнительные TLV для передачи/доступные поля TLV). список доступных полей TLV, которые могут использоваться портом для объявлений. Возможные значения:
  - **Network Policy** (Сетевая политика). сетевая политика, связанная с портом.
  - **Location** (Местоположение). местоположение порта.
  - **PoE-PSE**. Отображает подключенное устройство как устройство PoE или устройство PSE (Питающее оборудование).
- **Network Policy / Available Network Policy** (Сетевая политика/доступная сетевая политика). содержит список сетевых политик, который можно назначить для порта.
- **Location Coordinate (16 Bytes in Hex)** (Координата места положения, 16-битное 16-ричное число). отображает координаты места положения устройства в виде 16-битного 16-ричного числа.
- **Location Civic Address (6-160 Bytes in Hex)** (Адрес местоположения, 6-160 битовое 16-ричное число). отображает город или название улицы для устройства, например 414 23rd Ave E. Возможное значение поля: 6 - 160 символов.
- **Location ECS ELIN (10-25 Bytes in Hex)** (Местоположение ECS ELIN, 10-25 битное 16-ричное число). отображает местоположение ECS ELIN

устройства. Возможные значения поля: 10-25.

Изменение параметров MED для порта

1. Откройте страницу **MED Port Settings** (Параметры MED для порта).
2. Измените поля.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

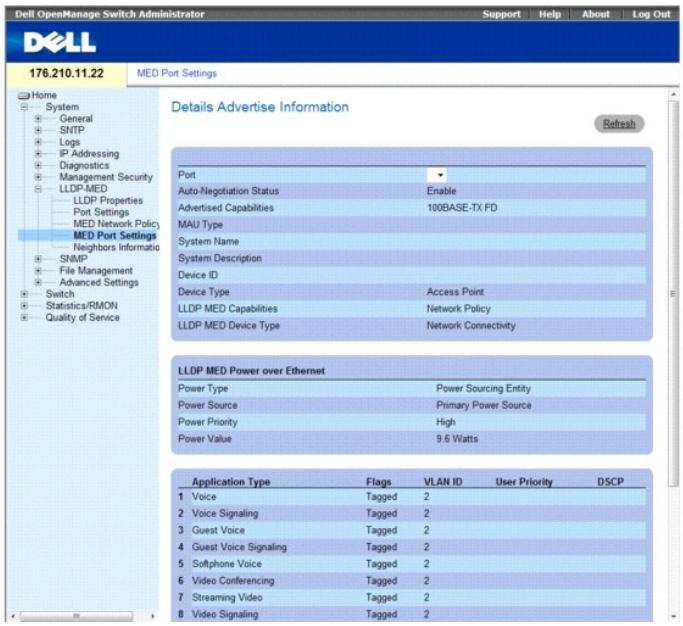
   Параметры будут сохранены а память этого устройства.

Отображение параметров объявляемой информации

1. Откройте страницу **MED Port Settings** (Параметры MED для порта).
2. Нажмите **Details** (Подробные сведения).

   Откроется страница **Details Advertise Information** (Объявляемая информация):

   Рис. 6-83. Страница Details Advertise Information Page (Объявляемая информация)



Страница **Details Advertise Information** (Объявляемая информация) содержит следующие поля.

- **Port** (Порт). порт, для которого отображается подробная информация.
- **Auto-Negotiation Status** (Состояние автоматического согласования). состояние автоматического согласования для порта. Возможные значения:
  - **Enabled** (Включено). автоматическое согласование включено для порта.
  - **Disabled** (Выключено). автоматическое согласование выключено для порта.
- **Advertised Capabilities** (Характеристики объявления). характеристики, объявляемые для порта.
- **MAU Type** (Тип MAU). обозначает тип устройства для подключения к линии связи.
- **System Name** (Имя системы). Объявляемое системное имя.
- **System Description** (Описание системы). объявляет описание системы.
- **Device ID** (Идентификатор устройства). объявляет идентификатор устройства, например, MAC-адрес.
- **Device Type** (Тип устройства). тип устройства.
- **LLDP MED Capabilities** (Характеристики LLDP MED). TLV, объявляемый портом.
- **LLDP MED Device Type** (Тип устройства LLDP MED). обозначает, является ли отправитель устройством с сетевым подключением или устройством,

подключенным к конечной точке.

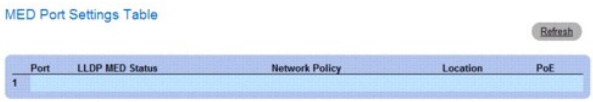
- **Power Type** (Тип питания). Тип питания порта.
- **Power Source** (Состояние питания). состояние источника питания.
- **Power Priority** (Приоритет питания). Уровень приоритета питания порта.
- **Power Value** (Мощность питания порта). Мощность питания порта в ваттах.
- **LLDP MED Network Policy** (Сетевая политика LLDP MED). сетевая политика LLDP порта для каждого из следующих типов применения:
  - Голос
  - Голосовые сигналы
  - Голос с подключенного устройства
  - Голосовые сигналы с подключенного устройства
  - Голос с программного телефона
  - Видео конференции
  - *Потоковое видео*
  - *Видеосигналы*
- **Flags** (Флажки). Отображает статус тегирования сети VLAN для данного типа приложения. Возможные значения:
  - ***Отмечено***. Пакеты помечены.
  - ***Не отмечено***. Пакеты не помечены.
- **VLAN ID** (Идентификатор сети VLAN). Отображает номер VLAN для данного типа приложения.
- **User Priority** (Приоритет пользователя). Отображает номер VLAN для данного типа приложения.
- **DSCP Value** (Значение DSCP). определяет значение DSCP, назначенное для сетевой политики. Возможные значения поля: 1-64.
- **LLDP MED Location** (Местоположение LLDP MED). объявленное местоположение LLDP порта.
  - ***Coordinates*** (Координаты). отображает координаты местоположения устройства.
  - ***Civic Address*** (Городской адрес). отображает город или название улицы для устройства, например 414 23rd Ave E. Возможное значение поля: 6 - 160 символов.
  - ***ECS ELIN***. отображает местоположение ECS ELIN устройства. Диапазон значений поля: 10 - 25.

Отображение таблицы параметров MED для порта:

1. Откройте страницу **MED Port Settings** (Параметры MED для порта).
2. Нажмите кнопку **Show All** (Показать все).

Откроется страница **MED Port Settings Table** (Таблица параметров MED для порта).

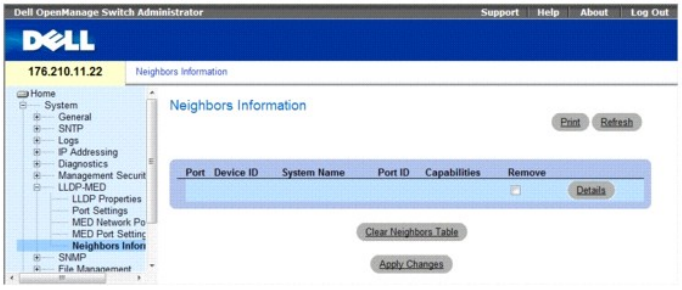
Рис. 6-84. MED Port Settings Table (Таблица параметров MED для порта)



Просмотр информации об окружении LLDP

Страница **Neighbors Information** (Информация об окружении) содержит сведения, полученные от близлежащих объявлений LLDP для устройства. Чтобы открыть страницу **Neighbor Information** (Информация об окружении), выберите **System** (Система)→ **LLDP-MED**→ **Neighbors Information** (Информация об окружении) на панели дерева**.**

Рис. 6-85. Страница Neighbors Information (Информация об окружении)



- **Port** (Порт). Отображает номер порта, для которого отображается информация об окружении.
- **Device ID** (Идентификатор устройства). отображает идентификатор соседнего устройства.
- **System Name** (Имя системы). отображает имя соседней системы.
- **Port ID** (Идентификатор порта). отображает идентификатор соседнего порта
- **Capabilities** (Возможности). отображает возможности соседнего устройства.

Удаление порта в таблице.

1. Откройте страницу **Neighbors Information** (Информация об окружении).
2. Установите флажок **Remove** (Удалить) рядом с каждым портом, который требуется удалить.
3. Нажмите кнопку **Apply Changes** (Применить изменения). Порты будут удалены.

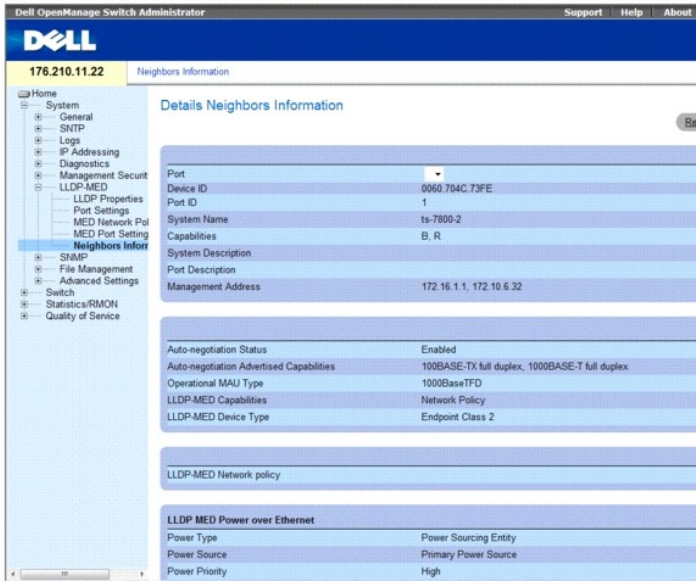
Очистка таблицы.

1. Откройте страницу **Neighbors Information** (Информация об окружении).
2. Выберите **Clear Neighbors Table** (Очистить таблицу соседей). Таблица будет очищена.

Просмотр подробной информации о LLDP MED, объявленной соседним устройством.

1. Откройте страницу **Neighbors Information** (Информация об окружении).
2. Нажмите кнопку **Details** (Подробности) рядом с нужной записью. Откроется страница Details Neighbor Information (Подробная информация об окружении).

Рис. 6-86. Страница Details Neighbors Information (Подробная информация об окружении)



Для получения информации о полях см. страницу Details Advertise Information (Объявляемая информация) выше.

Таблица 6-45. Команды консоли для информации об окружении LLDP

Команда консоли	Описание
`show lldp neighbors interface`	Отображает информацию о соседних устройствах, обнаруженных с помощью протокола LLDP (Link Layer Discovery Protocol).

Далее приведен пример команд консоли.

Port	Идентификатор устройства	Идентификатор порта	Имя системы	Возможности
3/e31	00:00:77:77:00:00	1/g3		0

Определение параметров SNMP

Протокол SNMP (Simple Network Management Protocol) обеспечивает способ управления устройствами в сети. Устройство поддерживает следующие версии протокола SNMP:

- SNMPv1 (версия 1)
- SNMPv2 (версия 2)
- SNMPv3 (версия 3)

SNMP версии 1 и версии 2

Агенты SNMP хранят список переменных, которые используются для управления устройством. Эти переменные задаются в базе данных Management Information Base (MIB). База данных MIB содержит переменные, которые контролируются агентом. Агент задает SNMP формат спецификации MIB и формат для доступа к информации через сеть. Управление правами доступа к агенту SNMP осуществляется с помощью строк доступа.

SNMPv1 и v2 включены по умолчанию.

SNMP версии 3

По протоколу SNMP версии 3 также осуществляется контроль доступа и применяется новый механизм системных прерываний для устройств распределения питания (PDU), поддерживающих протоколы SNMP версии 1 и 2. Кроме того, для протокола SNMP версии 3 определяется модель USM (User Security Model), которая включает в себя следующее.

- **Authentication** (Проверка подлинности). обеспечивает сохранность и проверку подлинности источника данных.
- **Privacy** (Конфиденциальность). предотвращает раскрытие содержания сообщения. Для шифрования используется режим CBC (Cipher-Bock-

Chaining). Для сообщения по протоколу SNMP включается или проверка подлинности, или и проверка подлинности, и конфиденциальность данных. Однако функция обеспечения конфиденциальности не может быть включена без проверки подлинности.

- **Timeliness** (Своевременность). предотвращает отсрочку или дублирование сообщений. Агент SNMP сравнивает входящее сообщение с данными о времени сообщения.
- **Key Management** (Управление ключами). генерация ключа, обновления ключа и использование ключа.

Коммутатор поддерживает фильтры уведомлений SNMP на основе идентификаторов объекта (OID). Система использует идентификаторы объекта (OID) для управления функциями коммутатора. Протокол SNMP версии 3 поддерживает следующие функции.

- Безопасность
- Функция контроля доступа
- Системные прерывания

Ключи проверки подлинности и конфиденциальности изменяются в модели **USM (User Security Model)** протокола SNMP версии 3.

SNMPv3 может быть включен, если включен идентификатор механизма Local Engine ID.

В этом разделе имеются следующие тематические подразделы:

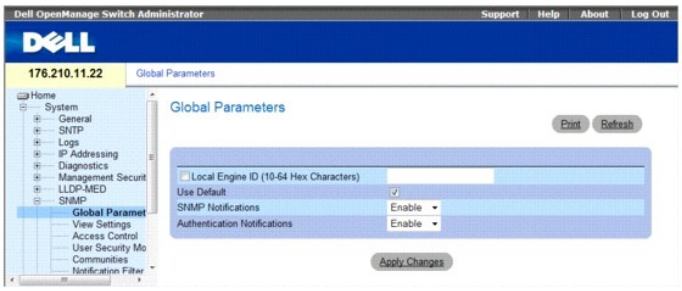
- Определение общих параметров SNMP
- Определение параметров представления SNMP
- Определение контроля доступа по протоколу SNMP
- Назначение уровня безопасности SNMP пользователя
- Определение сообществ SNMP
- Определение фильтров уведомлений SNMP
- Определение получателей уведомлений SNMP

Определение общих параметров SNMP

На странице **SNMP Global Parameters** (Общие параметры SNMP) можно включить уведомления о SNMP и о проверке подлинности.

Чтобы открыть страницу **SNMP Global Parameters** (Общие параметры SNMP), выберите **System** (Система)→ **SNMP**→ **Global Parameters** (Общие параметры) на панели дерева.

Рис. 6-87. Общие параметры SNMP



Страница **SNMP Global Parameters** (Общие параметры SNMP) содержит следующие поля:

- **Local Engine ID (10 - -64 Hex Characters)** (Идентификатор механизма на локальном устройстве (10 - 64 шестнадцатеричных символов)) - указывает идентификатор механизма на локальном устройстве. Значение этого поля является шестнадцатеричным. Каждый байт в строке шестнадцатеричного символа - это две шестнадцатеричных цифры. Каждый байт должен быть разделен точкой или двоеточием. Идентификатор механизма должен быть определен перед включением протокола SNMP версии 3.
  - Для автономных устройств выберите идентификатор механизма по умолчанию, который состоит из номера предприятия и MAC-адреса по умолчанию.
  - Для стековой системы следует настроить идентификатор механизма и проверить, что этот идентификатор является уникальным для домена администрирования. Это предотвращает появление в сети двух устройств с одинаковыми идентификаторами механизма.
- **Use Default** (Использовать стандартные установки). выберите эту опцию для того, чтобы использовать идентификатор механизма, сгенерированный устройством. Идентификатор механизма по умолчанию состоит из MAC-адреса устройства и определяется стандартом:
  - **Первые 4 октета**. первый бит = 1, остальные - номер предприятия IANA = 674.
  - **Пятый октет**. задайте значение 3, чтобы указать последующий MAC-адрес.
  - **Последние 6 октетов**. MAC-адрес устройства.
- **SNMP Notifications** (Уведомления SNMP). включает или отключает отправку маршрутизатором уведомлений SNMP.

- **Authentication Notifications** (Уведомления о проверке подлинности). включает или отключает отправку маршрутизатором системных прерываний SNMP при ошибке проверки подлинности.

Включение уведомлений SNMP

1. Откройте страницу **SNMP Global Parameters** (Общие параметры SNMP).
2. Выберите **Enable** (Включить) в поле **SNMP Notifications** (Уведомления SNMP).
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Уведомления SNMP будут включены, а устройство - обновлено.

Включение уведомлений о проверке подлинности

1. Откройте страницу **SNMP Global Parameters** (Общие параметры SNMP).
2. Выберите **Enable** (Включить) в поле **SNMP Notifications** (Уведомления SNMP).
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Включение уведомлений SNMP с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для просмотра полей на странице SNMP Global Parameters (Общие параметры SNMP).

Команда консоли	**Описание**
snmp-server enable traps	Разрешает маршрутизатору отправлять системные прерывания SNMP (Simple Network Management Protocol).
snmp-server trap authentication	Разрешает маршрутизатору отправлять системные прерывания SNMP (Simple Network Management Protocol) при ошибке проверки подлинности.
show snmp	Выполняет проверку состояния соединений по протоколу SNMP.
snmp-server engine ID local {*строка-идентификатора-механизма* | **default**}	Указывает идентификатор механизма на локальном устройстве. Значение этого поля является шестнадцатеричным. Каждый байт в строке шестнадцатеричного символа - это две шестнадцатеричных цифры. Каждый байт должен быть разделен точкой или двоеточием. Идентификатор механизма должен быть определен перед включением протокола SNMP версии 3.

Далее приведен пример команд консоли.

```
Console(config)# snmp-server enable traps

Console(config)# snmp-server trap authentication

Console# show snmp

Community-String        Community-Access        View name       IP address
----------------        ----------------        ---------       ----------
public                  read only               view-1          All

Community-String        Group name              IP address      Type
----------------        ----------              ----------      ----

Traps are enabled.
Authentication-failure trap is enabled.

Version 1,2 notifications
Target Address  Type  Community  Version  Udp Port  Filter name  To Sec  Retries
-------         ----  ---------  -------  ----      ------       ---     -------
```

Version 3 notifications							
Target Address	Type	Username	Security Level	Udp Port	Filter name	To Sec	Retries
--------	----	---------	--------	-----	-------	---	-------
System Contact: Robert							
System Location: Marketing							

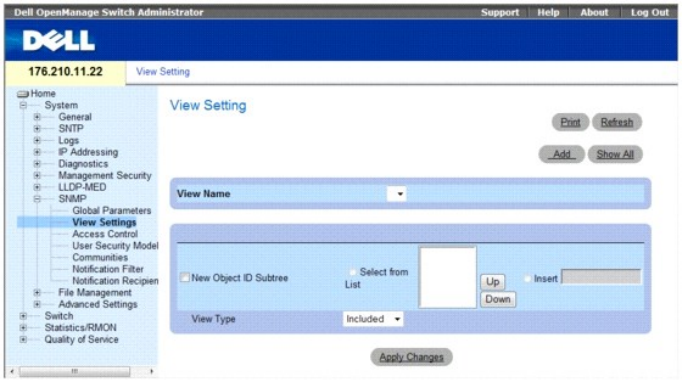
Определение параметров представления SNMP

Представления SNMP обеспечивают или блокируют доступ к функциям устройства или аспектам функций. Например, можно определить представление, которое устанавливает, что SNMP-группа A имеет доступ к группам многоадресной передачи только для чтения, тогда как SNMP-группа B имеет доступ к группам многоадресной передачи с возможностью чтения и записи. Доступ к функциям предоставляется с помощью имени MIB или идентификатора объекта MIB.

С помощью стрелок вверх и вниз можно выполнять навигацию в MIB-дереве и переходить между ветвями MIB-дерева.

Чтобы открыть страницу **SNMPv3 View Settings** (Параметры представления SNMP версии 3), выберите **System** (Система)→ **SNMP**→ **View Settings** (Параметры представлений SNMP) на панели дерева.

Рис. 6-88. Параметры представления SNMP версии 3



Страница **SNMPv3 View Settings** (Параметры SNMPv3) содержит следующие поля:

- **View Name** (Имя представления). содержит список видов, определенных пользователем. Имя представления может содержать не более 30 буквенно-цифровых символов.
- **New Object ID Subtree** (Новая ветвь идентификатора объекта). указывает наличие или отсутствие идентификатора объекта функции устройства в представлении SNMP.
  - **Selected from List** (Выбранный в списке). с помощью кнопок со стрелками вверх и вниз выберите идентификатор объекта устройства, прокрутив список всех идентификаторов объекта устройства (OID).
  - **Вставить**. укажите идентификатор объекта устройства.
- **View Type** (Тип представления). указывает, будет ли включен идентификатор ветви объекта в выбранное представление SNMP.

Добавление представления

1. Откройте страницу **SNMPv3 View Settings** (Параметры представления SNMP версии 3).
2. Нажмите кнопку **Add** (Добавить).

   Открывается страница**Add A View** (Добавление представления).

   Рис. 6-89. Страница Add A View (Добавление представления)

3. Определите поле.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

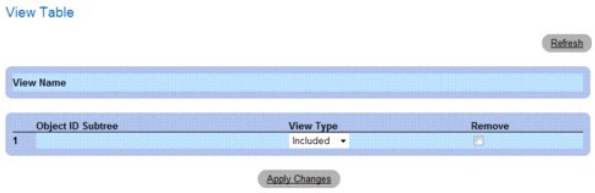
   Будет добавлено представление SNMP, а устройство - обновлено.

Отображение таблицы представлений

1. Откройте страницу **SNMPv3 View Settings** (Параметры представления SNMP версии 3).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **View Table** (Таблица представлений).

Рис. 6-90. Таблица представлений



Определение представлений SNMPv3 с помощью команд консоли

В следующей таблице приведены команды консоли для определения полей, отображаемых на странице **SNMPv3 View Settings** (Параметры представления SNMP версии 3).

Команда консоли	**Описание**
snmp-server view *имя-представления дерево-идентификаторов-объектов* {**included** | **excluded**}	Создает иди обновляет запись представления.
show snmp views [*имя_представления]*	Отображает конфигурацию представлений.

Далее приведен пример команд консоли:

```
Console (config)# snmp-server view user1 1 included

Console (config)# end

Console# show snmp views
```

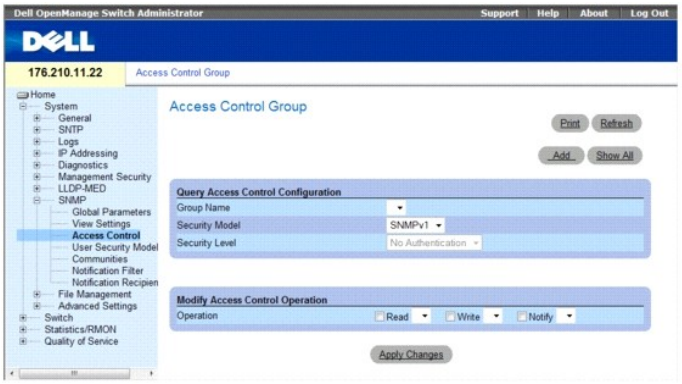
Name	OID Tree	Type
----------	----------	----------
user1	iso	included
Значение по умолчанию	iso	included
Значение по умолчанию	snmpVacmMIB	excluded
Значение по умолчанию	usmUser	excluded
Значение по умолчанию	rndCommunityTable	excluded
DefaultSuper	iso	included

Определение контроля доступа по протоколу SNMP

На странице **Access Control** (Контоль доступа) представлена информация для создания групп SNMP и назначения привилегий доступа к группам SNMP. Выделив группы, администраторы сети могут назначать права доступа к отдельным функциям устройства или аспектам функций.

Чтобы открыть страницу **Access Control Group** (Группа контроля доступа), выберите **System** (Система)→ **SNMP**→ **Access Control** (Контроль доступа) на панели дерева.

Рис. 6-91. Страница Access Control Group (Группа контроля доступа)



Страница **Access Control Group** (Группа контроля доступа) содержит следующие поля:

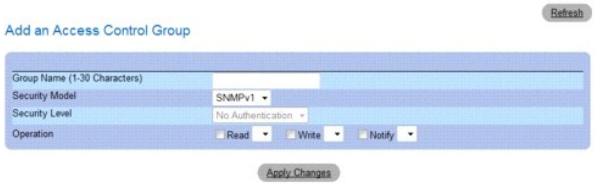
- **Group Name** (Имя группы). группа, определенная пользователем, к которой применяются правила контроля доступа. Диапазон значений поля: до 30 символов.
- **Security Model** (Модель безопасности). определяет версию SNMP, используемую для группы. Возможные значения:
  - **SNMPv1**(SNMP версия 1). для группы определен протокол SNMP версии 1.
  - **SNMPv2** (SNMP версия 2). для группы определен протокол SNMP версии 2.
  - **SNMPv3** (SNMP версия 3). для группы определен протокол SNMP версии 3.
- **Security Level** (Уровень безопасности). уровень безопасности, применяемый к группе. Уровни безопасности применяются только для SNMP версии 3. Возможные значения:
  - **No Authentication** (Нет проверки подлинности). для группы не назначаются ни проверка подлинности, ни уровни безопасности для обеспечения конфиденциальности данных.
  - **Authentication** (Проверка подлинности). выполняет проверку подлинности сообщений SNMP и обеспечивает проверку подлинности источника сообщений SNMP.
  - **Privacy** (Конфиденциальность). выполняет шифрование сообщений SNMP.
- **Operation** (Работа). определяет права доступа группы. Возможные значения:
  - **Read** (Чтение). доступ к управлению ограничивается доступом только для чтения, изменения назначенного представления SNMP невозможны.
  - **Write** (Запись). доступ к управлению характеризуется доступом для чтения и записи, возможны изменения назначенного представления SNMP.
  - **Notify** (Уведомление). отправляет прерывания для назначенного представления SNMP.

Определение групп SNMP

1. Откройте страницу **Access Control Group** (Группа контроля доступа).
2. Нажмите кнопку **Add** (Добавить).

   Откроется страница **Add an Access Control Group** (Добавление группы контроля доступа).

   Рис. 6-92. Страница Add an Access Control Group (Добавление группы контроля доступа)



3. Определите поля на странице **Add an Access Control Group** (Добавление группы контроля доступа).
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Группа будет добавлена, а устройство - обновлено.

Отображение таблицы доступа

1. Откройте страницу **Access Control Group** (Группа контроля доступа).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **Access Table** (Таблица доступа).

Рис. 6-93. Страница Access Table (Таблица доступа)

Удаление групп SNMP

1. Откройте страницу **Access Control Group** (Группа контроля доступа).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **Access Table** (Таблица доступа).
3. Выберите группу SNMP.
4. Установите флажок **Remove** (Удалить).
5. Нажмите кнопку **Apply Changes** (Применить изменения).

   Группа SNMP будет удалена, а устройство - обновлено.

Определение контроля доступа SNMP с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для определения полей, отображаемых на странице **Access Control Group** (Группа контроля доступа).

Команда консоли	**Описание**
snmp-server group *имя группы* {**v1 | v2 | v3** {**noauth** | **auth** | **priv**}} [**read** *чтение*] [**write** *запись*] [**notify** *уведомление*]	Определяет конфигурацию группы SNMP (Simple Network Management Protocol) или таблицы, в которой устанавливается соответствие между пользователями SNMP и представлениями SNMP.
show snmp groups [*имя_группы*]	Отображает конфигурацию групп.

Далее приведен пример команд консоли.

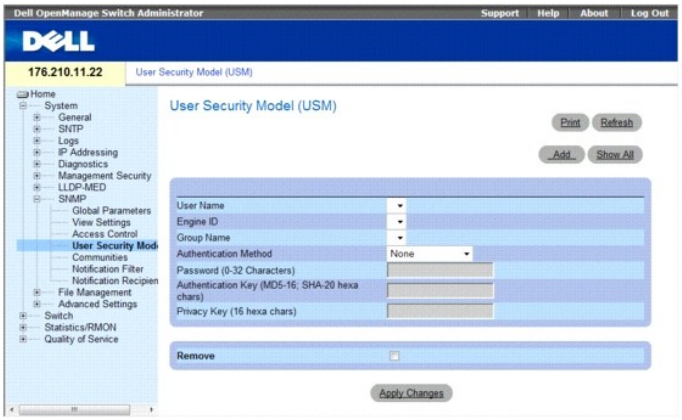
```
console (config)# snmp-server group user-group v3 priv read user-view
```

Назначение уровня безопасности SNMP пользователя

С помощью страницы **SNMPv3 User Security Model (USM)** (Модель USM протокола SNMP версии 3) можно назначить группу SNMP пользователей системы и определить метода проверки подлинности пользователей.

Чтобы открыть страницу **SNMPv3 User Security Model (USM)** (Модель USM протокола SNMP версии 3), нажмите **System** (Система)→ **SNMP** (Система SNMP)→ **User Security Model** (Модель USM) на *панели дерева.*

Рис. 6-94. Страница SNMPv3 User Security Model (USM) (Модель USM протокола SNMP версии 3)



Страница **SNMPv3 User Security Model (USM)** (Модель USM протокола SNMP версии 3) содержит следующие поля.

- **User Name** (Имя пользователя). содержит список имен пользователя, определенных пользователем. Диапазон значений поля: до 30 буквенно-цифровых символов.
- **Engine ID** (Идентификатор механизма). определяет локальный или удаленный объект SNMP, к которому подключен пользователь. При изменении или удалении локального идентификатора механизма SNMP будет удалена база данных пользователей SNMP версии 3.
- **Group Name** (Имя группы). содержит список групп SNMP, определенных пользователем. Группы SNMP определяются на странице **Access Control Group** (Группа контроля доступа).
- **Authentication Method** (Метод проверки подлинности). метод проверки подлинности, используемый для определения подлинности пользователей. Возможные значения:
  - **None** (Нет). проверка подлинности пользователей не используется.
  - **MD5 Password** (Пароль MD5). указывает, что для проверки подлинности используется пароль HMAC-MD5-96. Пользователь должен ввести пароль.
  - **SHA Password** (Пароль SHA). проверка пользователей осуществляется с использованием уровня проверки подлинности HMAC-SHA-96. Пользователь должен ввести пароль.
  - **MD5 Key** (Ключ MD5). проверка подлинности пользователей осуществляется с использованием алгоритма HMAC-MD5-96.
  - **SHA Key** (Ключ SHA). проверка подлинности пользователей осуществляется с использованием уровня HMAC-SHA-96.
- **Password (0-32 Characters)** (Пароль (0-32 символа)). изменяет определенный пользователем пароль для группы. Пароли могут содержать не более 32 буквенно-цифровых символов.
- **Authentication Key (MD5-16; SHA-20 hexa chars)** (Ключ проверки подлинности (MD5-16; SHA-20 шестнадцатеричных символов)). определяет уровень проверки подлинности HMAC-MD5 -96 or HMAC-SHA-96. Ключи проверки подлинности и конфиденциальности вводятся для определения ключа проверки подлинности. Если требуется только проверка подлинности, для MD5 определяются только 16 байт. Если требуется проверки и конфиденциальности, и подлинности, для MD5 определяются 32 байта. Каждый байт в строке шестнадцатеричного символа - это две шестнадцатеричных цифры. Каждый байт должен быть разделен точкой или двоеточием.
- **Privacy Key (16 hexa characters)** (Ключ конфиденциальности (16 шестнадцатеричных символов)). если требуется только проверка подлинности, определяются только 20 байт. Если требуется проверка и конфиденциальности, и подлинности, определяются 16 байт. Каждый байт в строке шестнадцатеричного символа - это две шестнадцатеричных цифры. Каждый байт должен быть разделен точкой или двоеточием.
- **Remove** (Удалить). когда установлен этот флажок, удаляются пользователи из указанной группы.
  - **Флажок установлен**. удаляет пользователя из указанной группы.
  - **Флажок снят**. оставляет пользователя в указанной группе.

Добавление пользователей в группу

1. Откройте страницу **SNMPv3 User Security Model (USM)** (Модель USM протокола SNMP версии 3).
2. Нажмите кнопку **Add** (Добавить).

   Откроется страница**Add SNMPv3 User Name** (Добавление имени пользователя SNMP версии 3).

   Рис. 6-95. Страница Add SNMPv3 User Name (Добавление имени пользователя SNMP версии 3)

3. Определите соответствующие поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Пользователь будет добавлен к группе, а устройство - обновлено.

Отображение таблицы USM (User Security Model)

1. Откройте страницу **SNMPv3 User Security Model (USM)** (Модель USM протокола SNMP версии 3).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **User Security Model Table** (Таблица USM (User Security Model)).

   Рис. 6-96. Таблица USM (User Security Model)

Удаление записи в таблице USM (User Security Model)

1. Откройте страницу **SNMPv3 User Security Model (USM)** (Модель USM протокола SNMP версии 3).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **User Security Model Table** (Таблица USM (User Security Model)).
3. Выберите запись **User Security Model Table** (Таблица USM (User Security Model)).
4. Установите флажок **Remove** (Удалить).
5. Нажмите кнопку **Apply Changes** (Применить изменения).

   Запись **User Security Model Table** (Таблица USM (User Security Model)) будет удалена, а устройство - обновлено.

Определение пользователей SNMP версии 3 с помощью команд консоли

В следующей таблице приведены команды консоли для определения полей, отображаемых на странице **SNMPv3 User Security Model (USM)** (Модель USM протокола SNMP версии 3).

Команда консоли	**Описание**
snmp-server user *имя_пользователя имя_группы* [**remote** *строка-идентификатора-механизма*][**auth-md5** *пароль* | **auth-sha** ***пароль*** | **auth-md5-key** *md5-des-ключ* | **auth-sha-key** *sha-des-ключ*]	Определяет конфигурацию нового пользователя SNMP версии 3.
show snmp users [*имя_пользователя*]	Отображает конфигурацию пользователей.

Далее приведен пример команд консоли.

```
console (config)# snmp-server user John user-group auth-md5 1234

console(config)# end

console# show snmp users
```

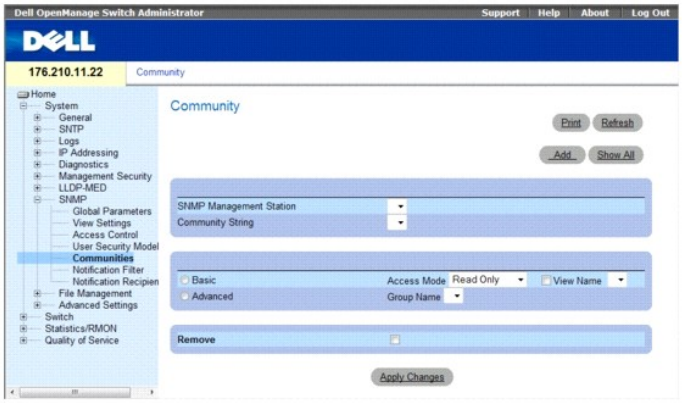
Name	Group Name	Auth Method	Remote
-------	----------	----------	------
John	user-group	md5	

Определение сообществ SNMP

Управление правами доступа осуществляется путем определения сообществ на странице **SNMP Community** (Сообщество SNMP). При изменении имен сообществ изменяются также и права доступа. Сообщества SNMP определяются только для протоколов SNMP версии 1 и SNMP версии 2.

Чтобы открыть страницу **SNMP Community** (Сообщество SNMP), выберите **System** (Система)→ **SNMP**→ **Communities** (Сообщества) на панели дерева.

Рис. 6-97. Страница SNMP Community (Сообщество SNMP)



Страница **SNMP Community** (Сообщество SNMP) содержит следующие поля:

- **SNMP Management Station** (Станция управления SNMP). станция управления, IP-адрес для которой определен в сообществе SNMP.
- **Community String** (Строка сообщества). работает в качестве пароля и используется для идентификации станции управления для устройства.
- **Basic** (Базовый). включает режим SNMP Basic для выбранного сообщества. Возможные значения:
  - **Access Mode** (Режим доступа). определяет права доступа для сообщества. Возможные значения:

    Read-Only (Только чтение). доступ к управлению ограничивается доступом только для чтения, изменения сообщества невозможны.

    Read-Write (Чтение и запись). при доступе к управлению можно выполнять чтение и запись и вносить изменения в конфигурацию устройства, но не сообщества.

    SNMP-Admin (Администратор SNMP). пользователь имеет доступ ко всем параметрам конфигурации устройства, а также имеет право изменять сообщество.
  - **View Name** (Имя представления). содержит список представлений SNMP, определенных пользователем.
- **Advanced** (Расширенный). содержит список групп, определенных пользователем. При выборе режима SNMP Advanced (Расширенный SNMP) правила контроля доступа SNMP, определенные для группы, будут включены для выбранного сообщества. В режиме Advanced (Расширенный) группы SNMP включаются для определенных сообществ SNMP. Режим SNMP Advanced определяется только с SNMP версия 3. Возможное значение поля:
  - **Group Name** (Имя группы). указывает имя группы при работе в режиме SNMP Advanced.

Remove (Удалить). удаляет сообщество из указанного устройства.

  - **Флажок установлен** . удаляет сообщество.
  - **Флажок снят**. оставляет сообщество в указанном устройстве.

При определении нового сервера SNMP, будет доступен следующий дополнительный параметр:

- **Supported IP Format** (Поддерживаемый формат IP-адресов). Отображает формат IP-адресов, поддерживаемый сообществом. Возможные значения:
  - **IPv6**. поддержка IP версии 6.

- **IPv4**. поддержка IP версии 4.

- **IPv6 Address Type** (Тип адреса IPv6). В случае, если сообщество поддерживает систему IPv6 (см. предыдущий параметр), здесь указывается поддерживаемый тип статических адресов. Возможные значения:
  - **Link Local** (Локальная связь). Адрес локальной связи, который не маршрутизируется, а используется только для связи в пределах той же сети.
  - **Global** (Глобальный). Глобальный уникальный адрес IPv6 address; он является видимым и доступным для различных подсетей.
- **Link Local Interface** (Интерфейс локальной связи). Если сервер поддерживает систему адресов локальной связи IPv6 (см. предыдущий параметр), здесь указывается интерфейс локальной связи. Возможные значения:
  - **VLAN1**. Интерфейс IPv6 конфигурируется по сети VLAN1.
  - **ISATAP**. Интерфейс IPv6 конфигурируется по туннелю ISATAP.

Определение нового сообщества

1. Откройте страницу **SNMP Community** (Сообщество SNMP).
2. Нажмите кнопку **Add** (Добавить).

   Откроется страница **Add SNMP Community** (Добавление сообщества SNMP):

   Рис. 6-98. Страница Add SNMP Community (Добавление сообщества SNMP)

3. Заполните соответствующие поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

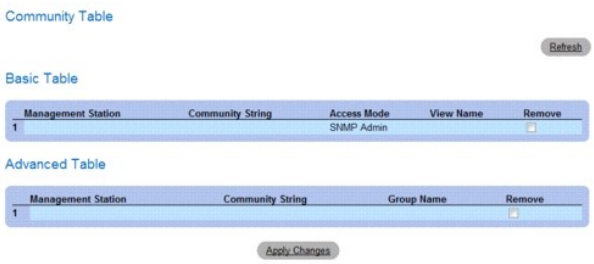
   Новое сообщество будет сохранено, а устройство - обновлено.

Удаление сообществ

1. Откройте страницу **SNMP Community** (Сообщество SNMP).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **Community Table** (Таблица сообществ).

   Рис. 6-99. Страница Community Table (Таблица сообществ)



3. Выберите сообщество и установите флажок **Remove** (Удалить).
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Запись сообщества будет удалена, а устройство - обновлено.

Настройка сообществ с помощью команд консоли

В следующей таблице приведены команды консоли, соответствующие полям на странице **SNMP Community** (Сообщество SNMP).

Команда консоли	Описание
snmp-server community *community* [**ro** | **rw** | **su**] [ipv4-address | ipv6-address][**view** *view-name*]	Задает строку доступа сообщества для разрешения доступа по протоколу SNMP.
snmp-server community-group *community group-name* [ipv4-address | ipv6-address]	Задает строку доступа сообщества для разрешения ограниченного доступа по протоколу SNMP на основе прав доступа группы.
show snmp	Отображает текущую конфигурацию устройства SNMP.

Далее приведен пример команд консоли.

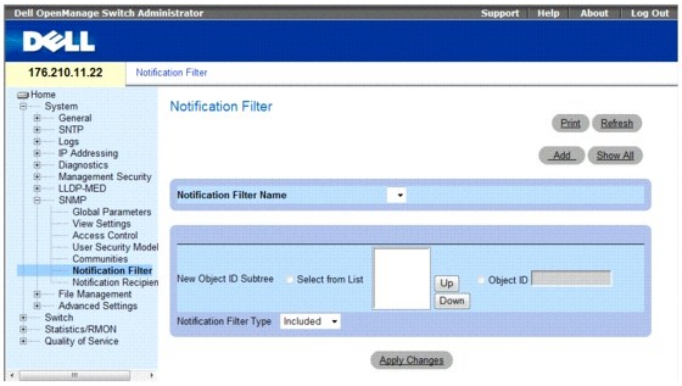
```
Console (config)# snmp-server community dell ro 10.1.1.1
```

Определение фильтров уведомлений SNMP

Страница **Notification Filter** (Фильтр уведомлений) разрешает фильтрацию системных прерываний на основе идентификаторов объекта (OID). Каждый идентификатор объекта (OID) связан с функцией или подфункцией устройства. С помощью страницы **Notification Filter** (Фильтр уведомлений) администраторы сети также могут осуществлять фильтрацию уведомлений.

Чтобы открыть страницу **Notification Filter** (Фильтр уведомлений)**,** выберите **System** (Система)→ **SNMP**→ **Notification Filters** (Фильтры уведомлений) на *панели дерева*.

Рис. 6-100. Страница Notification Filter (Фильтр уведомлений)



Страница **Notification Filter** (Фильтр уведомлений) содержит следующие поля.

- **Notification Filter Name** (Имя фильтра уведомлений). фильтры уведомлений, определенных пользователем.
- **New Object ID Tree** (Новая ветвь идентификатора объекта). Идентификатор объекта, указывающий, какие из уведомлений отправлены или заблокированы. Если к идентификатору объекта (OID) применяется фильтр, системные прерывания или сообщения генерируются и отправляются получателям системных прерываний. Идентификаторы объектов либо выбираются в окне Select from List (Выбор из списка), либо в списке Object ID (Идентификатор объекта).
- **Notification Filter Typ**e (Тип фильтра уведомлений). указывает, какой вид уведомлений - сообщения или системные прерывания с учетом идентификатора объекта (OID) - отправляется получателю системных прерываний.
  - **Excluded** (Отправка исключена). запрещает отправку системных прерываний или сообщений OID.
  - **Included** (Отправка включена). отправляет системные прерывания или сообщения OID.

Добавление фильтров SNMP

1. Откройте страницу **Notification Filter** (Фильтр уведомлений).
2. Нажмите кнопку **Add** (Добавить).

   Откроется страница **Add Filter** (Добавление фильтра).

   Рис. 6-101. Страница Add Filter (Добавление фильтра)

3. Определите соответствующие поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Новый фильтр будет добавлен, а устройство - обновлено.

Отображение таблицы фильтров

1. Откройте страницу **Notification Filter** (Фильтр уведомлений).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **Filter Table** (Таблица фильтров).

   Рис. 6-102. Страница Filter Table (Таблица фильтров)

Удаление фильтра

1. Откройте страницу **Notification Filter** (Фильтр уведомлений).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **Filter Table** (Таблица фильтров).

3. Выберите запись в таблице **Filter Table** (Таблица фильтров).
4. Установите флажок **Remove** (Удалить).

   Запись фильтра будет удалена, а устройство - обновлено.

Настройка фильтров уведомлений с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для определения полей, отображенных на странице **Notification Filter** (Фильтр уведомлений).

Команда консоли	Описание
snmp-server filter *имя_фильтра oid-tree* {**included** | **excluded**}	Создает или обновляет фильтр уведомлений SNMP.
show snmp filters [filtername]	Отображает конфигурацию фильтров уведомлений SNMP.

Далее приведен пример команд консоли:

```
Console (config)# snmp-server filter user1 iso included
Console (config)# end
Console # show snmp filters

Name        OID Tree      Type
----------  ------------  --------
user1       iso           Included
```

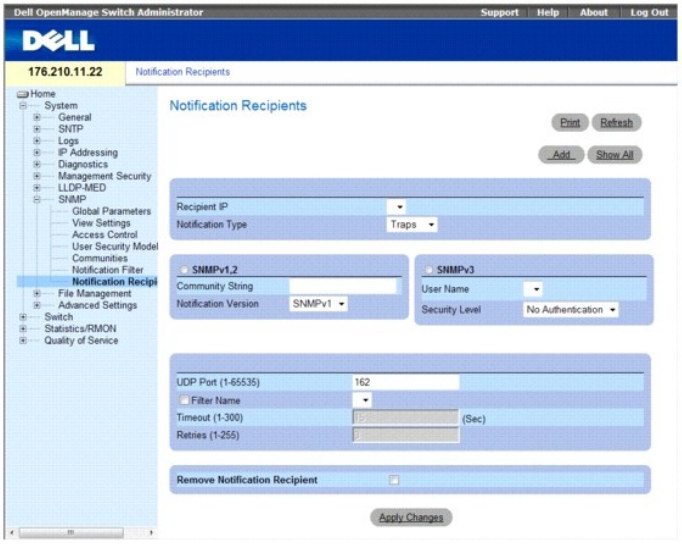
Определение получателей уведомлений SNMP

На странице **Notification Recipients** (Получатели уведомлений) представлена информация по настройке фильтров, которые указывают, отправляются ли системные прерывания определенным пользователям, а также тип системных прерываний. Фильтры уведомлений SNMP выполняют следующие функции.

- Определение объектов системных прерываний управления
- Фильтрация системных прерываний
- Выбор параметров генерации системных прерываний
- Обеспечение проверок контроля доступа

Чтобы открыть страницу **Notification Recipients** (Получатели уведомлений), выберите **System** (Система)→ **SNMP**→ **Notification Recipient** (Получатель уведомлений) на панели дерева.

Рис. 6-103. Страница Notification Recipients (Получатели уведомлений)



Страница **Notification Recipients** (Получатели уведомлений) содержит следующие поля.

- **Recipient IP** (IP-адрес получателя). IP-адрес, по которому отправляются системные прерывания.
- **Notification Type** (Тип уведомлений). отправленное уведомление. Возможные значения:
  - ***Trap*** (Системное прерывание). отправляются системные прерывания.
  - **Inform** (сообщение). отправляются сообщения.

SNMPv1,2 (версия 1,2)

Для выбранного получателя включен протокол SNMP версий 1 и 2. Заполните следующие поля для SNMPv1 и SNMPv2:

- **Community String (1-20 Characters)** (Строка сообщества (1-20 символов)). строка сообщества менеджера системных прерываний.
- **Notification Version** (Версия уведомления). определяет версию уведомления. Возможные значения:
  - **SNMP V1**. отправляются системные прерывания SNMP версии 1.
  - **SNMP V2**. отправляются системные прерывания SNMP версии 2.

SNMPv3 (версия 3)

SNMPv3 используется для отправки и получения прерываний. Заполните следующие поля для SNMPv3:

- **User Name** (Имя пользователя). пользователь, которому отправляются уведомления SNMP.
- **Security Level** (Уровень безопасности). определяет средства, с помощью которых проверяется подлинность пакета. Возможные значения:
  - **No Authentication** (Нет проверки подлинности). не производится ни проверка подлинности, ни шифрование пакета.
  - **Authentication** (Проверка подлинности). производится проверка подлинности пакета.
  - **Privacy** (Конфиденциальность). производится и проверка подлинности, и шифрование пакета.
- **UDP Port (1-65535)** (Порт UDP). порт UDP, используемый для отправки уведомлений. Значение по умолчанию: 162.
- **Filter Name** (Имя фильтра). включает или исключает фильтры SNMP.
  - **Флажок установлен**. включает фильтры SNMP.
  - **Флажок снят**. отключает фильтры SNMP.
- **Timeout (1-300)** (Тайм-аут). время ожидания устройства (в секундах) перед повторной отправкой сообщений. Значение по умолчанию: 15 секунд.
- **Retries (1-255)** (Повторные попытки). число повторных попыток отправки устройством запросов.
  Значение по умолчанию: 3.
- **Remove Notification Recipient** (Удаление получателя уведомлений). удаляет выбранных получателей уведомлений.
  - **Флажок установлен**. удаляет выбранных получателей уведомлений.
  - **Флажок снят**. оставляет получателя уведомлений.

При добавлении получателя уведомления, будут доступны следующие дополнительные параметры:

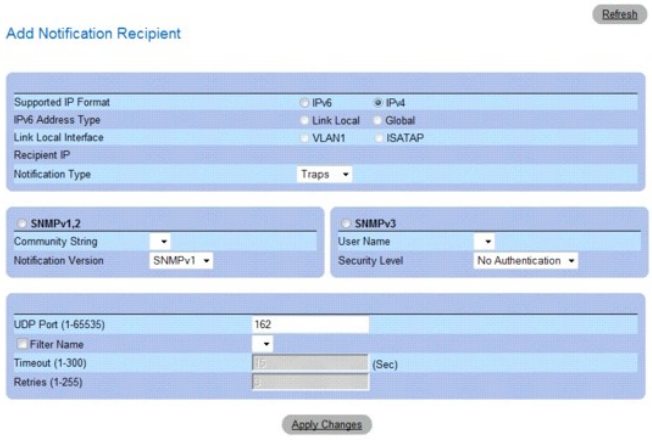
- **Supported IP Format** (Поддерживаемый формат IP-адресов). Отображает формат IP-адресов, поддерживаемый получателем. Возможные значения:
  - **IPv6**. поддержка IP версии 6.
  - **IPv4**. поддержка IP версии 4.
- **IPv6 Address Type** (Тип адреса IPv6). Если получатель поддерживает систему IPv6 (см. предыдущий параметр), здесь указывается поддерживаемый тип статических адресов. Возможные значения:
  - **Link Local** (Локальная связь). Адрес локальной связи, который не маршрутизируется, а используется только для связи в пределах той же сети.
  - **Global** (Глобальный). Глобальный уникальный адрес IPv6 address; он является видимым и доступным для различных подсетей.
- **Link Local Interface** (Интерфейс локальной связи). Если сервер поддерживает систему адресов локальной связи IPv6 (см. предыдущий параметр), здесь указывается интерфейс локальной связи. Возможные значения:
  - **VLAN1**. Интерфейс IPv6 конфигурируется по сети VLAN1.
  - **ISATAP**. Интерфейс IPv6 конфигурируется по туннелю ISATAP.

Добавление новых получателей системных прерываний

1. Откройте страницу **Notification Recipients** (Получатели уведомлений).
2. Нажмите кнопку **Add** (Добавить).

   Откроется страница **Add Notification Recipients** (Добавление получателей уведомлений)**.**

   Рис. 6-104. Добавление получателей уведомлений



3. Определите соответствующие поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

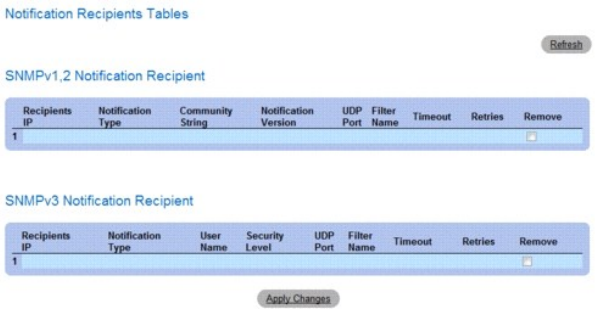
   Получатель уведомлений будет добавлен, а устройство - обновлено.

Отображение таблиц получателей уведомлений

1. Откройте страницу **Notification Recipients** (Получатели уведомлений).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **Notification Recipients Tables** (Таблицы получателей уведомлений).

   Рис. 6-105. Таблицы получателей уведомлений



Удаление получателей уведомлений

1. Откройте страницу **Notification Recipients** (Получатели уведомлений).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **Notification Recipients Tables** (Таблицы получателей уведомлений).

3. Выберите получателя уведомлений в таблице **SNMPV1,2 Notification Recipient** (Получатель уведомлений SNMP версии 1, 2) или **SNMPv3 Notification Recipient Tables** (Получатель уведомлений SNMP версии 3).
4. Установите флажок **Remove** (Удалить).
5. Нажмите кнопку **Apply Changes** (Применить изменения).

   Получатель будет удален, а устройство - обновлено.

Настройка получателей уведомлений SNMP с помощью команд консоли

В следующих таблицах приведены команды консоли для определения полей, отображаемых на странице **Notification Recipients** (Получатели уведомлений).

Команда консоли	Описание
snmp-server host {*ip-адрес* | *имя_хоста*} *community-string* [**traps** | **informs**] [**1** | **2**] [**udp-port** *номер_порта*] [**filter** *имя_фильтра*] [**timeout** *секунды*] [**retries** *число_попыток*]	Создает или обновляет получателя уведомлений SNMP версий 1 или 2.
snmp-server v3-host {ip-*адрес* | *имя_хоста*} *имя_пользователя* [**traps** | **informs**] {**noauth** | **auth** | **priv**} [**udp-port** *номер_порта*] [**filter** *имя_фильтра*] [**timeout** *секунды*] [**retries** *число_попыток*]	Создает или обновляет получателя уведомлений SNMP версии 3.
show snmp	Показывает текущую конфигурацию SNMP.

Далее приведен пример команд консоли.

```
console (config)# snmp-server host 172.16.1.1 private

console(config)# end

console# show snmp
```

Community-String	Community-Access	View name	IP address
---	---	---	---
public	read only	просмотр пользователя	All
private	read write	по умолчанию	172.16.1.1
private	su	DefaultSuper	172.17.1.1

Управление файлами

Для управления программным обеспечением устройства, файлами образов и файлами настройки используйте страницу **File Management** (Управление файлами). Файлы можно передавать или загружать через сервер TFTP. Управление файловой структурой состоит из следующих элементов:

- **Startup Configuration File** (Файл конфигурации для запуска). содержит команды, необходимые для конфигурации устройства при запуске или перезагрузке. Файл конфигурации для запуска создается путем копирования команд настройки из файла рабочей настройки или файла образа.
- **Running Configuration File** (Файл рабочей настройки). содержит все команды файла настройки для запуска, а также все команды, введенные во время последнего сеанса. После отключения или перезагрузки устройства все команды, сохраненные в файле рабочей настройки, теряются. В ходе запуска все команды файла для запуска копируются в файл конфигурации для запуска и применяются для устройства. Во время сеанса все новые команды добавляются к существующим командам файла рабочей настройки. Чтобы изменить файл конфигурации для запуска, нужно перед отключением устройства скопировать файл рабочей настройки в файл настройки для запуска.
- **Image Files** (Файлы образа). системные образы файлов сохраняются в двух файлах Flash, называемых Image 1 (Образ 1) и Image 2 (Образ 2). Активный образ хранит активную копию, а другой - вторую копию. Устройство загружается и запускается из активного образа. Если активный образ поврежден, система автоматически загружается из неактивного образа. Эта функция защиты от сбоев, возникающих в процессе обновления программного обеспечения.

Чтобы открыть страницу **File Management** (Управление файлами), выберите **System** (Система)→ **File Management** (Управление файлами) на панели дерева.

В этом разделе имеются следующие тематические подразделы:

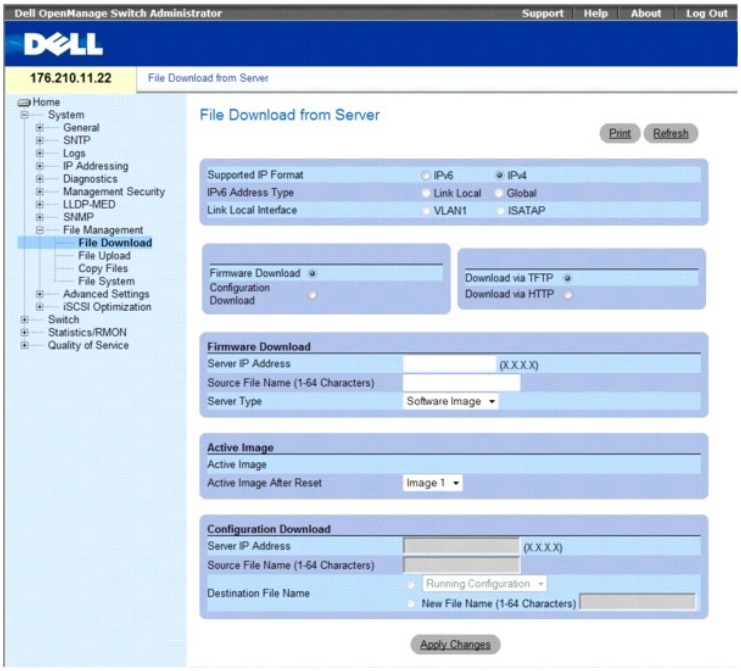
- Загрузка файлов
- Передача файлов на сервер
- Активизация файла образа
- Копирование файлов
- Управление файлами устройства

Загрузка файлов

Страница **File Download from Server** (Загрузка файлов с сервера) содержит поля для загрузки системного образа и файлов настройки с сервера TFTP или HTTP-клиента на устройство.

Чтобы открыть страницу **File Download from Server** (Загрузка файлов с сервера), выберите **System** (Система)→ **File Management** (Управление файлами)→ **File Download** (Загрузка файла) на панели дерева.

Рис. 6-106. File Страница Download from Server (Загрузка файлов с сервера)



Страница **File Download From Server** (Загрузка файлов с сервера) содержит следующие поля.

- **Supported IP Format** (Поддерживаемый формат IP-адресов). Отображает формат IP-адресов, поддерживаемый сервером SNTP. Возможные значения:
  - **IPv6**. поддержка IP версии 6.
  - **IPv4**. поддержка IP версии 4.
- **IPv6 Address Type**. В случае, если сервер поддерживает систему IPv6 (см. предыдущий параметр), здесь указывается поддерживаемый тип статических адресов. Возможные значения:
  - **Link Local** (Локальная связь). Адрес локальной связи, который не маршрутизируется, а используется только для связи в пределах той же сети.
  - **Global** (Глобальный). Глобальный уникальный адрес IPv6 address; он является видимым и доступным для различных подсетей.
- **Link Local Interface** (Интерфейс локальной связи). Если сервер поддерживает систему адресов локальной связи IPv6 (см. предыдущий параметр), здесь указывается интерфейс локальной связи. Возможные значения:
  - **VLAN1**. Интерфейс IPv6 конфигурируется по сети VLAN1.
  - **ISATAP**. Интерфейс IPv6 конфигурируется по туннелю ISATAP.
- **Firmware Download** (Загрузка микропрограммы). загружается файл микропрограммы. Если поле **Firmware Download** (Загрузка микропрограммы) выделено, то поля **Configuration Download** (Загрузка конфигурации) недоступны.
- **Configuration Download** (Загрузка настройки). загружается файл настройки. Если выбран параметр **Configuration Download** (Загрузка настройки), поля **Firmware Download** (Загрузка микропрограммы) недоступны.
- **Download via TFTP** (Загрузить через TFTP). загружает образ через сервер TFTP.
- **Download via HTTP** (Загрузить через HTTP). загружает образ через сервер HTTP.

Firmware Download (Загрузка микропрограммы)

- **Server IP Address** (IP-адрес сервера). IP-адрес сервера, с которого загружаются файлы микропрограммы.
- **Source File Name (1-64 characters)** (Имя исходного файла (1-64 символа)). обозначает файл для загрузки.
- **Destination File Name** (Имя файла для загрузки). тип файла, в который будет загружен файл. Возможные значения:
  - **Software Image** (Образ программы). загружает файл образа. Образ из файла заменяет неактивный образ. Рекомендуется определить неактивный образ, который станет активным после сброса, а затем выполнить сброс устройства после загрузки. Во время загрузки файла образа откроется диалоговое окно, в котором отобразится состояние процесса выполнения. Окно закроется автоматически по завершении загрузки.
  - **Boot Code** (Код загрузки). загружает загрузочный файл.

Configuration Download (Загрузка конфигурации)

- **Server IP Address** (IP-адрес сервера). IP-адрес сервера TFTP, с которого загружаются файлы конфигурации.
- **Source File Name (1-64 Characters)** (Имя исходного файла (1-64 символа)). обозначает файлы конфигурации для загрузки.
- **Destination** (Файл назначения). файл, в который будет загружен файл конфигурации. Возможные значения:
  - **Running Configuration** (Рабочая настройка). команды загружаются в файл рабочей настройки.
  - **Startup Configuration** (Конфигурация для запуска). загружается и переписывается файл настройки для запуска.
  - **<filename>**. Загружает команды в резервный конфигурационный файл. Имя файла определяется пользователем при загрузке.

Загрузка файлов

1. Откройте страницу **File Download from Server** (Загрузка файлов с сервера).
2. Определите тип файла для загрузки.
3. Определите поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Программное обеспечение будет загружено на устройство. Для активизации выбранного файла образа перезагрузите устройство. Более подробную информацию о перезагрузке устройства см. в разделе **Switching Between Stack Masters** (Переключение главных устройств).

Загрузка файлов с сервера с помощью команд консоли

В следующей таблице приведены команды консоли для настройки полей, отображаемых на странице **File Download From Server** (Загрузка файлов с сервера).

Команда консоли	**Описание**
source-url destination-url	Копирует файл из исходного местоположения в место назначения.

Далее приведен пример команд консоли.

```
console# copy tftp://10.6.6.64/pp.txt startup-config

....!

Copy: 575 bytes copied in 00:00:06 [hh:mm:ss]

01-Jan-2000 06:41:55 %COPY-W-TRAP: The copy operation was completed successfully
```

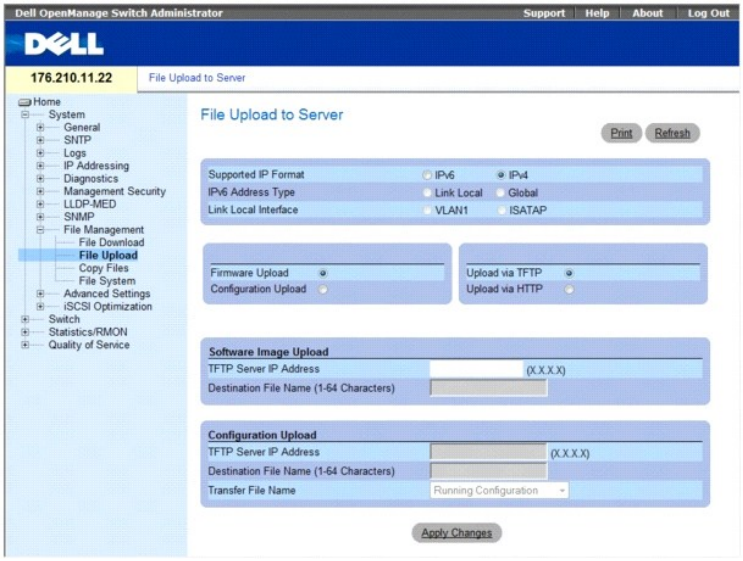
ПРИМЕЧАНИЕ. Каждый восклицательный знак (!) означает успешную передачу десяти пакетов.

Передача файлов на сервер

На странице **File Upload to Server** (Загрузка файла на сервер) содержатся поля для загрузки программного обеспечения устройства на сервер TFTP. Файл образа также можно загрузить со страницы **File Upload to Server** (Передача файлов на сервер).

Чтобы открыть страницу **File Upload to Server** (Передача файлов на сервер), выберите **System** (Система)→ **File Management** (Управление файлами)→ **File Upload** (Передача файла) на панели дерева.

Рис. 6-107. Страница File Upload to Server (Передача файлов на сервер)



Страница **File Upload to Server** (Загрузка файлов на сервер) содержит следующие поля.

- **Supported IP Format** (Поддерживаемый формат IP-адресов). Отображает формат IP-адресов, поддерживаемый сервером SNTP. Возможные значения:
  - **IPv6**. поддержка IP версии 6.
  - **IPv4**. поддержка IP версии 4.
- **IPv6 Address Type** (Тип адреса IPv6). В случае, если сервер поддерживает систему IPv6 (см. предыдущий параметр), здесь указывается поддерживаемый тип статических адресов. Возможные значения:
  - **Link Local** (Локальная связь). Адрес локальной связи, который не маршрутизируется, а используется только для связи в пределах той же сети.
  - **Global** (Глобальный). Глобальный уникальный адрес IPv6 address; он является видимым и доступным для различных подсетей.
- **Link Local Interface** (Интерфейс локальной связи). Если сервер поддерживает систему адресов локальной связи IPv6 (см. предыдущий параметр), здесь указывается интерфейс локальной связи. Возможные значения:
  - **VLAN1**. Интерфейс IPv6 конфигурируется по сети VLAN1.
  - **ISATAP**. Интерфейс IPv6 конфигурируется по туннелю ISATAP.
- **Firmware Upload** (Передача микропрограммы). передается файл микропрограммы. Если выбран параметр **Firmware Upload** (Передача микропрограммы), поля **Configuration Upload** (Передача настройки) недоступны.
- **Configuration Upload** (Передача настройки). передается файл настройки. Если выбран параметр **Firmware Upload** (Передача настройки), поля **Configuration Upload** (Передача микропрограммы) недоступны.
- **Upload via TFTP** (Передача через TFTP). передает образ через сервер TFTP.
- **Upload via HTTP** (Передача через HTTP). передает образ через сервер FTP.

Software Image Upload (Передача образа программы)

- **TFTP Server IP Address** (IP-адрес сервера TFTP). IP-адрес сервера TFTP, на который передается файл образа программы.
- **Destination File Name (1-64 Characters)** (Имя файла назначения (1-64 символа)). путь к файлу образа программы, куда передается файл.

Configuration Upload (Передача файла настройки)

- **TFTP Server IP Address** (IP-адрес сервера TFTP). IP-адрес сервера TFTP, на который передается файл настройки.
- **Destination File Name (1-64 Characters)** (Имя файла назначения (1-64 символа)). путь к файлу настройки, куда передается файл.
- **Transfer File Name** (Имя передаваемого файла). программный файл, в который выполняется передача файла настройки. Возможные значения:
  - **Running Configuration** (Рабочая настройка). передает текущий файл настройки.
  - **Startup Configuration** (Настройка для запуска). передает файл настройки для запуска.
  - **My Backup Configuration** (Резервная настройка). передает файл резервной настройки. Этот определенный пользователем список файлов настройки отображается, если пользователь создал резервные файлы настройки. Например, если пользователь скопировал файлы рабочей настройки в определенный пользователем файл настройки BACKUP-SITE-1, этот список отобразится на странице File Upload to Server (Передача файла на сервер) и файл настройки BACKUP-SITE-1 отобразится в списке.

Передача файлов на сервер

1. Откройте страницу **File Upload to Server** (Передача файлов на сервер).
2. Определите тип файла для загрузки.
3. Определите поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Программное обеспечение будет загружено на сервер TFTP.

Передача файлов на сервер с помощью команд консоли

В следующей таблице приведены команды консоли для настройки полей, отображаемых на странице **File Upload to Server** (Загрузка файлов на сервер).

Команда консоли	Описание
copy source-url destination-url	Копирует файл из исходного местоположения в место назначения.

Далее приведен пример команд консоли.

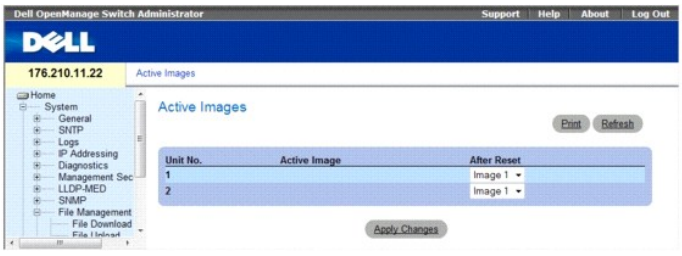
```
console# copy image tftp://10.6.6.64/uploaded.ros

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Copy (Копировать): 4234656 bytes copied in 00:00:33 [hh:mm:ss]

01-Jan-2000 07:30:42 %COPY-W-TRAP: The copy operation was completed successfully
```

Активизация файла образа

Страница **Active Images** (Активные образы) позволяет системные администраторам выбирать и очищать файлы образа. Для каждого устройства в стеке можно выбрать отдельный файл активного образа.

Чтобы открыть страницу **Active Images** (Активные образы), выберите **System** (Система)→ **File Management** (Управление файлами)→ **Active Images** (Активные образы) на панели дерева.

Рис. 6-108. Страница Active Images (Активные образы)



Страница **Active Images** (Активные образы) содержит следующие поля:

- **Unit No.** (Номер устройства). указывает номер устройства, для которого выбран файл образа.
- **Active Image** (Активный образ). файл образа, который в данный момент является активным для данного устройства.
- **After Reset** (После перезагрузки). файл образа, который станет активным после перезагрузки устройства. Возможные значения:

- **Image 1** (Образ 1). активирует файл образа 1 после перезагрузки устройства.
- **Image 2** (Образ 2). активирует файл образа 2 после перезагрузки устройства.

Выбор файла образа

1. Откройте страницу **Active Images** (Активные образы).
2. Выберите файл образа для определенного устройства в поле **After Reset** (После перезагрузки).
3. Нажмите кнопку **Apply Changes** (Применить изменения).

   Файл образа будет выбран. Файл образа будет загружен только после следующей перезагрузки устройства. Выбранный файл образа будет продолжать работать до следующей перезагрузки устройства.

Работа с файлом активного образа с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для просмотра полей, отображенных на странице **Active Images** (Активные образы).

Команда консоли	**Описание**
boot system [**unit** | *unit*] {**image-1** | **image-2**}	Указывает системные образ, который загружается устройством при запуске.
show version [**unit** *устройство*]	Отображает сведения о версии системы.

Далее приведен пример команд консоли.

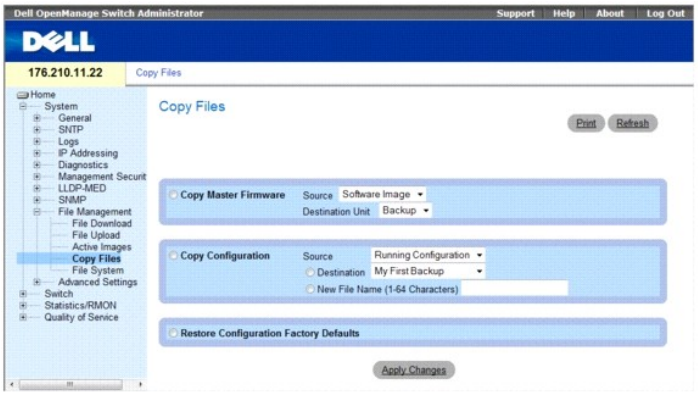
```
Console# boot system image-1
```

Копирование файлов

Файлы можно копировать и удалять со страницы **Copy Files** (Копирование файлов).

Чтобы открыть страницу **Copy Files** (Копирование файлов), выберите **System** (Система)→ **File Management** (Управление файлами)→ **Copy Files** (Копирование файлов) на панели дерева.

Рис. 6-109. Copy Files (Копирование файлов)



Страница **Copy Files** (Копирование файлов) содержит следующие поля.

- **Copy Master Firmware** (Скопировать встроенные программы главного устройства). указывает, какие файлы встроенных программ следует скопировать. Возможные значения:
  - **Source** (Источник). копирует файл образа программного обеспечения или файл Boot главного устройства стека.
  - **Destination Unit** (Устройство назначения). указывает компонент стека для загрузки файла.
- **Copy Configuration** (Копировать конфигурацию). Копирует файл рабочей конфигурации, конфигурации для запуска или резервной конфигурации, который находится в файле главного устройства, в файл назначения.

- **Source** (Источник). указывает тип файла, который необходимо скопировать в файл назначения. Выберите файл рабочей конфигурации или файл конфигурации для запуска.
- **Destination** (Назначение). указывает файл конфигурации, в который копируется исходный файл. Выберите файл рабочей конфигурации, резервной конфигурации или файл конфигурации для запуска.
- **New File Name (1-64 characters)** (Имя нового файла, 1-64 символов). указывает имя вновь созданного резервного файла конфигурации.

- **Restore Configuration Factory Defaults** (Восстановить заводские параметры конфигурации). указывает, что текущие параметры конфигурации необходимо заменить на заводские параметры конфигурации по умолчанию. Если поле не отмечено, это значит, что можно продолжать применять текущие параметры конфигурации. Если это поле пустое, указывает, что текущие параметры конфигурации заменять не следует.

Копирование файлов

1. Откройте страницу **Copy Files** (Копирование файлов).
2. Определите поля **Source** (Источник) и **Destination** (Назначение).
3. Нажмите кнопку **Apply Changes** (Применить изменения).

   Файл будет скопирован, а устройство - обновлено.

Восстановление заводских настроек по умолчанию

1. Откройте страницу **Copy Files** (Копирование файлов).
2. Выберите **Restore Company Factory Defaults** (Восстановить заводские файлы настройки).
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Заводские настройки по умолчанию будут восстановлены, а устройство - обновлено.

Копирование и удаление файлов с помощью команд консоли

В следующей таблице приведены команды консоли для настройки полей, отображаемых на странице **Copy Files** (Копирование файлов).

Команда консоли	**Описание**
copy *url_источника url_приемника*	Копирует файл из исходного местоположения в место назначения.
delete startup-config	Удаляет файл конфигурации для запуска.
delete *url*	Удаляет файл из устройства ФЛЭШ-памяти.

Далее приведен пример команд консоли.

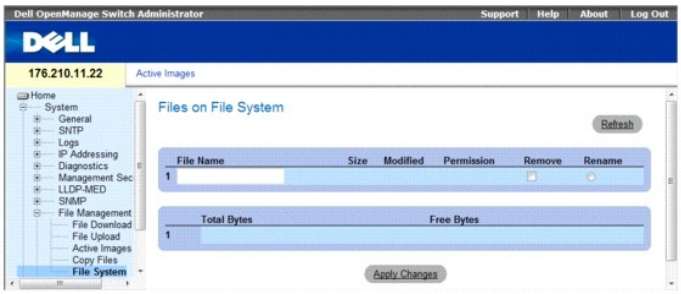
```
console# delete startup-config

Startup file was deleted

console#

console# copy running-config startup-config

01-Jan-2000 06:55:32 %COPY-W-TRAP: The copy operation was completed
successfully

Copy succeeded

console#
```

Управление файлами устройства

На странице **Files on File System** (Файлы в файловой системе) представлена информация о файлах, хранящихся в системе, включая имена файлов, размеры файлов, изменения файлов и разрешения файлов. Файловая система позволяет управлять пятью файлами; максимальный размер одного файла составляет 0,5 МБ.

Чтобы открыть страницу **Files on File System** (Файлы в файловой системе), выберите **System** (Система)→ **File Management** (Управление файлами)→ **File System** (Файловая система) на панели дерева.

Рис. 6-110. Файлы в файловой системе



На странице **Files on File System** (Файлы в файловой системе) содержатся следующие поля:

- **File Name** (Имя файла). обозначает файл, хранящийся в системе управления файлами.
- **Size** (Размер). означает размер файла.
- **Modified** (Изменен). обозначает дату изменения файла.
- **Permission** (Разрешение). указывает тип разрешения, назначенный файлу. Возможные значения:
  - **Read Only** (Только чтение). обозначает файл, предназначенный только для чтения.
  - **Read Write** (Чтение и запись). обозначает файл, предназначенный для чтения и записи.
- **Remove** (Удалить). удаляет файл.
  - **Флажок установлен**. удаляет определенный файл из системы управления файлами.
  - **Флажок снят**. сохраняет определенный файл в системе управления файлами.
- **Rename** (Переименовать). изменяет имя файла. Имя файла изменяется в поле **File Name** (Имя файла).
- **Total Bytes** (Всего байт). обозначает общее количество занятого в данный момент места.
- **Free Bytes** (Свободные байты). обозначает количество оставшегося на данный момент свободного места.

Управление файлами с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для управления файлами системы

Команда консоли	**Описание**
dir	Отображение списка файлов в файловой системе флэш-памяти

Далее приведен пример команд консоли.

```
console# dir
Папка флэш-памяти:

Имя файла       Разрешение  Объем флэш-памяти  Размер данных  Изменено
--------------  ------      ------             ------         --------------------
3.txt           rw          524288             523776         22-Feb-2005 18:49:27
setup           rw          524288             95             22-Feb-2005 15:58:19
setup2          rw          524288             95             22-Feb-2005 15:58:35
image-1         rw          4325376            4325376        06-Feb-2005 17:55:32
image-2         rw          4325376            4325376        06-Feb-2005 17:55:31
test.txt        rw          524288             95             22-Feb-2005 12:16:44
aaafile.prv     --          131072             --             06-Feb-2005 19:09:02
syslog1.sys     r-          262144             --             22-Feb-2005 18:49:27
syslog2.sys     r-          262144             --             22-Feb-2005 18:49:27
directory.prv   --          262144             --             06-Feb-2005 17:55:31
startup-config  rw          524288             347            22-Feb-2005 11:56:03
```

```
Общий объем флэш-памяти: 16646144 байт
Свободное место на флэш-памяти: 4456448 байт
```

Расширенные параметры

Используйте страницу Advanced Settings (Расширенные параметры) для настройки различных общих атрибутов коммутатора. Внесенные изменения вступают в силу только после перезагрузки коммутатора.

Для получения интерактивной справки для текущей страницы перейдите по указанной ниже ссылке.

Чтобы открыть страницу **Advanced Settings** (Расширенные параметры), выберите **System** (Система)→ **Advanced Settings** (Расширенные параметры) на панели дерева.

Страница **Advanced Settings** (Расширенные параметры) содержит ссылки для настройки общих параметров.

В этом разделе имеются следующие тематические подразделы:

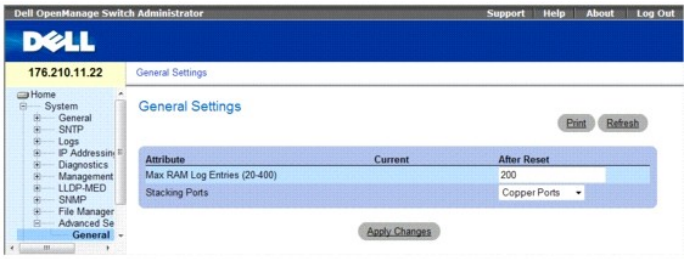
- Настройка общих параметров

Настройка общих параметров

Страница **General Settings** (Общие параметры) сдержит информацию, позволяющую определить общие параметры устройства.

Чтобы открыть страницу **General Settings** (Общие параметры), выберите **System** (Система)→ **Advanced Settings** (Расширенные параметры)→ **General** (Общие параметры) на панели дерева.

Рис. 6-111. Страница General Settings (Общие параметры)



Страница **General Settings** (Общие параметры) содержит следующую информацию:

- **Attribute** (Атрибут). общий атрибут параметра.
- **Current** (Текущее). текущее настроенное значение.
- **After Reset** (После перезагрузки). будущее значение (после перезагрузки). При вводе значения в столбце After Reset (После сброса) выделяется память для поля таблицы.
- **Max RAM Log Entries (20-400)** (Максимальное число записей журнала ОЗУ). максимальное число записей журнала ОЗУ. Когда журнал заполнен, он очищается, и файл журнала перезагружается.
- **Stacking Ports** (Порты стекирования). тип портов стекирования: порты с медными разъемами или оптоволоконные порты.

Просмотр счетчика записей журнала ОЗУ с помощью команд консоли

В следующей таблице приведены команды консоли для настройки полей, отображаемых на странице **General Settings** (Общие параметры).

Команда консоли	**Описание**
logging buffered size *число*	Задает число системных сообщений, хранящихся во внутреннем буфере (ОЗУ).

Далее приведен пример команд консоли.

```
console(config)# logging buffered size 300
```

Назад на страницу "Содержание"

Назад на страницу Содержание

Информация о настройке коммутатора

Руководство пользователя систем Dell™ PowerConnect™ 35xx

- Настройка безопасности сети
- Обзор списка ACL
- Настройка наблюдения по протоколу DHCP
- Настройка портов
- Настройка адресных таблиц
- Настройка протокола GARP
- Настройка протокола STP
- Настройка сетей VLAN
- Настройка голосовых сетей VLAN
- Объединение портов
- Поддержка пересылки многоадресного трафика

В этом разделе приведены все системные операции и общие сведения по настройке безопасности сети, портов, адресных таблиц, протокола GARP, сети VLAN, протокола STP, объединения портов и многоадресной поддержки.

Настройка безопасности сети

Используйте страницу **Network Security** (Безопасность сети) для настройки безопасности сети с помощью списков управления доступом и заблокированных портов. Чтобы открыть страницу **Network Security** (Безопасность сети), выберите Switch (Коммутатор)→ **Network Security** (Безопасность сети).

Раздел включает следующие темы:

- Проверка подлинности на основе порта
- Настройка расширенной проверки подлинности на основе порта
- Проверка подлинности пользователей
- Настройка безопасности портов

Расширенная проверка подлинности на основе порта

Проверка подлинности на основе порта обеспечивает проверку подлинности пользователей системы на основе портов через внешний сервер. Только прошедшие проверку подлинности и одобренные пользователи системы могут передавать и принимать данные. Проверка подлинности портов выполняется с помощью сервера RADIUS, использующего протокол EAP (Extensible Authentication Protocol). Проверка подлинности на основе порта включает:

- **Authenticators (Удостоверения)**. Определяет порт, для которого выполняется проверка подлинности перед разрешением доступа к системе.
- **Supplicants (Просители)**. Указывает хост, подключенный к проверенному порту, запрашивающему доступ к службам системы.
- **Authentication Server (Сервер проверки подлинности)**. Указывает внешний сервер, например сервер RADIUS, который выполняет проверку подлинности от имени администратора, а также указывает, может ли пользователь получить доступ к службам системы.

Проверка подлинности на основе портов формирует два состояния доступа:

- **Controlled Access (Управляемый доступ)**. Разрешает связь между просителем и системой, если проситель прошел проверку.
- **Uncontrolled Access (Неконтролируемый доступ)**. Разрешает неконтролируемый обмен данными независимо от состояния порта.

Устройство в настоящее время поддерживает проверку подлинности на основе порта с помощью серверов RADIUS.

Проверка подлинности на базе MAC

Проверка подлинности на базе MAC является альтернативой для 802.1x, которая обеспечивает доступ по сети к устройствам (таким как принтеры или IP-телефоны), которые не поддерживают формат запросов 802.1X. Проверка подлинности на базе MAC использует MAC-адрес подключаемого устройства для предоставления или запрета доступа по сети.

Расширенная проверка подлинности на основе порта

Расширенная проверка подлинности на основе порта

- Позволяет нескольким хостам подключаться к одному порту.
- Чтобы доступ к системе имели все хосты, требуется авторизация только одного хоста. Если порт не авторизован, то доступ всех присоединенных к нему хостов к сети закрыт.
- Устанавливает проверку подлинности по имени пользователя. Определенные группы VLAN в устройстве являются всегда доступными, даже если порты, подключенные к группе VLAN, не прошли авторизацию.
    - Например, для передачи голоса по IP не требуется проверка подлинности, а для трафика передачи данных требуется. Можно определить группы VLAN, для которых не требуется проверка подлинности. Непрошедшие проверку группы VLAN доступны для пользователей, даже если порты, подключенные к группе VLAN, определены как проверенные.

Расширенная проверка подлинности на основе порта реализована в следующих режимах:

- **Режим одиночного хоста**. Включает только авторизованный хост и обеспечивает один сеанс доступа к порту.
- **Многохостовый режим**. Обеспечивает один сеанс доступа нескольких хостов к одному порту. Требуется авторизация только одного хоста, чтобы доступ к сети имели все хосты. В случае неудачной проверки подлинности хоста или появления сообщения выхода EAPOL доступ запрещается для всех подключенных клиентов.
- **Многосеансовый режим**. Обеспечивает многосеансовый доступ авторизованного хоста к порту.
- **Гостевая сеть VLAN - предоставляет ограниченный доступ к сети для неавторизованных портов**. Если для порта запрещается доступ к сети через авторизацию на основе порта, а гостевая сеть VLAN включена, порт получает ограниченный доступ к сети. Например, администратор сети может использовать гостевые сети VLAN, чтобы запретить доступ к сети через проверку подлинности на основе порта, но разрешить доступ к Интернету для неавторизованных пользователей.

Страница **Port Based Authentication** (Проверка подлинности на основе порта) позволяет сетевому администратору провести настройку проверки подлинности на основе порта.

Чтобы открыть страницу **Port Based Authentication** (Проверка подлинности на основе порта), выберите **Switch** (Коммутатор)→ **Network Security** (Безопасность сети)→ **Port Based Authentication** (Проверка подлинности на основе порта).

Рис. 7-1. Страница Port Based Authentication (Проверка подлинности на основе порта)

Страница **Port Based Authentication** (Проверка подлинности на основе порта) содержит следующие поля:

- **Port Based Authentication State (Состояние проверки подлинности на основе порта)**. Позволяет выполнять проверку подлинности на основе порта для устройства. Возможные значения:
  - **Enable (Включено)**. Выполняется проверка подлинности на основе порта для устройства.
  - **Disable (Выключено)**. Отключена проверка подлинности на основе порта для устройства.
- **Authentication Method (Метод проверки подлинности)**. Указывает используемый метод проверки подлинности. Возможные значения:
  - **None (Нет)**. Для проверки подлинности порта не используется никакой метод проверки.
  - **RADIUS**. Сообщает, что проверка подлинности на основе порта выполняется на сервере RADIUS.
  - **RADIUS, None (RADIUS, Нет)**. Сообщает, что проверка подлинности на основе порта сначала выполняется на сервере RADIUS. Если проверка подлинности порта не выполняется, то не используется никакой метод проверки подлинности, и сеанс разрешается.
- **Guest VLAN (Гостевая сеть VLAN) - определяет, включена ли гостевая сеть VLAN для устройства**. Возможные значения:
  - **Enable (Включено)**. Включение гостевой сети VLAN для неавторизованных портов. Если включен параметр гостевой сети VLAN, неавторизованный порт автоматически присоединяется к сети VLAN, выбранной в поле со списком сетей VLAN.
  - **Disable (Выключено)**. Отключает использование голосовых сетей VLAN для неавторизованных портов. Это значение по умолчанию.
- **VLAN List (Список сетей VLAN)**. Выводит список сетей VLAN. Гостевая VLAN выбирается из списка сетей VLAN.

Параметры интерфейса

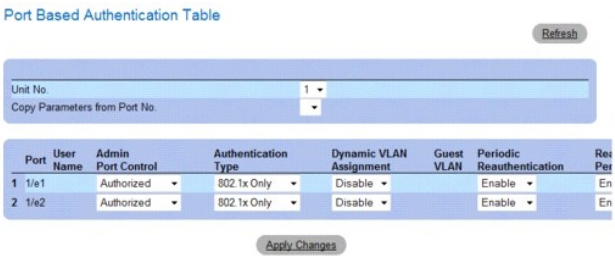
- **Interface (Интерфейс)**. Содержит список интерфейсов, для которых можно включить проверку подлинности на основе порта.
- **User Name (Имя пользователя)**. Указывает имя пользователя просителя.
- **Admin Interface Control** (Управление интерфейсом) - определяет состояние авторизации порта. Возможные значения:
  - **Auto (Автоматический)**. Включает проверку подлинности на основе порта для устройства. Авторизация интерфейса включается или выключается в зависимости от обмена данными между устройством и клиентом в ходе проверки подлинности.
  - **Authorized (Авторизирован)**. Устанавливает интерфейс в состояние авторизации без проверки подлинности. Интерфейс посылает и получает нормальный трафик без проверки подлинности клиента на основе порта.
  - **Unauthorized (Неавторизирован)**. Запрещает доступ к выбранной системе интерфейса и переводит интерфейс в неавторизованное состояние. Устройство не обеспечивает проверку подлинности клиента через интерфейс.
- **Current Interface Control (Текущее управление интерфейсом) - текущее состояние авторизации порта**.
- **Authentication Type (Тип авторизации)**. Определяет тип авторизации порта. Возможные значения:
  - **802.1x Only (Только 802.1x)**. Устанавливает тип авторизации только на основе 802.1x.
  - **MAC Only (Только MAC)**. Устанавливает тип авторизации только на основе MAC.
  - **802.1x & MAC**. Устанавливает типы авторизации 802.1x и MAC.
- **Dynamic VLAN Assignment (Динамическое распределение VLAN)**. Показывает, включен ли режим динамического распределения VLAN для этого порта. Эта функция позволяет сетевым администраторам автоматически распределять пользователей сетям VLAN при авторизации на сервере RADIUS. После авторизации пользователя сервером RADIUS, он автоматически подключается к сети VLAN, конфигурация которой произведена сервером RADIUS.
  - При включении функции DVA необходимо отключить функции Port Lock и Port Monitor.
  - Динамическое распределение VLAN (DVA) может работать только при условии того, что выполнено конфигурирование сервера RADIUS, включена функция авторизации порта и установлен режим авторизации 802.1x для многосеансового доступа.
  - Если ответное сообщение сервера RADIUS не содержит названия сети VLAN пользователя, значит, пользователю отказано в доступе.
  - Авторизованные порты будут добавлены к VLAN пользователя как непомеченные.
  - Неавторизованные порты остаются членами VLAN и Гостевой VLAN. Конфигурация статической VLAN не была применена к этому порту.
  - В списке, (см. ниже), указаны сети VLAN, которые не подлежат обработке функцией DVA: Неавторизованная VLAN, Динамическая VLAN, созданная GVRP, Голосовая VLAN, VLAN, созданная по умолчанию и Гостевая VLAN.
  - Сетевые администраторы могут удалять VLAN пользователя, пока он зарегистрирован в системе. Пользователь авторизуется при следующей повторной авторизации, если VLAN этого пользователя будет создана заново или на сервере RADIUS будет сконфигурирована новая VLAN.
- **Guest VLAN (Гостевая VLAN)**. Если включен параметр, то неавторизованные пользователи, подключенные к этому интерфейсу, могут иметь доступ к гостевой сети VLAN.
  - **Enable (Включить)** . Обеспечивает доступ к гостевой сети VLAN для неавторизованных пользователей.
  - **Disable (Выключить)**. Закрывает доступ к гостевой сети VLAN для неавторизованных пользователей.
- **Periodic Reauthentication (Периодическое повторение проверки подлинности)**. для выбранного порта, выполняется периодическая проверка подлинности. Период повторения проверки подлинности определяется в поле **Reauthentication Period (300-4294967295)** (Период повторения проверки подлинности).
  - **Enable (Включить)**. Включает периодическую проверку подлинности порта.
  - **Disable (Выключить)**. Выключает периодическую проверку подлинности порта.
- **Reauthentication Period (300-4294967295)** (Период повторения проверки подлинности) - определяет время, по истечению которого для выбранного порта будет выполнена повторная проверка подлинности. Значение этого поля указывается в секундах. Значение по умолчанию: 3600 секунд.
- **Reauthenticate Now** (Немедленная повторная проверка подлинности) - выполняет повторную проверку подлинности выбранного порта.
  - **Флажок установлен**. Включает немедленную проверку подлинности порта.
  - **Disable (Выключить)**. Выключает немедленную проверку подлинности порта.
- **Authentication Server Timeout (1-65535)** (Время ответа сервера проверки подлинности) - определяет время, которое проходит, прежде чем устройство посылает повторный запрос серверу проверки подлинности. Значение этого поля отображается в секундах. Значение по умолчанию: 30 секунд.
- **Resending EAP Identity Request (1-65535)** (Повторная отправка запроса EAP) - определяет время до повторной отправки запроса EAP. Значение по умолчанию: 30 секунд.
- **Quiet Period (0-65535) (Период молчания)**. Число секунд, в течение которых устройство остается в состоянии молчания после обмена данными в ходе неудачной проверки подлинности. Возможные значения поля: 0-65535. Значение по умолчанию: 60 секунд.
- **Supplicant Timeout (1-65535) (Тайм-аут просителя)**.Время до повторной отправки запросов EAP пользователю. Значение этого поля указывается в секундах. Значение по умолчанию: 30 секунд.
- **Max EAP Requests (1-10) (Максимальное число запросов EAP)**. Общее число отправляемых запросов EAP. Если ответ не получен по истечении указанного периода, процесс проверки подлинности начинается заново. Значение по умолчанию: 2 попытки.

Отображение таблицы проверки подлинности на основе порта

1. Откройте страницу **Port Based Authentication** (Проверка подлинности на основе порта).
2. Нажмите кнопку **Show All** (Показать все).

Откроется страница **Port Based Authentication Table** (Таблица проверки подлинности на основе порта).

Рис. 7-2. Таблица Port Based Authentication Table (Таблица проверки подлинности на основе порта)



Помимо полей, имеющихся на странице **Port Based Authentication Table** (Таблица проверки подлинности на основе порта), имеются следующие поля:

- **Unit No. (Номер устройства)**. Выбор номера устройства стека.
- **Copy Parameters from Port No. (Копировать параметр с порта номер...)**. Копирует параметры выбранного порта.

Копирование параметров в таблицу Port Based Authentication Table (Таблица проверки подлинности на основе порта)

1. Откройте страницу.
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **Port Based Authentication Table** (Таблица проверки подлинности на основе порта).
3. Выберите интерфейс в поле **Copy Parameters from Port No.** (Копировать параметры из порта №).
4. Выберите интерфейс в таблице **Port Based Authentication Table** (Таблица проверки подлинности на основе порта).
5. Установите флажок в поле **Copy to** (Копировать в), чтобы определить интерфейс, для которого будут скопированы параметры проверки подлинности на основе порта.
6. Нажмите кнопку **Apply Changes** (Применить изменения).

Включение проверки подлинности на основе порта с использованием команд консоли

В следующей таблице приведены команды консоли для включения расширенной проверки подлинности на основе порта, соответствии с таблицей **Port Based Authentication** (Проверка подлинности на основании порта).

Команда консоли	**Описание**
aaa authentication dot1x default *метод1* [*метод2*.]	Указывает один или несколько методов проверки подлинности, авторизации и учета (AAA), используемые на интерфейсах IEEE 802.1X.
dot1x auth-not-req	Обеспечивает доступ к VLAN авторизованных устройств.
dot1x guest-vlan	Определяет Гостевую VLAN.
dot1x guest vlan enable	Обеспечивает интерфейсный доступ авторизованных пользователей к Гостевой VLAN.
dot1x mac-authentication	Выполняет проверку подлинности на основе MAC-адреса станции (проверка подлинности на основе MAC).
dot1x max-req *число*	Устанавливает максимальное число попыток отправки запросов EAP клиенту перед возобновлением процесса проверки подлинности.
dot1x re-authenticate [**ethernet** *интерфейс*]	Инициализирует вручную повторную проверку подлинности всех портов, поддерживающих 802.1X или указанного порта, поддерживающего 802.1X.
dot1x re- authentication	Включает периодические повторные проверки подлинности клиента.
dot1x timeout quiet-period *секунды*	Устанавливает число секунд, в течение которых устройство остается в состоянии молчания после обмена данными в ходе неудачной проверки подлинности.
dot1x timeout re-authperiod *секунды*	Устанавливает число секунд между попытками повторной проверки подлинности.
dot1x timeout server-timeout *секунды*	Устанавливает время повторной передачи пакетов на сервер проверки подлинности.

dot1x timeout supp-timeout *секунды*	Устанавливает время для повторной отправки кадра запроса EAP клиенту.
dot1x timeout tx- period *секунды*	Устанавливает число секунд, в течение которых устройство ожидает ответа на запрос EAP от клиента перед повторной отправкой запроса.
dot1x traps mac-authentication failure	Посылает сигнал прерывания при отрицательном результате проверки подлинности MAC-адреса (при проверке подлинности на основе MAC-адресов).
dot1x radius-attribues vlan	Обеспечивает подключение пользователя к сети VLAN, в зависимости от типа пользователя.
show dot1x [ethernet ***интерфейс***]	Отображает состояние 802.1X для устройства или указанного интерфейса.
show dot1x advanced	Отображает расширенные функции 802.1X коммутатора указанного интерфейса.
show dot1x users [**username** *имя пользователя*]	Отображает пользователей 802.1X для устройства.
dot1x guest-vlan enable	Включает использование гостевой сети VLAN для неавторизованных портов. Если включен параметр гостевой сети VLAN, неавторизованный порт автоматически присоединяется к сети VLAN, выбранной в поле со списком сетей VLAN. Значение по умолчанию: отключено.
dot1x guest-vlan	Выводит список гостевых сетей VLAN. Гостевая VLAN выбирается из списка сетей VLAN.

Далее приведен пример команд консоли.

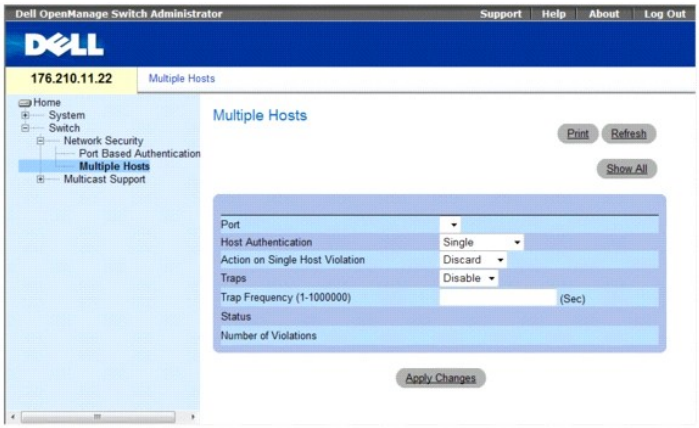
```
Console# show dot1x

Interface  Admin Mode  Oper Mode    Reauth Control  Reauth Period  Username
---------  ----------  -----------  --------------  -------------  --------
1/e1       Auto        Authorized   Ena             3600           Bob
1/e2       Auto        Authorized   Ena             3600           John
1/e3       Auto        Unauthorized Ena             3600           Clark
1/e4       Force-auth  Authorized   Dis             3600           n/a
```

Настройка расширенной проверки подлинности на основе порта

Страница **Multiple Hosts** (Несколько хостов) содержит информацию, позволяющую определить параметры расширенной проверки подлинности на основе порта для определенных портов и сетей VLAN.Для получения более подробной информации по расширенной проверке подлинности на основе порта, см. раздел **Advanced Port Based Authentication** (Настройка расширенной проверки подлинности на базе портов).

Чтобы открыть страницу **Multiple Hosts** (Несколько хостов), выберите **Switch** (Коммутатор)→ **Network Security** (Безопасность сети)→ **Multiple Hosts** (Несколько хостов).

Рис. 7-3. Страница Multiple Hosts (Несколько хостов)



Страница **Multiple Hosts** **(Несколько хостов) содержит следующие поля:**

- **Port (Порт)**. Номер порта, для которого включен режим расширенной проверки подлинности на основе порта.
- **Host Authentication (Проверка подлинности хоста)**. Определяет тип проверки подлинности хоста. Возможные значения полей:
  - **Single (Режим одиночного хоста)**. Включает только авторизованный хост и обеспечивает один сеанс доступа к порту.

- **Multiple Host (Несколько хостов)**. Задействует один хост для авторизации нескольких хостов, для осуществления одного сеанса входа в систему. Этот параметр необходимо включить, чтобы отключить фильтр на входе или использовать защиту блокировки для выбранного порта.
- **Multiple Session (Несколько сеансов)**. Предоставляет многосеансовый доступ одного авторизованного хоста к системе. Это значение по умолчанию.

- **Action on Single Host Violation (Действие при нарушении доступа одного хоста)**. Определяет действие, которое необходимо применять для пакетов, поступающих в режиме одного хоста от хоста, MAC-адрес которого отличается от MAC-адреса клиента (просителя). Возможные значения:
  - **Forward (Переслать)**. Пересылает пакет от неизвестного источника, но MAC-адреса не распознаются.
  - **Discard (Отвергнуть)**. Отбрасывает пакеты от любого неизвестного источника. Это значение по умолчанию.
  - **Shutdown (Завершить работу)**. Отбрасывает пакеты от любого неизвестного источника и блокирует порт. Порты останутся выключенными, пока не будет выполнена их активизация или сброс коммутатора.
- **Traps (Системные прерывания)**. Включает или отключает отправку системных прерываний на хост в случае нарушения доступа.
  - **Enable (Включить)**. Включает пересылку прерываний.
  - **Disable (Выключить)**. Выключает пересылку прерываний.
- **Trap Frequency (1-1000000) (Частота системных прерываний (сек))**. Определяет временной интервал между отправками системных прерываний на хост. Поле **Trap Frequency (1-1000000)** (Частота системных прерываний) можно определить только в том случае, если для поля **Multiple Hosts** (Несколько хостов) указано значение **Disable** (Отключить). Значение по умолчанию: 10 секунд.
- **Status (Состояние)**. Состояние хоста. Возможные значения:
  - **Unauthorized (Неавторизован)**. Означает, что управление портом является *Force Unauthorized* (Принудительно не авторизовано), соединение порта закрыто или порт управляется автоматически (Auto), но проверка подлинности клиента не была произведена через порт.
  - **Not in Auto Mode (Автоматический режим отключен)**. Указывает, что управление портом является *Forced Authorized* (Принудительно авторизован) и клиенты имеют полный доступ к порту.
  - **Single-host Lock (Блокировка одного хоста)**. Указывает, что портом управляется автоматически (*Auto*) и была произведена проверка подлинности одного клиента через порт.
  - **No Single Host (Не один хост)**. Указывает, что включен параметр Multiple Host (Несколько хостов).
- **Number of Violations (Число нарушений)**. Число пакетов, поступивших на интерфейс в режиме одного хоста от хоста, MAC-адрес которого отличается от MAC-адреса клиента (просителя).

Отображение таблицы Multiple Hosts Table (Таблица нескольких хостов)

1. Откройте страницу **Multiple Hosts** (Несколько хостов).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется таблица **Multiple Hosts Table** (Таблица нескольких хостов) opens.

Рис. 7-4. Страница Multiple Hosts Table (Таблица нескольких хостов)

Таблица **Multiple Hosts Table** (Таблица нескольких хостов) имеет следующее дополнительное поле:

- **Unit No. (Номер устройства)**. Выбор номера устройства стека.

Включение нескольких хостов с использованием команд консоли

В следующей таблице приведены команды консоли для включения расширенной проверки подлинности на основе порта, соответствующие полям на странице **Multiple Hosts** (Несколько хостов).

Команда консоли	Описание
dot1x multiple-hosts	Разрешает наличие нескольких хостов (клиентов) на проверяемом порту 802.1X, для которых в команде настройки интерфейса dot1x port-control установлено значение auto.

dot1x single-host-violation {forward |discard |discard-shutdown}[trap секунды]	Настраивает действие, которое необходимо выполнить, когда станция, MAC-адрес которой отличается от MAC-адреса клиента (просителя), осуществляет попытку доступа к интерфейсу.

Далее приведен пример команды консоли.

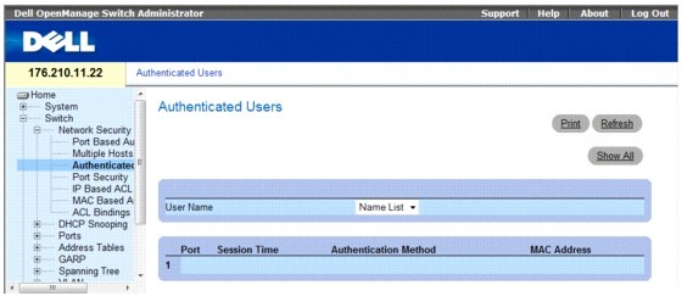
```
Console(config)# interface ethernet 1/e1

Console(config-if)# dot1x multiple-hosts
```

Проверка подлинности пользователей

Страница **Authenticated Users** (Проверяемые пользователи) отображает список доступа пользователей к портам. Этот список определяется на странице **Add User Name** (Добавление имени пользователя).

Чтобы открыть страницу **Authenticated Users** (Проверка подлинности пользователей), выберите **Switch** (Коммутатор)→ **Network Security** (Безопасность сети)→ **Authenticated Users** (Пользователи, подлинность которых прошла проверку).

Рис. 7-5. Страница Authenticated Users (Проверка подлинности пользователей)



Страница **Authenticated Users** (Проверка подлинности пользователей) содержит следующие поля:

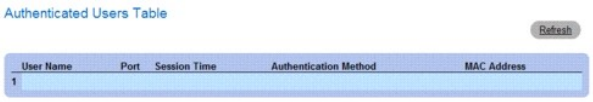
- **User Name (Имя пользователя)**. Список пользователей, авторизованных с использованием сервера RADIUS.
- **Port (Порт)**. Номера портов, используемые для проверки подлинности - для каждого имени пользователя.
- **Session Time (Время сеанса)**. Время с момента входа пользователя на устройство. Формат поля **дни:часы:минуты:секунды**, например 3 дня: 2 часа: 4 минуты: 39 секунд.
- **Authentication Method (Метод проверки подлинности)**. Метод, использовавшийся при последней проверке подлинности. Возможные значения:
  - **Remote (Удаленно)**. Проверка подлинности пользователя выполняется на удаленном сервере.
  - **None (Нет)**. Проверка подлинности пользователя не выполнялась.
- **MAC Address (MAC-адрес) - MAC-адрес просителя.**

Отображение таблицы проверки подлинности пользователей

1. Откройте страницу **Authenticated Users** (Проверка подлинности пользователей).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **Authenticated Users Table** (Таблица проверки подлинности пользователей).

   Рис. 7-6. Страница Authenticated Users Table (Таблица проверки подлинности пользователей)



Проверка подлинности пользователей с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для проверки подлинности пользователей, соответствующие полям на странице

Authenticated Users (Проверка подлинности пользователя).

Команда консоли	Описание
show dot1x users [**username** *имя пользователя*]	Отображает пользователей 802.1X для устройства.

Далее приведен пример команд консоли.

```
console# show dot1x users

Port Username Session Time Auth Method MAC Address

-----------------------------------------------------------------

1/e11 gili 00:09:27 Remote 00:80:c8:b9:dc:1d
```

Настройка безопасности портов

Безопасность сети можно повысить, если разрешить доступ к определенным портам только пользователям с определенными MAC-адресами. MAC-адреса определяются динамически в процессе подключения или настраиваются статически. Функция безопасности блокировки портов проверяет полученные пакеты и определяет, откуда был получен пакет для определенных портов. Доступ к заблокированным портам разрешается только пользователям с определенными MAC-адресами. Эти адреса вводятся вручную для порта или определяются при попытке доступа к заблокированному порту. Когда заблокированный порт получает пакет, и MAC-адрес источника пакета не связан с этим портом (определен на другом порте или неизвестен системе), активизируется механизм защиты и могут быть выполнены различные действия. Несанкционированные пакеты, поступающие на заблокированный порт:

- Пересылаются
- Игнорируются без системного прерывания
- Игнорируются с системным прерыванием
- Порт отключен

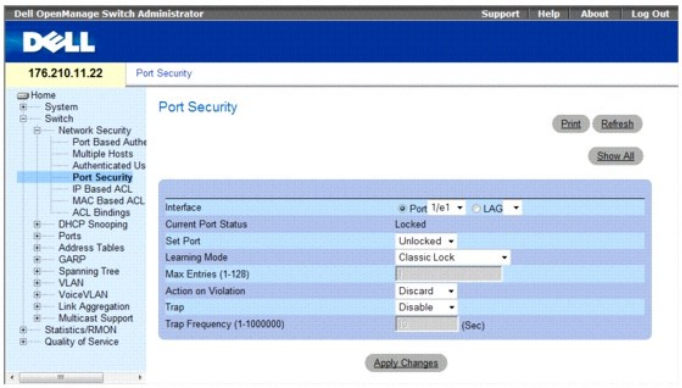
Функция безопасности Locked Port (Заблокированный порт) позволяет сохранить список MAC-адресов в файле конфигурации. Этот список MAC-адресов можно восстановить после перезагрузки устройства.

Чтобы включить функцию безопасности портов, сначала необходимо включить функцию **Multiple Hosts** (Несколько хостов) на выбранных портах.

Отключенные порты могут быть включены на странице **Port Security** (Безопасность портов). На странице **Ports** (Порты) находятся ссылки для настройки работы портов, в том числе таких функций, как контроль «лавины», зеркалирование портов и виртуальное тестирование портов.

Чтобы открыть страницу **Port Security** (Безопасность портов), выберите **Switch** (Коммутатор)→ **Network Security** (Безопасность сети)→ **Port Security** (Безопасность портов).

Рис. 7-7. Страница Port Security (Безопасность портов)



Страница **Port Security** (Безопасность портов) содержит следующие поля:

- **Interface (Интерфейс)**. Выбранный тип интерфейса, на котором включена блокировка порта.
  - **Port (Порт)**. Выбранный тип интерфейса - порт.
  - **LAG**. Выбранный тип интерфейса - LAG.
- **Current Port Status (Текущее состояние порта)**. Определяет текущее состояние порта.
- **Set Port (Установить порт)**. Порт заблокирован или разблокирован. Возможные значения:
  - **Unlocked (Разблокирован)**. Порт разблокирован. Это значение по умолчанию.
  - **Locked (Заблокирован)**. Порт заблокирован.
- **Learning Mode (Метод определения)**. Определение типа заблокированного порта. Поле **Learning Mode (Метод определения)** будет активно

только в том случае, если выбран параметр **Locked** в поле **Set Port**. Возможные значения поля:

- **Classic Lock (Классическая блокировка)**. Блокирует порт с использованием классического механизма блокировки. Порт блокируется сразу же, независимо от числа адресов, уже определенных.
- **Limited Dynamic Lock (Ограниченная динамическая блокировка)**. Блокирует порт путем удаления текущего динамического MAC-адреса, ассоциированного с этим портом. Порт может определять только некоторое максимальное количество допустимых для него адресов. Включаются вновь определенные и MAC-адреса и адреса с истекшим сроком действия.

- **Max Entries (1-128) (Максимальное число записей 1-128)**. Указывает число MAC-адресов, которые можно определить для данного порта. Поле **Max Entries** (Максимальное число записей) будет активно только в том случае, если выбран параметр **Locked** (Заблокировано) в поле **Set Port** (Установить порт). Кроме того, выбирается ограниченная динамическая блокировка. Значение по умолчанию: 1.
- **Action on Violation (Действие при нарушении)**. Действие, которое должно применяться к пакетам, поступающим на заблокированный порт. Возможные значения:
  - **Forward (Переслать)**. Пересылает пакет от неизвестного источника, но MAC-адреса не распознаются.
  - **Discard (Отвергнуть)**. Отбрасывает пакеты от любого неизвестного источника. Это значение по умолчанию.
  - **Shutdown** (Завершить работу) - отбрасывает пакеты от любого неизвестного источника и блокирует порт. Порты останутся выключенными, пока не будет выполнена их повторная активизация или сброс устройства.
- **Trap (Системное прерывание)**. Включает системные прерывания, отправляемые при получении пакета на заблокированный порт.
- **Trap Frequency (1-1000000) (Частота системных прерываний)**. Время в секундах, которое проходит между системными прерываниями. Значение по умолчанию: 10 секунд.

Определение заблокированного порта

1. Откройте страницу **Port Security** (Безопасность портов).
2. Выберите тип и номер интерфейса.
3. Определите поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Заблокированный порт будет добавлен в **Port Security Table** (Таблицу безопасности портов), а устройство обновлено.

Отображение таблицы безопасности портов

1. Откройте страницу **Port Security** (Безопасность портов).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **Port Security Table** (Таблица безопасности портов).

   Отключенные порты могут быть определены на странице **Port Security Table** (Таблица безопасности портов)**.**

Рис. 7-8. Страница Port Security Table (Таблица безопасности портов)

Таблица безопасности портов (Port Security Table) содержит следующие дополнительные поля:

- **Unit No. (Номер устройства)**. Указывает номер устройства стека, для которого отображается информация о заблокированных портах.
- **Copy Parameters from (Копировать параметры из)**. Указывает порт, из которого нужно скопировать параметры, и который назначен устройству с данным номером.

Настройка безопасности заблокированных портов с помощью команд консоли

В следующей таблице приведены команды консоли для настройки функции безопасности заблокированных портов, как отображается на странице Port Security (Безопасность портов).

Команда консоли	**Описание**
Завершение работы	Отключает интерфейсы.
set interface active {**ethernet** *интерфейс* | **port-channel** *номер_канала_порта*}	Вновь активизирует интерфейс, отключенный по причинам безопасности порта.
port security learning {disabled | dynamic}	Определение типа заблокированного порта.
port security max *max-addr*	Указывает количество MAC-адресов, которое может быть определено для данного порта.
port security [**forward** | **discard** | **discard-shutdown**] [**trap** *секунды*]	Блокирует функцию опознавания новых адресов для интерфейса.
show ports security {**ethernet** *интерфейс* | **port-channel** *номер_канала_порта*}	Выводит состояние блокировки для порта.

Далее приведен пример команд консоли.

console # **show ports security**

Port	Status	Action	Trap	Frequency	Counter
1/e1	locked	Discard	Enable	100	88
1/e2	locked	Discard, Shutdown	Disable		
1/e3	Unlocked	-	-	-	-

Обзор списка ACL

Списки управления доступом (ACL) позволяют сетевым администраторам определять классификационные действия и правила для определенных входных портов. Пакеты, поступающие на входной порт с активным списком ACL, пропускаются или отбрасываются и входной порт отключается. Если они отбрасываются, пользователь может отключить порт.

В этом разделе имеются следующие тематические подразделы:

- Определение списков ACL, основанных на IP-адресах
- Определение списков управления доступом, основанных на MAC-адресах
- Определение привязки списка ACL

Определение списков ACL, основанных на IP-адресах

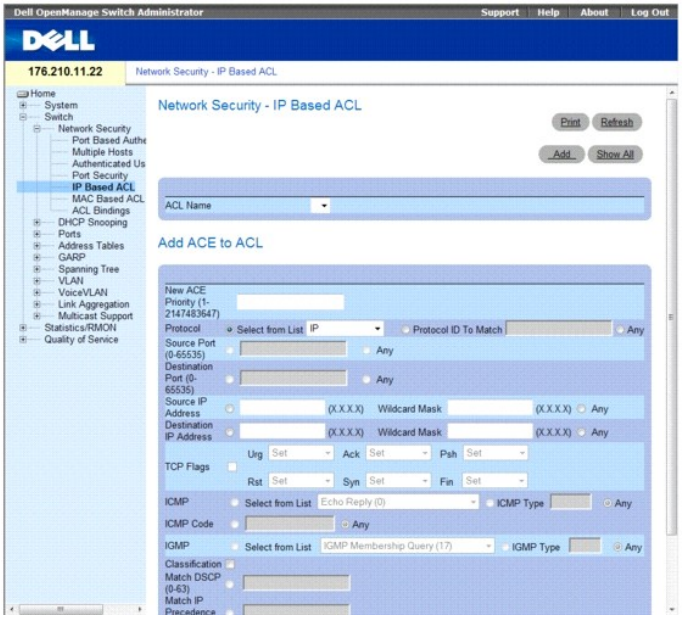
Списки управления доступом (ACL), состоящие из записей управления доступом (ACE), позволяют сетевым администраторам определять классификационные действия и правила для определенных входных портов. Пакеты, поступающие на входной порт с активным списком ACL, пропускаются или отбрасываются и входной порт отключается. Если они отбрасываются, пользователь может отключить порт.

Например, администратор сети определяет правило ACL, которое устанавливает, что порт с номером 20 может получить пакеты TCP, но если будет получен пакет UDP, этот пакет будет отброшен.

Списки ACL состоят из элементов управления доступом (ACE), которые создают фильтры, определяющие классификации трафиков. Каждая запись ACE является правилом; доступно 256 правил. Правила предназначены не только для конфигурации пользователя, они также используются для отслеживания протоколов DHCP, группировки протоколов VLAN и PVE, поэтому не все 256 правил доступны для записей ACE. Предполагается, что для пользователя доступно по крайней мере 124 правил. Если обнаружено, что доступно меньшее количество правил, причиной этого, возможно, является отслеживание протокола DHCP. Для того, чтобы сделать правила для записей ACE доступными, можно изменить число записей функции отслеживания протокола DHCP.

Чтобы определить ACL на основе IP, выберите **Switch** (Коммутатор)→ **Network Security** (Безопасность сети)→ **IP Based ACL** (ACL на основе IP).

Рис. 7-9. Network Security - IP Based ACL (Безопасность сети - ACL на основе IP-адресов)



- **ACL Name (Имя ACL)**. Определенный пользователем список ACL.
- **New ACE Priority (Новый приоритет ACE)**. Приоритет ACE, определяющий, какая запись ACE соответствует пакету на основе схемы первого совпадения.
- **Protocol (Протокол)**. Включает создание новой записи ACE, основанной на определенном протоколе. Возможные значения:
  - ***IP - протокол Интернета (IP)***. Определяет формат пакетов и способ назначения адресов для них. IP назначает пакетам адреса и пересылает пакеты на нужный порт.
  - ***ICMP - Internet Control Message Protocol (протокол управления сообщениями в сети - ICMP)***. Протокол ICMP позволяет шлюзу или хосту назначения устанавливать связь с хостом, являющимся источником данных, например, для передачи отчета об ошибке обработки.
  - ***IGMP - протокол управления группами Интернета (Internet Group Management Protocol (IGMP))***. Позволяет хостам уведомлять локальный коммутатор или маршрутизатор о том, что они могут получить передачи, назначенные для определенной многоадресной группы.
  - ***TCP - протокол управления передачей (Transmission Control Protocol (TCP))***. Обеспечивает двум хостам возможность установки связи и обмена потоками данных. TCP гарантирует доставку пакета, а также передачу и прием пакетов в порядке их отправки.
  - ***EGP - протокол внешнего шлюза (Exterior Gateway Protocol (EGP))***. Разрешает обмен данными маршрутизации между двумя соседними хостами шлюза в сети автономных систем.
  - ***IGP - протокол внутреннего шлюза (Interior Gateway Protocol (IGP)).*** Позволяет выполнять обмен данными маршрутизации между шлюзами в автономной сети.
  - ***UDP - протокол пользовательских датаграмм (User Datagram Protocol (UDP))***. Протокол связи, который передает пакеты, но не гарантирует их доставку.
  - ***HMP - протокол отображения хоста (Host Mapping Protocol (HMP))***. Собирает сетевую информацию с различных сетевых хостов. HMP контролирует разброс хостов в Интернете, а также хосты в отдельной сети.
  - ***RDP - протокол удаленного рабочего стола (Remote Desktop Protocol (RDP))***. Позволяет клиенту устанавливать связь с сервером терминала в сети.
  - ***IDPR*** - сопоставляет пакет с протоколом IDPR.
  - ***IPV6*** - сопоставляет пакет с протоколом IPV6.
  - ***IPV6 ROUTE*** - сопоставляет пакет с протоколом маршрутизации IPV6.
  - ***IPV6 FRAG*** - сопоставляет пакет с протоколом IPV6 FRAG.
  - ***IDRP - сопоставляет пакет с протоколом IDRP (Inter-Domain Routing Protocol)***.
  - ***RVSP - сопоставляет пакет с протоколом RSVP (ReSerVation Protocol)***.
  - ***AH - заголовок проверки подлинности (AH)***. Обеспечивает проверку подлинности хоста, являющегося источником данных, и целостность данных.
  - ***EIGRP - расширенный протокол маршрутизации внутреннего шлюза (Enhanced Interior Gateway Routing Protocol (EIGRP))***. Обеспечивает быструю сходимость, поддержку масок подсети различной длины, а также поддерживает протоколы нескольких уровней сети.
  - ***OSPF - протокол Open Shortest Path First (OSPF) -*** это протокол состояния канала, иерархический протокол внутреннего шлюза (IGP) для сетевого протокола туннелирования канального уровня (L2TP), дополнение к протоколу PPP, который используется поставщиками услуг Интернета для работы виртуальных частных сетей (VPN).
  - ***IPIP - IP через IP (IPIP)***. Формирует пакеты IP для создания туннелей между двумя маршрутизаторами. В результате туннель IPIP отображается как один интерефейс, а не как несколько отдельных интерфейсов. IPIP обеспечивает выход в Интернет в интрасетях с туннельным доступом и является альтернативой маршрутизации от источника.
  - ***PIM - сопоставляет пакет с протокольно независимой многоадресной рассылкой (PIM)***.

- ***L2TP - сопоставляет пакет с протоколом Интернета (L2IP)***.
- ***ISIS - промежуточная система - промежуточная система (ISIS)***. Распределяет информацию маршрутизации IP через единую автономную систему в сетях IP
- ***Protocol ID To Match (Идентификатор протокола для сопоставления)***. Добавляет определенные пользователем протоколы, пакеты которых будут сопоставляться с записью ACE. У каждого протокола имеется определенный уникальный номер. Возможные значения поля: 0-255.
- ***Any (Любой) - сопоставляет протокол с любым другим протоколом***.

- **Source Port (Порт-источник)**. Исходный порт TCP/UDP. Выберите значение **Any** (Любой), чтобы включить все порты.
- **Destination Port (Порт-приемник)**. Порт назначения TCP/UDP. Выберите значение **Any** (Любой), чтобы включить все порты.
- **Source IP Address (IP-адрес источника)**. Сопоставляет IP-адрес исходного порта, на который адресованы пакеты, с записью ACE. Маски ввода указывают, какие биты используются, а какие игнорируются. Маска ввода 0.0.0.0 указывает, что все биты важны.
- **Destination IP Address (IP-адрес назначения)**. Сопоставляет IP-адрес порта назначения, на который адресованы пакеты, с записью ACE. Маски ввода указывают, какие биты используются, а какие игнорируются. Маска ввода 0.0.0.0 указывает, что все биты важны.
- **TCP Flags (Флаги**). Устанавливает указанный флаг TCP, который может быть запущен. Для использования флагов TCP установите флажок **TCP Flag** (Флаг TCP), а затем выберите необходимые флаги.
- **ICMP**. Указывает тип сообщения ICMP для фильтрации пакетов ICMP. Можно выбрать из списка, ввести сообщение или выбрать значение **Any** (Любой) для всех типов сообщений ICMP. Это поле доступно, только когда в поле **Protocol** (Протокол) выбран ICMP.
- **ICMP Code (Код ICMP)**. Указывает код сообщения ICMP для фильтрации пакетов ICMP, которые могут фильтроваться по типу сообщения ICMP или по коду сообщения ICMP. Это поле доступно, только когда в поле **Protocol** (Протокол) выбран ICMP.
- **IGMP**. Пакеты IGMP могут фильтроваться по типу сообщения IGMP. Можно выбрать из списка, ввести сообщение или выбрать значение **Any** (Любой) для всех типов сообщений IGMP. Это поле доступно, только когда в поле **Protocol** (Протокол) выбран IGMP.
- **Classification Mach DSCP (Соответствие классификации DSCP)**. Сопоставляет значение пакета DSCP с записью ACL. При сравнении пакетов с записями ACL используется значение DSCP или значение приоритета пакета IP. Возможные значения поля: 0-63.
- **Match IP Precedence (Соответствие приоритета IP)**. Обозначает сопоставление приоритета IP-пакетов со значением приоритета IP-пакетов. Приоритет IP-пакетов включает маркированные кадры, превышающие пороговое значение CIR. В перегруженной сети кадры с высокой скоростью обработки данных не учитываются в отличие от кадров с низкой скоростью обработки данных.
- **Action (Действие)**. Указывает операцию передачи для ACL. Возможные значения:
  - **Permit (Разрешить)**. Пересылает пакеты, отвечающие критериям ACL.
  - **Deny (Запретить)**.Отбрасывает пакеты, отвечающие критериям ACL.
  - **Shutdown (Завершение работы)**. Отбрасывает пакет, отвечающий критериям ACL, и отключает порт, на который он был адресован.

Добавление записей ACE к спискам ACL, основанных на IP-адресах

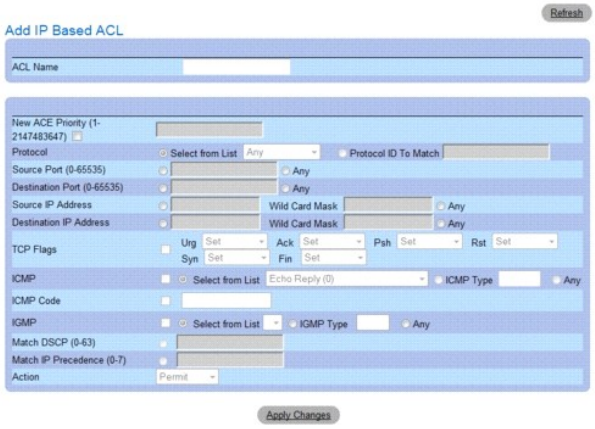
1. Откройте страницу **Network Security - IP Based ACL** (Безопасность сети - ACL на основе IP-адресов).
2. Выберите ACL.
3. Измените соответствующие поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Добавление списков ACL, основанных на IP-адресах

1. Откройте страницу **IP Based ACL** (ACL на основе IP-адресов):
2. Нажмите кнопку **Add** (Добавить).

   Откроется страница **Network Security - IP Based ACL** (Безопасность сети - ACL, основанный на IP-адресах).

   Рис. 7-10. Add IP Based ACL (Добавление ACL, основанного на MAC-адресах).



3. Определите соответствующие поля.

4. Нажмите кнопку **Apply Changes** (Применить изменения). Протокол, основанный на IP-адресах, будет определен, а устройство обновлено.

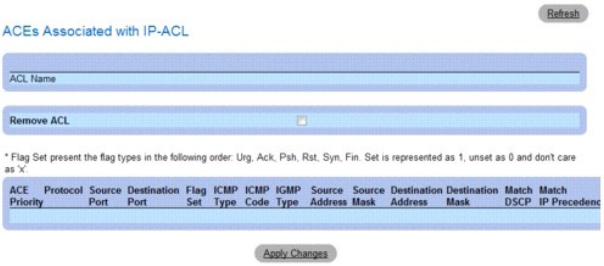
Отображение записей ACE, связанных со списками ACL на основе IP-адресов

1. Откройте страницу **Network Security - IP Based ACL** (Безопасность сети - ACL, основанный на IP-адресах).

2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница ACEs Associated with IP-ACL (Записи ACE, связанные с ACL, основанным на IP-адресах) .

Рис. 7-11. Страница ACEs Associated with IP-ACL (Записи ACE, связанные с ACL, основанным на IP-адресах)



Удаление списка ACL, основанного на IP-адресах

1. Откройте страницу **Network Security - IP Based ACL** (Безопасность сети - ACL, основанный на IP-адресах).

2. Нажмите кнопку **Show All** (Показать все). Откроется страница **ACEs Associated with IP-ACL Table** (Таблица с записями ACE, связанными с ACL, основанным на IP-адресах).

3. Установите флажок **Remove ACL** (Удалить ACL).

4. Нажмите кнопку **Apply Changes** (Применить изменения).

Удаление записи ACE, основанной на IP-адресах

1. Откройте страницу **Network Security - IP Based ACL** (Безопасность сети - ACL, основанный на IP-адресах).

2. Нажмите кнопку **Show All** (Показать все). Откроется страница **ACEs Associated with IP-ACL Table** (Таблица с записями ACE, связанными с ACL, основанным на IP-адресах).

3. Установите флажок **Remove** (Удалить) рядом с записью ACE.

4. Нажмите кнопку **Apply Changes** (Применить изменения).

Настройка списков ACL, основанных на IP-адресах, с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для настройки списков ACL, основанных на IP-адресах.

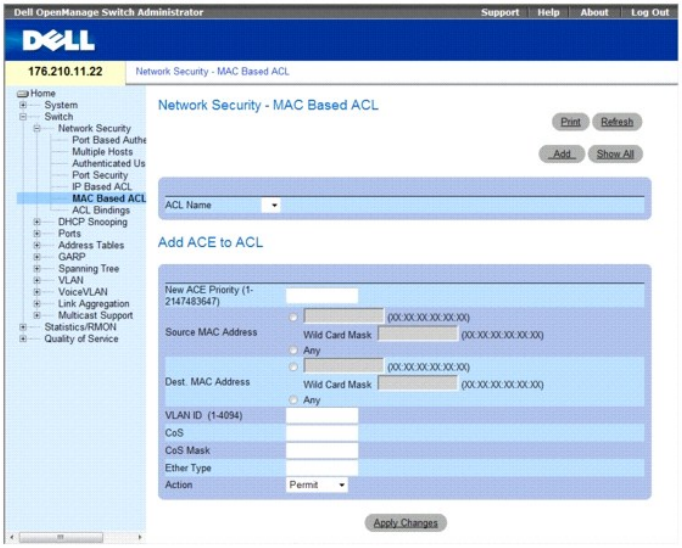
Команда консоли	**Описание**
ip access-list *имя-списка-доступа* **no ip access-list** *имя-списка-доступа*	Чтобы определить список доступа IPv4 и перейти в режим настройки списка доступа IPv4, используйте команду ipv4 access-list в режиме Global Configuration. Для удаления списка доступа используйте форму no этой команды.
permit {any| *протокол*} {any|{*источник маска_ввода_источника*}} {any|{*destination маска_ввода_назначения*}} [dscp *номер* | ip-precedence *номер*] [fragments] permit-icmp {any|{*источник маска_ввода_источника*}} {any|{*назначение маска_ввода_назначения*}} {any|*тип_icmp*} {any|*код_icmp*} [dscp *номер* | ip-precedence *номер*] permit-igmp {any|{*источник маска_ввода_источника*}} {any|{*назначение маска_ввода_назначения*}} {any|*тип_igmp*} [dscp *номер* | ip-precedence *номер*] permit-tcp {any|{ *источник маска_ввода_источника*}} {any|*порт_источника*} {any|{ *назначение маска_ввода_назначения*}} {any|*порт_назначения*} [dscp *номер* | ip-precedence *номер*] [flags *список_флагов*] permit-udp {any|{ *источник маска_ввода_источника*}} {any| *порт_источника*} {any|{*назначение маска_ввода_назначения*}} {any|*порт_назначения*} [dscp *номер* | ip-precedence *номер*]	Чтобы задать условия для прохождения пакета в именованный список доступа на основе IP-адресов, используйте команду разрешения в режиме настройки списка доступа.
deny [disable-port] {any| *протокол*} {any|{*источник маска_ввода_источника*}} {any|{*назначение маска_ввода_назначения*}} [dscp *номер* | ip-precedence *номер*] [fragments] deny-icmp [disable-port] {any|{*источник маска_ввода_источника*}} {any|{*назначение маска_ввода_назначения*}} {any|*тип_icmp*} {any|*код_icmp*} [dscp *номер* | ip-precedence *номер*] deny-igmp [disable-port] {any|{*источник маска_ввода_источника*}} {any|{*назначение маска_ввода_назначения*}} {any|*тип_igmp*} [dscp *номер* | ip-precedence *номер*] deny-tcp [disable-port] {any|{ *источник маска_ввода_источника*}} {any|*порт_источника*} {any|{ *назначение маска_ввода_назначения*}} {any|*порт_назначения*} [dscp *номер* | ip-precedence *номер*] [flags *список_флагов*] deny-udp [disable-port] {any|{ *источник маска_ввода_источника*}} {any|*источник_порта*} {any|{*назначение маска_ввода_назначения*}} {any|*порт_назначения*} [dscp *номер* | ip-precedence *номер*]	Чтобы задать условия для прохождения пакета в именованный список доступа на основе IP-адресов, используйте команду запрета в режиме настройки списка доступа.

Определение списков управления доступом, основанных на MAC-адресах

На странице **Network Security - MAC Based ACL** (Безопасность сети - ACL, основанный на MAC-адресах) можно определить списки ACL, основанные на MAC-адресах. Запись ACE может быть добавлена только в том случае, если список ACL не связан с интерфейсом.

Чтобы определить списки ACL, основанные на MAC-адресах, выберите **Switch** (Коммутатор)→ **Network Security** (Безопасность сети)→ **MAC Based ACL** (ACL, основанный на MAC-адресах).

- Network Security (Безопасность сети) - MAC Based ACL (ACL, основанный на MAC-адресах).



- **ACL Name (Имя ACL)**. Отображает определенные пользователем списки ACL, основанные на MAC-адресах.
- **New ACE Priority (Новый приоритет ACE)**. Приоритет ACE, определяющий, какая запись ACE соответствует пакету на основе схемы первого совпадения. Возможные значения: 1-2147483647.
- **Source Address (Адрес источника)**. Сопоставляет исходный MAC-адрес, на который адресованы пакеты, с записью ACE. Маски ввода указывают, какие биты используются, а какие игнорируются. Маска ввода 0.0.0.0 указывает, что все биты важны.
- **Destination Address (Адрес назначения)**. Сопоставляет MAC-адрес назначения, на который адресованы пакеты, с записью ACE. Маски ввода указывают, какие биты используются, а какие игнорируются. Маска ввода 0.0.0.0 указывает, что все биты важны.
- **VLAN ID (Идентификатор сети VLAN)**. Сопоставляет идентификатор сети VLAN пакета с записью ACE. Возможные значения этого поля от 1 до 4095.
- **CoS**. Указывает значения CoS, по которым фильтруются пакеты.
- **Cos Mask (Маска Cos)**. Указывает маску CoS, по которой фильтруются пакеты.
- **Ethertype**. Указывает пакет Ethertype, по которому фильтруются пакеты.
- **Action (Действие)**. Указывает операцию передачи для ACL. Возможные значения этого поля:
  - **Permit (Разрешить)**. Пересылает пакеты, отвечающие критериям ACL.
  - **Deny(Запретить)**. Отбрасывает пакеты, отвечающие критериям ACL.
  - **Shutdown (Завершение работы)**. Отбрасывает пакет, отвечающий критериям ACL, и отключает порт, на который он был адресован.

Добавление записей ACE к спискам ACL, основанных на IP-адресах

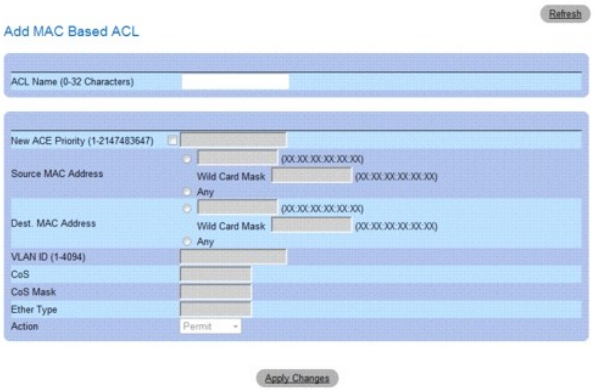
1. Откройте страницу **Network Security - MAC Based ACL** (Безопасность сети - ACL, основанный на MAC-адресах).
2. Выберите ACL.
3. Измените соответствующие поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Добавление списков ACL, основанных на MAC-адресах

1. Откройте страницу **MAC Based ACL** (ACL, основанный на MAC-адресах):
2. Нажмите кнопку **Add** (Добавить).

   Откроется страница **Network Security - MAC Based ACL** (Безопасность сети - ACL, основанный на MAC-адресах).

Рис. 7-12. Страница Add Mac Based ACL (Добавление ACL, основанного на MAC-адресах)

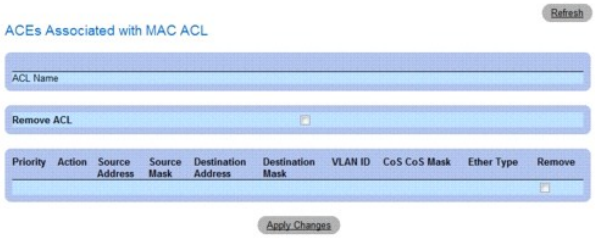


3. Определите соответствующие поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения). Протокол, основанный на MAC-адресах, будет определен, а устройство обновлено.

Отображение записей ACE, связанных со списками ACL на основе MAC-адресов

1. Откройте страницу **Network Security - MAC Based ACL** (Безопасность сети - ACL, основанный на MAC-адресах).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница ACEs Associated with MAC Based ACL (Таблица с записями ACE, связанными с ACL, основанным на MAC-адресах).



Удаление списка ACL, основанного на MAC-адресах

1. Откройте страницу **Network Security - MAC Based ACL** (Безопасность сети - ACL, основанный на MAC-адресах).
2. Нажмите кнопку **Show All** (Показать все). Откроется страница **ACEs Associated with MAC-ACL Table** (Таблица с записями ACE, связанными с ACL, основанным на MAC-адресах).
3. Установите флажок **Remove ACL** (Удалить ACL).
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Удаление записи ACE, основанной на MAC-адресах

1. Откройте страницу **Network Security - MAC Based ACL** (Безопасность сети - ACL, основанный на MAC-адресах).
2. Нажмите кнопку **Show All** (Показать все). Откроется страница **ACEs Associated with MAC-ACL Table** (Таблица с записями ACE, связанными с ACL, основанным на MAC-адресах).
3. Установите флажок **Remove** (Удалить) рядом с записью ACE.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Настройка списков ACL, основанных на MAC-адресах, с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для настройки списков ACL, основанных на MAC-адресах.

Команда консоли	Описание
mac access-list *имя-списка-доступа* **no mac access-list** *имя-списка-доступа*	Чтобы определить список доступа Layer 2 и перейти в режим настройки списка доступа MAC, используйте команду mac access-list в режиме Global Configuration. Для удаления списка доступа используйте форму no этой команды.
permit {any|{*источник маска_ввода_источника*} {any|{ *назначение маска_ввода_назначения*}} [vlan *идентификатор-vlan*] [cos *cos маска_ввода_cos*] [ethtype *тип-eth*] [inner-vlan *идентификатор-vlan*]	Чтобы задать условия разрешения для списка доступа на основе MAC-адресов, используйте команду разрешения в режиме настройки списка доступа на основе MAC-адресов.
deny [disable-port] {any|{*источник маска_ввода_источника*} {any| { *назначение маска_ввода_назначения*}} [vlan *идентификатор-vlan*] [cos *cos маска_ввода_cos*] [ethtype *тип-eth*] [inner-vlan *идентификатор-vlan*]	Чтобы задать условия запрета для списка доступа на основе MAC-адресов, используйте команду запрета в режиме настройки списка доступа на основе MAC-адресов.

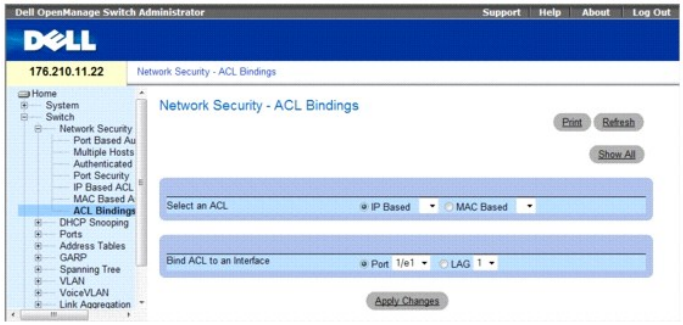
Определение привязки списка ACL

Когда выполняется связь списка ACL с интерфейсом, все правила, определенные в записях ACE, применяются для выбранного интерфейса. Каждый раз, когда список ACL назначается для порта или группы LAG или VLAN, потоки с этого входящего интерфейса, которые не соответствуют списку ACL, сравниваются с правилом по умолчанию (опускание несоответствующих пакетов).

Для привязки списков ACL к интерфейсам выполните следующие действия.

1. Откройте страницу **Network Security - ACL Bindings** (Безопасность сети - Привязки ACL), выберите **Switch** (Коммутатор)→ **Network Security** (Безопасность сети)→ **ACL Binding**s (Привязки ACL).

   Рис. 7-13. Страница Network Security - ACL Binding (Безопасность сети - Привязки ACL)



2. В поле **Select an ACL** (Выбрать ACL) выберите значение IP Based (ACL на основе IP-адресов) или MAC Based (ACL на основе MAC-адресов).

3. В поле **Bind ACL to an Interface** (Привязать список ACL к интерфейсу) выберите порт или LAG.

4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Список ACL будет привязан к интерфейсу.

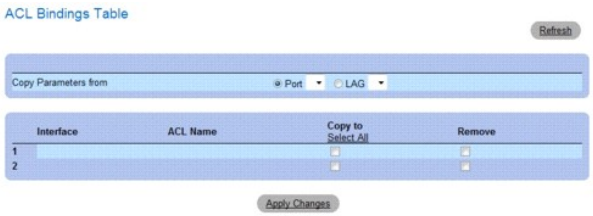
Отображение таблицы привязки ACL

1. Откройте страницу **Network Security - ACL Binding** (Безопасность сети - Привязки ACL).

2. Нажмите кнопку **Show All** (Показать все).

   Откроется страницаACL Bindings Table (Таблица привязки ACL).

   Рис. 7-14. Страница ACL Bindings Table (Таблица привязки ACL)



Копирование параметров ACL на другие интерфейсы

1. Откройте страницу **Network Security - ACL Binding** (Безопасность сети - Привязки ACL).
2. Нажмите кнопку **Show All** (Показать все). Откроется страница **ACL Bindings Table** (Таблица привязки ACL).
3. В поле **Copy Parameters from** (Копировать параметры из) выберите порт или группу LAG, откуда необходимо скопировать параметры ACL.
4. В таблице установите флажок **Copy to** (Копировать в) для каждой записи, для которой требуется скопировать параметры.
5. Нажмите кнопку **Apply Changes** (Применить изменения).

Удаление привязок ACL

1. Откройте страницу **Network Security - ACL Binding** (Безопасность сети - Привязки ACL).
2. Нажмите кнопку **Show All** (Показать все). Откроется страница **ACL Bindings Table** (Таблица привязки ACL).
3. В таблице установите флажок **Remove** (Удалить) для каждой привязки, которую требуется удалить.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Настройка привязок ACL с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для настройки привязки ACL.

Команда консоли	**Описание**
service-acl input *имя-acl* no service-acl input	Для управления доступом к интерфейсу используйте команду service-acl в режиме настройки интерфейса. Для удаления функции управления доступом используйте форму no этой команды.
show access-lists [имя]	Используйте команду show access-lists в режиме Privileged EXEC для отображения списков управления доступом (ACL), настроенных на коммутаторе.

Далее приведен пример нескольких команд консоли.

```
Switch# show access-lists

IP access list ACL1

permit 234 172.30.40.1 0.0.0.0 any

permit 234 172.30.8.8 0.0.0.0 any
```

Настройка наблюдения по протоколу DHCP

Наблюдение по протоколу DHCP усиливает безопасность сети, обеспечивая с помощью брандмауэра защиту между серверами DHCP и ненадежными интерфейсами. Благодаря использованию наблюдения по протоколу DHCP сетевые администраторы могут различать доверенные интерфейсы, подключенные к компьютерам конечных пользователей или серверам DHCP и ненадежные интерфейсы, отсутствующие в правилах сетевого брандмауэра.

С помощью наблюдения по протоколу DHCP фильтруются ненадежные сообщения. Наблюдение по протоколу DHCP создает и поддерживает таблицу наблюдения по протоколу DHCP, в которой содержится информация, полученная от ненадежных пакетов. Если пакет поступает с интерфейса, находящегося за пределами сети или отсутствующего в правилах сетевого брандмауэра, такие интерфейсы считаются ненадежными. На доверенные

интерфейсы пакеты поступают только из сети или от сетевого брандмауэра.

В таблице наблюдения по протоколу DHCP отображаются MAC-адрес, IP-адрес, время использования и идентификатор VLAN для ненадежных интерфейсов, а также информация об интерфейсах.

Раздел протокола DHCP включает следующие темы.

- Определение свойств для наблюдения по протоколу DHCP.
- Определение в сетях VLAN наблюдения по протоколу DHCP.
- Определение доверенных интерфейсов.
- Добавление интерфейсов в базу данных для наблюдения по протоколу DHCP.

В этом разделе имеются следующие тематические подразделы:

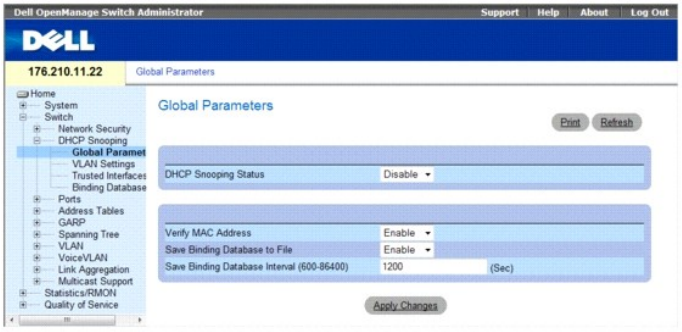
- Определение общих параметров для наблюдения по протоколу DHCP
- Определение в сетях VLAN наблюдения по протоколу DHCP.
- Определение доверенных интерфейсов.
- Добавление интерфейсов в базу данных для наблюдения по протоколу DHCP.

Определение общих параметров для наблюдения по протоколу DHCP

На странице **DHCP Snooping Global Parameters** (Общие параметры для наблюдения по протоколу DHCP) содержатся параметры для включения и настройки наблюдения по протоколу DHCP на устройстве.

Чтобы определить общие параметры для наблюдения по протоколу DHCP, выберите **Switch** (Коммутатор)→ **DHCP Snooping** (Наблюдение по протоколу DHCP)→ **Global Parameters** (Общие параметры).

Рис. 7-15. Страница Global Parameters (Общие параметры)



- **DHCP Snooping Status (Состояние наблюдения по протоколу DHCP)**. Обозначает, включено ли наблюдение по протоколу DHCP на устройстве. Возможные значения:
  - **Enable (Включено)**. Включает наблюдение по протоколу DHCP на устройстве.
  - **Disable (Выключено)**. Выключает наблюдение по протоколу DHCP на устройстве. Это значение по умолчанию.
- **Verify MAC Address (Проверить MAC-адреса)**. Обозначает, выполнена ли проверка MAC-адресов. Возможные значения:
  - **Enable (Включено)**. Выполняется проверка на соответствие исходного MAC-адреса ненадежного порта MAC-адресу клиента.
  - **Disable (Выключено)**. Отключает проверку на соответствие исходного MAC-адреса ненадежного порта MAC-адресу клиента. Это значение по умолчанию.
- **Save Binding Database to File (Сохранить базу данных привязки в файл)**. Указывает способ сохранения базы данных для наблюдения по протоколу DHCP, а именно сохранение в файл. Возможные значения:
  - **Enable (Включено)**. Сохранение базы данных в файл. Это значение по умолчанию.
  - **Disable (Выключено)**. Выключено сохранение базы данных в файл.
- **Save Binding Database Internal (Сохранить базу данных привязки внутри)**. Обозначает, как часто обновляется база данных для наблюдения по протоколу DHCP. Возможные значения поля: 600 - 86400 секунд. Значение по умолчанию: 1200 секунд.

Настройка общих параметров для наблюдения по протоколу DHCP с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для настройки общих параметров для наблюдения по протоколу DHCP.

Команда консоли	Описание
ip dhcp snooping	Команда настройки общих параметров ip dhcp snooping используется для глобального включения наблюдения

no ip dhcp snooping	по протоколу DHCP. Чтобы восстановить значение по умолчанию, используйте форму no этой команды.
ip dhcp snooping verify no ip dhcp snooping verify	Команда настройки общих параметров ip dhcp используется для того, чтобы настроить коммутатор, который будет проверять на ненадежном порте соответствие исходного MAC-адреса в пакете DHCP с адресом оборудования клиента. Чтобы настроить коммутатор на отмену проверки MAC-адресов, используйте форму no этой команды.
ip dhcp snooping database no ip dhcp snooping database	Команда настройки общих параметров ip dhcp snooping database используется для настройки файла привязки для наблюдения по протоколу DHCP. Чтобы удалить файл привязки, используйте форму no этой команды.
ip dhcp snooping database update-freq *секунды* no ip dhcp snooping database update-freq	Команда настройки общих параметров ip dhcp snooping database update-freq используется для настройки частоты обновления файла привязки для наблюдения по протоколу DHCP. Для возврата к значениям по умолчанию используйте форму no этой команды
show ip dhcp snooping [ethernet *интерфейс* | port-channel *номер_порта_канала*]	В режиме EXEC с помощью команды show ip dhcp snooping отображается конфигурация наблюдения по протоколу DHCP.

Далее приведен пример нескольких команд консоли.

```
Console# show ip dhcp snooping


DHCP snooping is enabled

DHCP snooping is configured on following VLANs: 2, 7-18

DHCP snooping database: enabled

Option 82 on untrusted port is allowed

Verification of hwaddr field is enabled (Проверка поля адреса апп. об.включена)
```

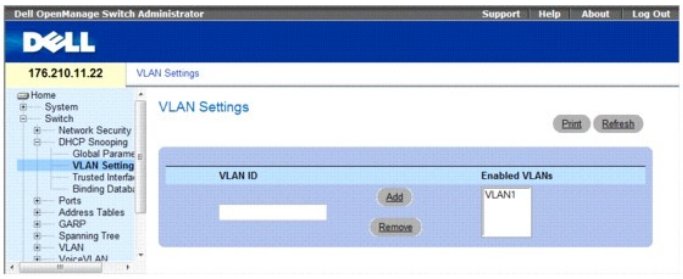
	Interface	Trusted			
	----------	----------			
	1/1	yes			
	1/2	yes			

Определение в сетях VLAN наблюдения по протоколу DHCP

С помощью страницы **DHCP Snooping VLAN Settings** (Параметры VLAN для наблюдения по протоколу DHCP) администраторы сети могут включать в сетях VLAN наблюдение по протоколу DHCP. Наблюдение по протоколу DHCP разделяет порты в сети VLAN. Чтобы включить наблюдение по протоколу DHCP в сети VLAN, убедитесь, что наблюдение по протоколу DHCP включено на устройстве. Для включения наблюдения по протоколу DHCP в сетях VLAN:

Чтобы определить в сетях VLAN наблюдение по протоколу DHCP, выберите **Switch** (Коммутатор)→ **DHCP Snooping** (Наблюдение по протоколу DHCP)→ **VLAN Settings** (Параметры VLAN).

Рис. 7-16. Страница VLAN Settings (Параметры VLAN)



- **VLAN ID (Идентификатор VLAN)**. Сеть VLAN, для которой можно включить наблюдение по протоколу DHCP.
- **Enabled VLANs (Включенные сети VLAN)**. Список сетей VLAN, для которых включено наблюдение по протоколу DHCP.

Определение в сетях VLAN наблюдения по протоколу DHCP

1. Откройте страницу DHCP Snooping VLAN Settings (Параметры VLAN для наблюдения по протоколу DHCP).

2. Выберите **Add** (Добавить) или **Remove** (Удалить), чтобы добавить или удалить идентификаторы сети VLAN из списка включенных сетей VLAN.

3. Нажмите кнопку **Apply Changes** (Применить изменения).

Настройка в сетях VLAN наблюдения по протоколу DHCP с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для настройки в сетях VLAN наблюдения по протоколу DHCP.

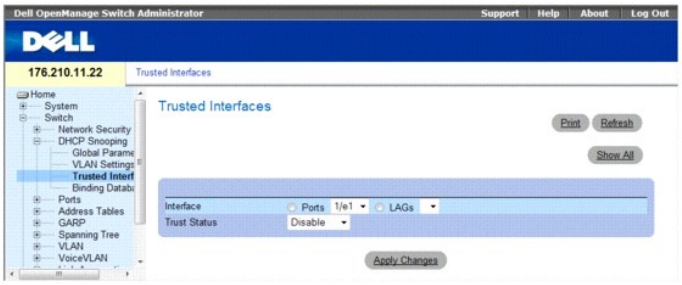
Команда консоли	Описание
ip dhcp snooping vlan *идентификатор_vlan* no ip dhcp snooping *идентификатор_vlan*	Команда настройки общих параметров ip dhcp snooping vlan используется для включения наблюдения по протоколу DHCP в сети VLAN. Чтобы отключить наблюдение по протоколу DHCP в сети VLAN, используйте форму no этой команды.

Определение доверенных интерфейсов

С помощью страницы **Trusted Interfaces** (Доверенные интерфейсы) администраторы сети могут определить доверенные интерфейсы. Если пакет поступает с интерфейса, находящегося за пределами сети или отсутствующего в правилах сетевого брандмауэра, такие интерфейсы считаются ненадежными. На доверенные интерфейсы пакеты поступают только из сети или от сетевого брандмауэра.

Чтобы определить доверенные интерфейсы, выберите **Switch** (Коммутатор)→ **DHCP Snooping** (Наблюдение по протоколу DHCP)→ **Trusted Interface** (Доверенный интерфейс)

Рис. 7-17. Страница Trusted Interfaces (Доверенные интерфейсы)



- **Interface (Интерфейс)**. Обозначает порт или группу LAG, для которой включен режим доверия при использовании наблюдения по протоколу DHCP.
- **Trust Status (Статус доверия)**. Обозначает, включен ли режим доверия для порта или группы LAG при использовании наблюдения по протоколу DHCP. Возможные значения:
  - **Enable (Включить)**. Указывает, что режим доверия для порта или группы LAG при наблюдении по протоколу DHCP включен.
  - **Disable (Отключить)**. Указывает, что режим доверия для порта или группы LAG при наблюдении по протоколу DHCP отключен.

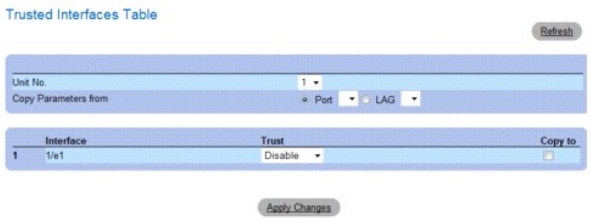
Отображение таблицы доверенных интерфейсов:

1. Откройте страницу **Trusted Interfaces** (Доверенные интерфейсы).

2. Нажмите кнопку **Show All** (Показать все).

   Отобразится таблица Trusted Interfaces (Таблица доверенных интерфейсов).

Рис. 7-18. Таблица доверенных интерфейсов



Копирование параметров доверенных интерфейсов на другие интерфейсы

1. Откройте страницу **Trusted Interfaces** (Доверенные интерфейсы).
2. Нажмите кнопку **Show All** (Показать все). Отобразится таблица **Trusted Interfaces Table** (Таблица доверенных интерфейсов).
3. В полях **Unit** (Устройство) и **Copy from** (Копировать из) выберите порт или группу LAG, откуда необходимо скопировать параметры.
4. В таблице установите флажок **Copy to** (Копировать в) для каждой записи, для которой требуется скопировать параметры.
5. Нажмите кнопку **Apply Changes** (Применить изменения).

Назначение доверенных и ненадежных интерфейсов

1. Откройте страницу **Trusted Interfaces** (Доверенные интерфейсы).
2. Нажмите кнопку **Show All** (Показать все). Отобразится таблица **Trusted Interfaces Table** (Таблица доверенных интерфейсов).
3. В столбце **Trust** (Доверие) включите или отключите режим доверия для интерфейса.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Настройка наблюдения по протоколу DHCP для доверенных интерфейсов с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для настройки наблюдения по протоколу DHCP для доверенных интерфейсов.

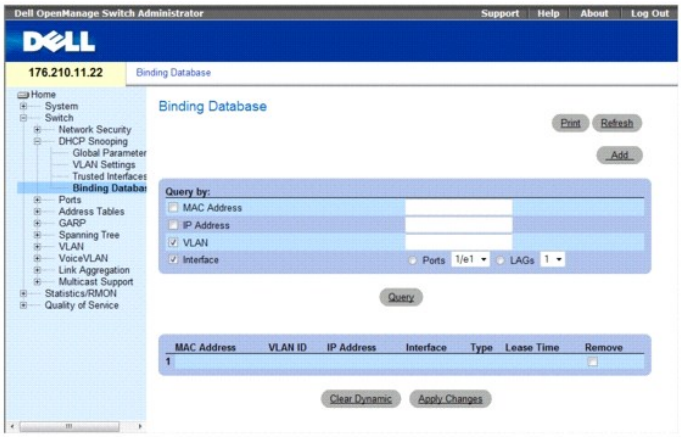
Команда консоли	**Описание**
ip dhcp snooping trust **no ip dhcp snooping trust**	Команда настройки доверия для интерфейса ip dhcp snooping trust используется для включения режима доверия для порта при наблюдении по протоколу DHCP. Чтобы восстановить значение по умолчанию, используйте форму по этой команды.

Добавление интерфейсов в базу данных для наблюдения по протоколу DHCP

На странице **DHCP Snooping Binding Database** (База данных привязки для наблюдения по протоколу DHCP) содержатся параметры для запроса и добавления IP-адресов в базу данных для наблюдения по протоколу DHCP.

Чтобы открыть страницу включения в базу данных, выберите **Switch** (Коммутатор)→ **DHCP Snooping** (Наблюдение по протоколу DHCP)→ **Binding Database** (База данных привязки)

Рис. 7-19. Страница Binding Database (База данных привязки)



Выполнение запроса к базе данных

1. Откройте страницу **Binding Database** (База данных привязки).
2. Выберите следующие категории:
   - **MAC Address (MAC-адрес)**. MAC-адреса, включенные в базу данных для наблюдения по протоколу DHCP.
   - **IP Address (IP-адрес)**. IP-адреса, включенные в базу данных для наблюдения по протоколу DHCP.
   - **VLAN (Сеть VLAN)**. Сети VLAN, включенные в базу данных наблюдения по протоколу DHCP.
   - **Interface (Интерфейс)**. Список интерфейсов, включенных в базу данных для наблюдения по протоколу DHCP. Возможные значения: Port (Порт) и LAG (Группа LAG).

   Кроме перечисленных выше полей, в таблице результатов запроса отображаются следующие поля:

   - **VLAN ID (Идентификатор сети VLAN)**. Идентификатор сети VLAN, с которой связан IP-адрес в базе данных для наблюдения по протоколу DHCP.
   - **Type (Тип)**. Тип назначения IP-адреса. Возможные значения: **Static** (Статический) - IP-адрес назначен статически; **Dynamic** (Динамический) - IP-адрес назначен динамически.
   - **Lease Time (Время использования)**. Время использования. Параметр Lease Time (время использования) указывает период времени, в течение которого запись в базе данных DHCP является активной. Коммутатор игнорирует записи с истекшим временем использования.
3. Нажмите кнопку Query (Запрос).

Удаление записи из базы данных

1. Откройте страницу **Binding Database** (База данных привязки).
2. В таблице установите флажок в столбце **Remove** (Удалить) рядом с нужной записью.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Очистка динамической базы данных

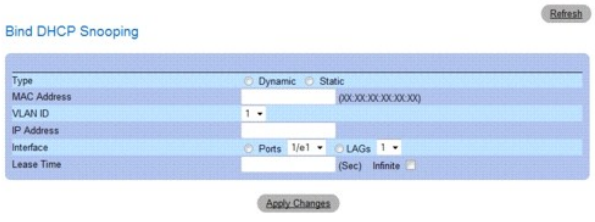
1. Откройте страницу **Binding Database** (База данных привязки).
2. Нажмите кнопку **Clear Dynamic** (Динамическая очистка).

Привязка базы данных для наблюдения по протоколу DHCP

1. Откройте страницу **Binding Database** (База данных привязки).
2. Нажмите кнопку **Add** (Добавить).

   Откроется страница **Bind DHCP Snooping** (Привязка для наблюдения по протоколу DHCP).

   Рис. 7-20. Страница Bind DHCP Snooping (Привязка для наблюдения по протоколу DHCP)



3. Определите поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Настройка базы данных привязки для наблюдения по протоколу DHCP с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для настройки базы данных привязки для наблюдения по протоколу DHCP.

Команда консоли	**Описание**
ip dhcp snooping binding *mac-адрес идентификатор_vlan ip-адрес* {ethernet *интерфейс* | port-channel *номер_порта-канала*} expiry *секунды* **no ip dhcp snooping binding** *mac-адрес идентификатор_vlan*	В режиме экрана Privileged EXEC с помощью команды **ip dhcp snooping binding** выполняется настройка базы данных для наблюдения по протоколу DHCP или добавление в базу данных записей привязки. Чтобы удалить записи из базы данных привязки, используйте форму no этой команды.
clear ip dhcp snooping database	В режиме экрана Privileged EXEC с помощью команды **clear ip dhcp snooping database** можно удалить базу данных привязки для наблюдения по протоколу DHCP.
show ip dhcp snooping binding [mac-address *mac-адрес*] [ip-address *ip-адрес*] [vlan *vlan*] [ethernet *интерфейс* | port-channel *номер_порта-канала*]	В режиме User EXEC помощью команды **show ip dhcp snooping binding** отображается база данных привязки для наблюдения по протоколу DHCP и информации о настройке для всех интерфейсов коммутатора.

Далее приведен пример нескольких команд консоли.

```
Console# show ip dhcp snooping binding

Update frequency: 1200

Total number of binding: 2
```

Mac Address	IP-адрес	Lease (sec)	Type	VLAN	Интерфейс
----------	----------	----------	--------	--------	-------
0060.704C.73FF	10.1.8.1	7983	snooping	3	1/21
0060.704C.7BC1	10.1.8.2	92332	snooping	(s)3	1/22

Настройка портов

На странице **Ports** (Порты) находятся ссылки для настройки работы портов, в том числе таких функций, как контроль «лавины», зеркалирование портов и виртуальное тестирование портов.

Чтобы открыть страницу **Ports** (Порты), выберите **Switch** (Коммутатор)→ **Ports** (Порты).

В этом разделе имеются следующие тематические подразделы:

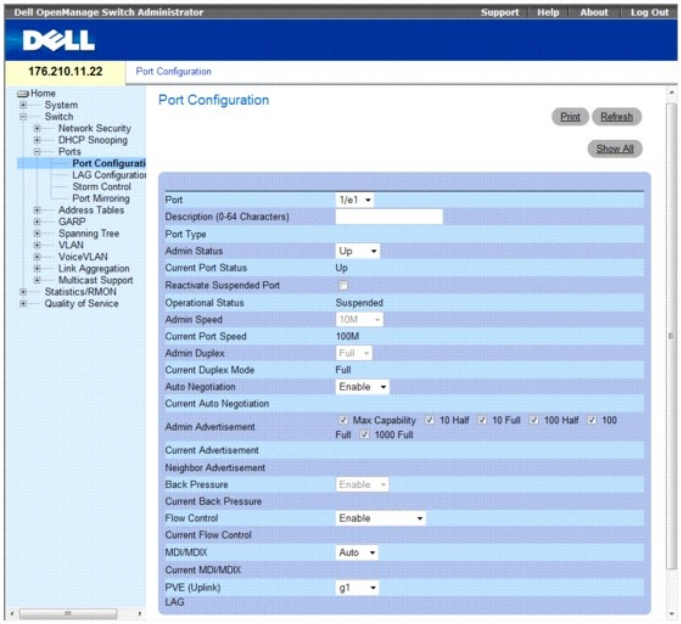
- Определение настройки портов
- Определение параметров LAG
- Включение контроля «лавины»
- Определение сеансов с зеркалированием портов

Определение настройки портов

Используйте страницу Port Configuration (Настройка портов) для определения параметров портов. При изменении конфигурации порта, входящего в группу LAG, изменения вступают в силу только после удаления порта из этой группы.

Чтобы открыть страницу Port Configuration (Настройка портов), выберите Switch (Коммутатор)→ **Ports** (Порты)→ **Port Configuration** (Настройка портов) на панели дерева.

Рис. 7-21. Страница Port Configuration (Настройка портов)



Страница Port Configuration (Настройка портов) содержит следующие поля:

- **Port (Порт)**. Номер порта, для которого определяются параметры.
- **Description (Описание) (064 символов)**. Краткое описание интерфейса, например Ethernet.
- **Port Type (Тип порта)**. Тип порта.
- **Admin Status (Состояние администрирования)**. Включает или отключает пересылку трафика через порт.
  - **Up (Включено)**. Пересылка трафика через порт включена.
  - **Down (Выключена)**. Пересылка трафика через порт выключена.
- **Current Port Status (Текущее состояние порта)**. Показывает, в работоспособном ли состоянии находится в настоящий момент порт.
- **Reactivate Suspended Port (Возврат отключенного порта к работе)**. Заново активизирует порт, если он был отключен системой безопасности.
  - **Флажок установлен**. Восстановление порта.
  - **Флажок снят**. Оставляет статус работы порта прежним.
- **Operational Status (Рабочее состояние)**. Показывает рабочее состояние порта. Возможные значения этого поля:

  Suspended (Приостановлен). Порт активен, но в настоящий момент не получает и не передает трафик.

  Active (Включен). Порт активен и получает/передает трафик.

  Disable (Отключен). Порт отключен и в настоящий момент не получает и не передает трафик.

- **Admin Speed (Администрирование скорости)**. Настроенная скорость порта. Тип порта определяет доступные параметры скорости. Значение скорости порта может быть изменено только в том случае, если порт отключен. Возможные значения:
  - **10M**. Порт в настоящий момент работает на скорости 10 Мбит/с.
  - **100M**. Порт в настоящий момент работает на скорости 100 Мбит/с.
  - **1000M**. Порт в настоящий момент работает на скорости 1000 Мбит/с.
- **Current Port Speed (Текущая скорость порта)**. Показывает скорость синхронизации порта (в битах в секунду).
- **Admin Duplex (Администрирование дуплексного режима)**. Скорость порта в дуплексном режиме (в битах в секунду).
  - **Full (Дуплексный)**. Указывает, что интерфейс поддерживает передачу между устройством и клиентом одновременно в обоих направлениях.
  - **Half (Полудуплексный)**. Указывает, что интерфейс поддерживает передачу между устройством и клиентом только в одном направлении в каждый момент времени.
- **Current Duplex Mode** (Дуплексный режим) - показывает дуплексный режим синхронизации порта.
- **Auto Negotiation (Автоматическое согласование)**. Это протокол между двумя партнерами по связи, который позволяет группе LAG оповестить партнера канала связи о своей скорости передачи, возможности работы в дуплексном режиме и управлении потоком (управление потоком по умолчанию выключено).
  - **Enable (Включено)**. Включает автоматическое согласование для порта.
  - **Disable (Выключено)**. Выключает автоматическое согласование для порта.
- **Current Auto Negotiation** (Текущее автоматическое согласование) - показывает текущую настройку автоматического согласования.

- **Admin Advertisement (Объявления администрированеия)**. Определяет автоматическое согласование при выводе объявления порта. Возможные значения:
  - **Max Capability (Максимальная производительность)**. Указывает все параметры скорости портов и дуплексного режима, которые можно использовать.
  - **10 Half (10 полудуплексный)**. Указывает, что порт объявляет параметры скорости 10 Мбит/с и полудуплексного режима.
  - **10 Full (10 дуплексный)**. Указывает, что порт объявляет параметры скорости 10 Мбит/с и полного дуплексного режима.
  - **100 Half (100 полудуплексный)**. Указывает, что порт объявляет параметры скорости 100 Мбит/с и полудуплексного режима.
  - **100 Full (100 дуплексный)**. Указывает, что порт объявляет параметры скорости 100 Мбит/с и полного дуплексного режима.
  - **1000 Full (1000 дуплексный)**. Указывает, что порт объявляет параметры скорости 1000 Мбит/с и полного дуплексного режима.
- **Current Advertisement (Текущее объявление)**. Порт объявляет скорость соседнему порту для начала согласования. Возможные значения полей указаны в поле Admin Advertisement (Объявление администрирования).
- **Neighbor Advertisement (Объявление соседнего порта)**. Объявляемые параметры соседнего порта. Значения этого поля совпадают со значениями поля Admin Advertisement (Объявление администрирования).
- Режим обратного давления используется с полудуплексным режимом, чтобы отключить получение сообщений на порты. Функция обратного давления не поддерживается для портов OOB.
  - **Enable (Включено)**. Включает режим обратного давления для порта.
  - **Disable (Выключено)**. Выключает режим обратного давления для порта.
- **Current Back Pressure** (Текущий режим обратного давления) - текущая настройка режима обратного давления.
- **Flow Control (Управление потоком)**. Определяет состояние управления потоком.
  - **Enable (включено)**. Включает управление потоком для порта.
  - **Disable (Выключено)**. Выключает управление потоком для порта.
  - **Auto-negotiation (Автоматическое определение)**. Включает автоматическое согласование управления потоком для порта.
- **Current Flow Control** (Текущее управление потоком) - текущая настройка управления потоком.
- **MDI/MDIX** - позволяет устройству определять, какой используется кабель - перекрестный и неперекрестный. В концентраторах и коммутаторах специально используется противоположная схема подключения проводов, чем на конечных станциях. Поэтому при подключении концентратора или коммутатора к конечной станции можно использовать соединение напрямую кабелем Ethernet, так как провода совпадают. При соединении между собой двух концентраторов/коммутаторов или двух конечных станций используют перекрестный кабель, который соединяет правильные пары. Функция автоматического выбора MDIX не работает на портах FE, если автоматическое согласование отключено. Возможные значения:
  - **Auto (Авто)**. Используется для автоматического определения типа кабеля.
  - **MDIX**. Кабель, используемый для концентраторов и коммутаторов.
  - **MDI**. Кабель, используемый для конечных станций.
- **Current MDI/MDIX (Текущий MDI/MDIX)**. Указывает текущие настройки устройства MDIX. Возможные значения:
  - **MDI** - для параметра MDI установлено значение MDI.
  - **MDIX** - для параметра MDI установлено значение MDIX.
- **Private VLAN Edge (PVE)**. Указывает группу (PVE) для которой необходимо настроить LAG. Порт, назначенный как PVE защищается линией связи с центральным узлом и, таким образом, изолируется от других портов той же сети VLAN. Такой линией связи должен быть порт GE.
- **LAG**. Показывает, что порт входит в группу LAG.

При изменении конфигурации порта, входящего в группу LAG, изменения вступают в силу только после удаления порта из этой группы.

Определение параметров порта

1. Откройте страницу **Port Configuration** (Настройка портов).
2. Выберите порт в поле **Port** (Порт).
3. Заполните доступные поля в диалоговом окне.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

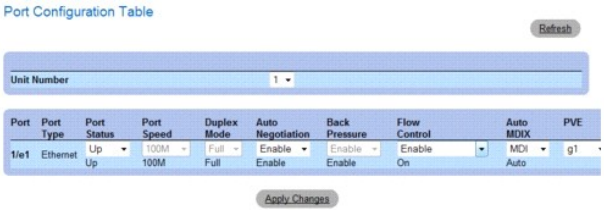
   Параметры порта будут сохранены для этого устройства.

Отображение и изменение настроек портов

1. Откройте страницу **Port Configuration** (Настройка портов).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **Ports Configuration Table** (Таблица настройки портов).

Рис. 7-22. Страница Ports Configuration Table (Таблица настройки портов)



3. Заполните имеющиеся поля для нужных портов.

4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Параметры порта будут сохранены для этого устройства.

Настройка портов с помощью команд консоли

В следующей таблице приведены команды консоли для настройки портов, как показано на странице **Port Configuration** (Настройка портов).

Табл. 7-12. Команды консоли для настройки портов

Команда консоли	**Описание**
interface ethernet *интерфейс*	Включает режим настройки интерфейса для настройки типа интерфейса Ethernet.
description *строка*	Добавляет описание в конфигурацию интерфейса.
shutdown	Выключает интерфейсы, которые входят в состав текущего заданного контекста.
set interface active {**ethernet** *интерфейс* | **port-channel** *номер_канала_порта}*	Вновь активизирует интерфейс, отключенный по причинам безопасности.
speed *Мбит/с*	Настраивает скорость заданного интерфейса Ethernet, если не используется автоматическое согласование.
duplex {half | full}	Настраивает дуплексный или полудуплексный режим для заданного интерфейса Ethernet, если не используется автоматическое согласование.
negotiation [capability1 [capability2...capability5]	Включает автоматическое согласование для параметров скорости и дуплексного режима данного интерфейса.
back-pressure	Включает режим обратного давления для заданного интерфейса.
flowcontrol {auto | on | off}	Настраивает управление потоком для заданного интерфейса.
mdix {on | auto}	Включает автоматическое использование перекрестного кабеля для заданного интерфейса или канала порта.
show interfaces configuration [**ethernet *интерфейс* |port-channel *номер_порта-канала***]	Отображает конфигурацию для всех настроенных интерфейсов.
show interface advertise	Отображает установки объявлений согласования интерфейса.
show interfaces status [**ethernet *интерфейс* | port-channel *номер_порта-канала***]	Отображает состояние для всех настроенных интерфейсов.
show interfaces description [**ethernet** *интерфейс* **| port-channel** *номер_порта-канала*]	Отображает описание для всех настроенных интерфейсов.

Далее приведен пример команд консоли.

```
console(config)# interface ethernet 1/e3

console(config-if)# description «RD SW#3»

console(config-if)# shutdown

console(config-if)# no shutdown

console(config-if)# speed 100

console(config-if)# duplex full

console(config-if)# negotiation

console(config-if)# back-pressure
```

```
console(config-if)# flowcontrol on

console(config-if)# mdix auto

console(config-if)# end

console# show interfaces configuration ethernet 1/e3
```

Port	Type	Duplex	Speed	Neg	Flow Control	Admin State	Back Pressure	Mdix Mode
----	-----	------	------	----	------	-----	------	----
1/e3	100	Full	100	Enabled	On	Up	Enable	Auto

Console# **show interfaces status**

Port	Type	Duplex	Speed	Neg	Flow Control	Link State	Back Pressure	MdixMode
----	-----	------	------	----	------	-----	------	----
1/e3	100	Full	100	Auto	On	Up	Enable	On
1/e4	100	Full	1000	Off	Off	Up	Disable	On

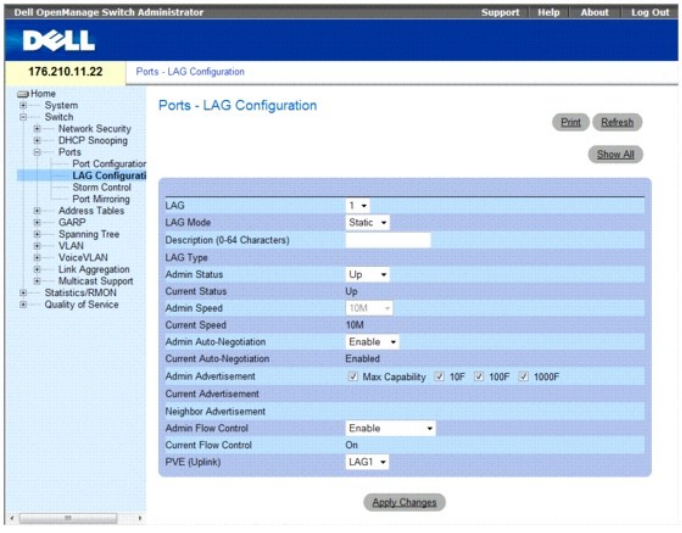
Ch	Type	Duplex	Speed	Neg	Flow Control	Back Pressure	Link State	
---	----	------	-----	-----	-------	--------	------	
ch1	1000	Full	1000	Off	Off	Disable	Up	

Определение параметров LAG

Страница Ports - LAG Configuration (Порты - настройка LAG) содержит поля, позволяющие определить параметры настройки LAG. Устройство поддерживает до 15 групп LAG для каждой системы. Дополнительную информацию об объединенных группах каналов (LAG) и назначении портов в группы LAG см. в разделе Объединение портов.

Чтобы открыть страницу Ports - LAG Configuration (Порты - настройка LAG), выберите **Switch** (Коммутатор)→ **Ports** (Порты)→ **LAG Configuration** (Настройка LAG) на панели дерева.

Рис. 7-23. Порты - настройка LAG



Страница Ports - LAG Configuration (Порты - настройка LAG) содержит следующие поля:

- **LAG** - номер группы LAG.
- **LAG Mode (Режим LAG)**. Тип LAG. Возможные значения:
  - **Static (Статический)**. Порты составляют единый логический порт для высокоскоростного соединения между сетевыми устройствами.
  - **LACP**. Link Aggregate Control Protocol (Протокол объединения связей). Группы LAG с протоколом LACP могут обмениваться информацией с

другими связями, чтобы автоматически обмениваться информацией с другими связями для автоматического обновления и поддержки настроек LAG.

- **Description (064 Characters) (Описание (0-64 символов))**. Описание группы LAG, задаваемое пользователем.
- **LAG Type (Тип LAG)**. Типы портов, входящих в состав LAG.
- **Admin Status (Состояние администрирования)**. Включает или выключает выбранную группу LAG.
  - **Up (Включено)**. Пересылка трафика через LAG включена.
  - **Down (Выключена)**. Пересылка трафика через LAG выключена.
- **Current Status** (Текущее состояние) - показывает, работает ли в данный момент группа LAG.
- **Admin Speed** (Администрирование скорости) - скорость, на которой работает LAG. Возможные значения:
  - **10M**. Показывает, что LAG в настоящее время работает на скорости 10 Мбит/с.
  - **100M**. Показывает, что LAG в настоящее время работает на скорости 100 Мбит/с.
  - **1000M**. Показывает, что LAG в настоящее время работает на скорости 1000 Мбит/с.
- **Current LAG Speed** (Текущая скорость группы LAG) - текущая скорость, на которой работает LAG.
- **Auto Negotiation (Автоматическое согласование)**. Это протокол между двумя партнерами по связи, который позволяет группе LAG оповестить партнера канала связи о своей скорости передачи, возможности работы в дуплексном режиме и управлении потоком.
  - **Enable (Включено)**. Включает автоматическое согласование для LAG.
  - **Disable (Выключено)**. Выключает автоматическое согласование для LAG.
- **Current Auto Negotiation** (Текущее автоматическое согласование) - показывает текущую настройку автоматического согласования.
- **Admin Advertisement (Объявления администрированеия)**. Определяет автоматическое согласование при выводе объявления группы LAG. Возможные значения:
  - **Max Capability (Максимальная производительность)**. Указывает все параметры скорости группы LAG и дуплексного режима, которые можно использовать.
  - **10 Full (10 дуплексный)**. Указывает, что группа LAG объявляет параметры скорости 10 Мбит/с и полного дуплексного режима.
  - **100 Full (100 дуплексный)**. Указывает, что группа LAG объявляет параметры скорости 100 Мбит/с и полного дуплексного режима.
  - **1000 Full (1000 дуплексный)**. Указывает, что группа LAG объявляет параметры скорости 1000 Мбит/с и полного дуплексного режима.
- **Current Advertisement (Текущее объявление)**. Группа LAG объявляет скорость соседнему порту для начала согласования. Возможные значения полей указаны в поле Admin Advertisement (Объявление администрирования).
- **Neighbor Advertisement (Объявление соседней группы)**. Объявляемые параметры соседней группы LAG. Значения этого поля совпадают со значениями поля Admin Advertisement (Объявление администрирования).
- **Admin Flow Control (Управление потоком)**. Определяет состояние управления потоком группы LAG. Режим управления потоком поддерживается, если порты в группе LAG работают в дуплексном режиме.
  - **Enable (Включено)**. Включает управление потоком для группы LAG.
  - **Disable (Выключено)**. Выключает управление потоком для группы LAG.
  - **Auto-negotiation (Автоматическое согласование)**. Включает автоматическое согласование управления потоком для группы LAG.
- **Current Flow Control (Текущее управление потоком)**. Текущая настройка управления потоком.
- **Private VLAN Edge (PVE)**. Указывает группу (PVE) для которой необходимо настроить LAG. Порт, назначенный как PVE защищается линией связи с центральным узлом и, таким образом, изолируется от других портов той же сети VLAN. Такой линией связи должен быть порт GE или LAG.

Определение параметров LAG

1. Откройте страницу Ports - LAG Configuration (Порты - настройка LAG).
2. Выберите группу LAG в поле **LAG**.
3. Определите поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Параметры группы LAG будут сохранены для этого устройства.

Изменение параметров группы LAG

1. Откройте страницу Ports - LAG Configuration (Порты - настройка LAG).
2. Выберите группу LAG в поле **LAG**.
3. Измените поля.

4. Нажмите кнопку **Apply Changes** (Применить изменения).

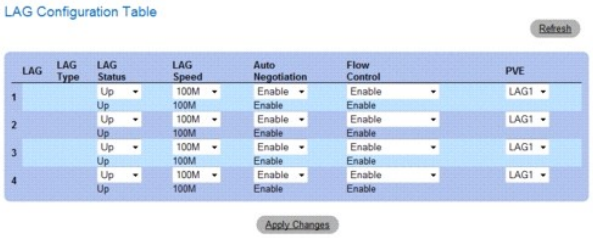
   Параметры группы LAG будут сохранены для этого устройства.

Отображение и изменение настроек группы LAG

1. Откройте страницу Ports - LAG Configuration (Порты - настройка LAG).
2. Нажмите кнопку **Show All (Показать все).**

   Откроется страница LAG Configuration Table (Таблица настройки LAG) .

   Рис. 7-24. Страница LAG Configuration Table (Таблица настройки LAG)



3. Заполните имеющиеся поля для нужных групп LAG.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Параметры группы LAG будут сохранены для этого устройства.

Настройка групп LAG с помощью команд консоли

В следующей таблице приведены команды консоли для настройки групп LAG, как показано на странице **Ports - LAG Configuration** (Порты - настройка LAG).

Таблица 7-13. Команды консоли для настройки LAG

Команда консоли	**Описание**
interface port-channel *номер_канала_порта*	Включает режим настройки интерфейса для указанного канала-порта.
description *строка*	Добавляет описание в конфигурацию интерфейса.
shutdown	Выключает интерфейсы, которые входят в состав текущего заданного контекста.
speed *бит/с*	Настраивает скорость заданного интерфейса Ethernet, если не используется автоматическое согласование.
negotiation [capability1 [capability2...capability5]	Включает автоматическое согласование скорости интерфейса.
back-pressure	Включает режим обратного давления для заданного интерфейса.
flowcontrol {auto | on | off}	Настраивает управление потоком для заданного интерфейса.
show interfaces configuration [**ethernet** *интерфейс*| **port-channel** *номер_порта-канала*]	Отображает конфигурацию для всех настроенных интерфейсов.
show interfaces status [**ethernet** *интерфейс* |**port-channel** *номер_порта-канала*]	Отображает состояние для всех настроенных интерфейсов.
show interfaces description [**ethernet** *интерфейс* |**port-channel** *номер_порта-канала*]	Отображает описание для всех настроенных интерфейсов.
show interfaces port-channel [*номер_канала_порта]*	Выводит сведения о канале порта (какие порты входят в канал порта, активны они на данный момент или нет).

Далее приведен пример команд консоли.

```
console(config)# interface port-channel 2

console(config-if)# no negotiation

console(config-if)# speed 100

console(config-if)# flowcontrol on
```

```
console(config-if)# exit

console(config)# interface port-channel 3

console(config-if)# shutdown

console(config-if)# exit

console(config)# interface port-channel 4

console(config-if)# back-pressure

console(config-if)# description p4

console(config-if)# end

console# show interfaces port-channel
```

Channel	Ports
---------	---------
ch1	Inactive: 1/e(11-13)
ch2	Active: 1/e14

Включение контроля «лавины»

Широковещательная «лавина» - это результат чрезмерного количества широковещательных сообщений, одновременно передаваемых по сети через один порт. Ответы на пересылаемые сообщения являются причиной чрезмерной нагрузки на сеть, перегружая ее ресурсы или вызывая задержки в сети.

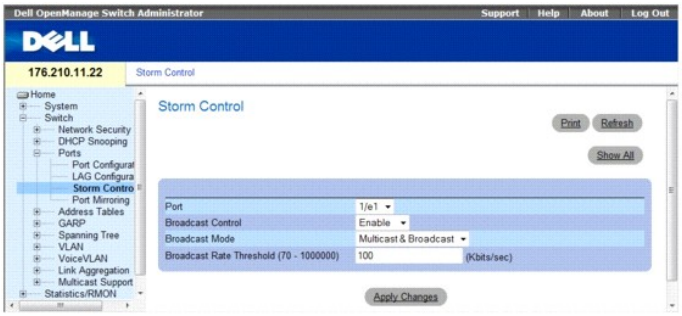
Контроль «лавины» включается для каждого порта путем определения типа пакета и скорости передачи пакетов.

Система измеряет скорость входящих кадров одноадресной, широковещательной и многоадресной передачи отдельно для каждого порта и отбрасывает кадры, если скорость превышает значение, указанное пользователем.

Страница Storm Control (Контроль «лавины») содержит поля для включения и настройки контроля «лавины».

Чтобы открыть страницу Storm Control (Контроль «лавины»), выберите **Switch**→ (Коммутатор) **Ports**→ (Порты) **Storm Control** (Контроль «лавины») на панели дерева.

Рис. 7-25. Страница Storm Control (Контроль «лавины»)



Страница Storm Control (Контроль «лавины») содержит следующие поля:

- **Port (Порт)**. Порт, для которого включен контроль «лавины».
- **Broadcast Control (Управление широковещательными передачами)**. Включает или отключает пересылку пакетов широковещательного типа на указанный интерфейс.
  - ***Enable (Включено)***. Включает пересылку пакетов широковещательного типа.
  - ***Disable (Выключено)***. Выключает пересылку пакетов широковещательного типа.
- **Broadcast Mode (Режим широковещательной передачи)**. Указывает режим широковещательной передачи, который в настоящее время включен для устройства или стека. Возможные значения:
  - **Multicast & Broadcast (Многоадресный и широковещательный трафик)**. Выполняет подсчет широковещательного и многоадресного трафика одновременно.
  - **Broadcast Only (Только широковещательный трафик)**. Выполняет подсчет только широковещательного трафика.
- **Broadcast Rate Threshold (70-1000000) (Порог скорости широковещательных пакетов)**. Максимальная скорость (в пакетах в секунду), при которой пересылаются неизвестные пакеты. Возможные значения поля: 70-1000000.

Включение контроля «лавины»

1. Откройте страницу Storm Control (Контроль «лавины»).
2. Выберите интерфейс, для которого хотите реализовать контроль «лавины».
3. Определите поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Функция контроля «лавины» будет включена.

Изменение параметров контроля «лавины» порта

1. Откройте страницу Storm Control (Контроль «лавины»).
2. Измените поля.
3. Нажмите кнопку **Apply Changes**

   (Применить изменения)

   Параметры контроля «лавины» порта будут сохранены для этого устройства.

Отображение таблицы параметров порта

1. Откройте страницу Storm Control (Контроль «лавины»).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница Storm Control Settings Table (Таблица параметров контроля «лавины»).

   Рис. 7-26. Таблица Storm Control Settings Table (Таблица параметров контроля «лавины»)

Помимо полей, имеющихся на странице Storm Control (Контроль «лавины»), таблица Storm Control Settings Table (Таблица параметров контроля «лавины») содержит следующие поля:

- **Unit No. (Номер устройства)**. Указывает номер устройства, для которого отображается информация о контроле «лавины».
- **Copy Parameters from Port (Копировать параметры из)**. Указывает порт, из которого нужно скопировать параметры контроля «лавины».
- **Copy To (Копировать в)**. Копирование параметров контроля «лавины» на выбранные порты.

Копирование параметров в таблицу параметров контроля «лавины»

1. Откройте страницу Storm Control (Контроль «лавины»).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница Storm Control Settings Table (Таблица параметров контроля «лавины»).

3. В поле Copy Parameters from Port (Копировать параметры из порта) выберите порт, из которого необходимо скопировать параметры.
4. Установите флажок Copy to (Копировать в), чтобы определить интерфейсы, в которые будут скопированы параметры контроля «лавины», или нажмите кнопку Select All (Выбрать все) для копирования определений во все порты.

5. Нажмите кнопку **Apply Changes** (Применить изменения).

   Параметры будут скопированы в выбранные порты в **Storm Control Settings Table** (Таблице параметров контроля «лавины»), а устройство обновлено.

Настройка контроля «лавины» с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для настройки контроля «лавины», как показано на странице **Storm Control** (Контроль «лавины»).

Таблица 7-14. Команды консоли для настройки контроля «лавины»

Команда консоли	Описание
`port storm-control include-multicast`	Позволяет устройству подсчитывать многоадресные пакеты вместе с одноадресными и широковещательными пакетами.
`port storm-control broadcast enable`	Включает контроль широковещательной «лавины».
`port storm-control broadcast rate`	Настраивает максимальную скорость для широковещательных пакетов.
`show ports storm-control port`	Отображает конфигурацию контроля «лавины».

Далее приведен пример команд консоли.

```
console(config)# port storm-control include-multicast

console(config)# interface ethernet 1/e1

console(config-if)# port storm-control broadcast enable

console(config-if)# port storm-control broadcast rate 100000

console(config-if)# end

console# show ports storm-control
```

Port	Broadcast Storm control [kbyes/sec]
-----	----------
1/e1	8000
2/e1	Disabled
3/e2	Disabled

Определение сеансов с зеркалированием портов

Зеркалирование порта делает следующее:

- Контролирует и дублирует сетевой трафик путем пересылки копий входящих и исходящих пакетов с одного порта на другой (контролирующий).
- Зеркалирование портов можно использовать как средство диагностики и/или отладки.
- Обеспечивает нормальную работу и мониторинг устройства.

При настройке зеркалирования портов, выбирается определенный порт для копирования всех пакетов и разные порты, с которых копируются пакеты.

Перед настройкой зеркалирования портов учтите следующее.

- Зеркалирование портов контролирует и дублирует сетевой трафик путем пересылки копий входящих и исходящих пакетов с контролируемого порта на контролирующий порт.
- Контролируемые порты не могут работать быстрее, чем контролирующие.
- Все пакеты RX/TX должны контролироваться на одном порте.

К портам, настроенным как порты назначения, применяются следующие ограничения.

- *Порты нельзя настроить в качестве портов-источников.*
- *Порты не могут входить в группу LAG.*
- *Для этого порта не настроены интерфейсы IP.*

- *Для этого порта не включен протокол GVRP.*
- *Порт не входит в сеть VLAN.*
- Можно определить только один порт назначения.

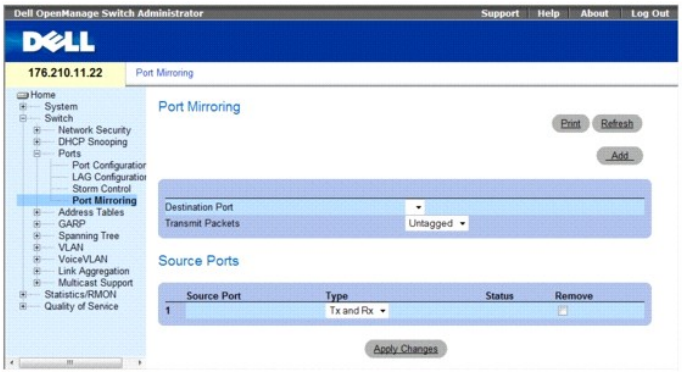
К портам, настроенным как порты-источники, применяются следующие ограничения.

- Порты-источники не могут входить в группу LAG.
- *Порты нельзя настроить в качестве портов назначения.*
- Функция зеркалирования поддерживает до 4 портов на устройстве.

Чтобы открыть страницу Port Mirroring (Зеркалирование портов), выберите **Switch** (Коммутатор)→ **Ports** (Порты)→ **Port Mirroring** (Зеркалирование портов) на панели дерева.

Если порт выбран в качестве порта назначения для сеанса с зеркалированием портов, все обычные операции с ним откладываются. К ним относятся операции Spanning Tree и LACP.

Рис. 7-27. Страница Port Mirroring (Зеркалирование портов)



Страница Port Mirroring (Зеркалирование портов) содержит следующие поля:

- **Destination Port (Порт назначения)**. Определяет номер порта, в который копируется трафик.
- **Transmit Packets (Передача пакетов)**. Определяет, каким образом происходит зеркалирование пакетов. Возможные значения:
  - **Untagged (Без меток)**. Зеркалирует пакеты как непомеченные пакеты VLAN. Это значение по умолчанию.
  - **Tagged (С метками)**. Зеркалирует пакеты как помеченные пакеты VLAN.

Порты-источники

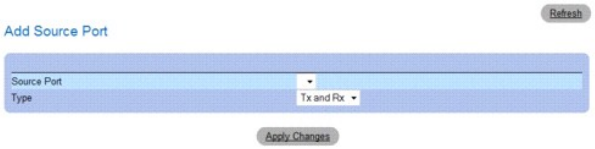
- **Source Port (Порт-источник)**. Определяет номер порта, с которого копируется трафик.
- **Type (Тип)**. Показывает, являются ли зеркалированные порты портами для приема, передачи или бифункциональными портами. Возможные значения:
  - ***RxOnly (Только прием)***. Зеркалирование портов приема. Это значение по умолчанию.
  - ***TxOnly (Только передача)***. Зеркалирование портов передачи.
  - ***Tx and Rx (Прием и передача)***. Зеркалирование портов приема и передачи.
- **Status (Состояние)**. Показывает, выполняется ли в настоящий момент контроль порта (**Active**) или не выполняется (**Ready**).
- **Remove (Удалить)**. Удаление сеанса зеркалирования портов. Возможные значения:
  - **Флажок установлен**. Удаляет текущие сеансы зеркалирования портов.
  - **Флажок снят**. Оставляет сеанс зеркалирования портов.

Добавление сеанса с зеркалирования портов

1. Откройте страницу Port Mirroring (Зеркалирование портов).
2. Нажмите кнопку **Add** (Добавить).

   Откроется страница Add Source Port (Добавление порта-источника).

Рис. 7-28. Добавление порта-источника



3. Определите поля **Source Port (Порт-источник)** и **Type (Тип)**.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Новый порт-источник будет определен, а устройство будет обновлено.

Удаление копии порта из сеанса с зеркалированием портов

1. Откройте страницу Port Mirroring (Зеркалирование портов).
2. В таблице портов-источников, установите флажок в поле **Remove** (Удалить).
3. Нажмите кнопку **Apply Changes** (Применить изменения).

   Выбранный сеанс с зеркалированием портов будет удален, а устройство обновлено.

Настройка сеанса с зеркалированием портов с помощью команд консоли

В следующей таблице приведены команды консоли, соответствующие полям страницы Port Mirroring (Зеркалирование портов) для настройки сеанса с зеркалированием портов.

Табл. 7-15. Команды консоли для настройки сеанса зеркалирования портов

Команда консоли	**Описание**
port monitor *интерфейс_src* [**rx** | **tx**]	Запускает сеанс с зеркалированием портов.

Далее приведен пример команд консоли.

```
Console(config)# interface ethernet 1/e1

console(config-if)# port monitor 1/e2

console(config-if)# end

console# show ports monitor
```

Source Port	Destination Port	Type	Status	VLAN Tagging
----------	----------	----------	-------	----------
1/e2	1/e1	RX, TX	Active	No

Настройка адресных таблиц

MAC-адреса хранятся в базах данных статических или динамических адресов. Пакет, адресованный приемнику, хранящемуся в одной из баз данных, немедленно пересылается на порт. Таблица динамических адресов может быть отсортирована по интерфейсу, группе VLAN и MAC-адресу. MAC-адреса определяются динамически, когда пакеты от источников поступают на устройство. Адреса связываются с портами путем опознавания их по исходному адресу входящих кадров. Кадры, адресованные на MAC-адрес приемника, который не связан ни с каким портом, рассылаются «лавиной» на все порты соответствующей VLAN. Статические адреса настраиваются вручную. Чтобы предотвратить переполнение таблицы связей, динамические MAC-адреса, с которых не наблюдается трафик в течение определенного периода, удаляются.

Чтобы открыть страницу **Address Tables** (Таблицы адресов), выберите **Switch** (Коммутатор)→ **Address Table** (Таблица адресов) на панели дерева.

В этом разделе имеются следующие тематические подразделы:

- Определение статических адресов

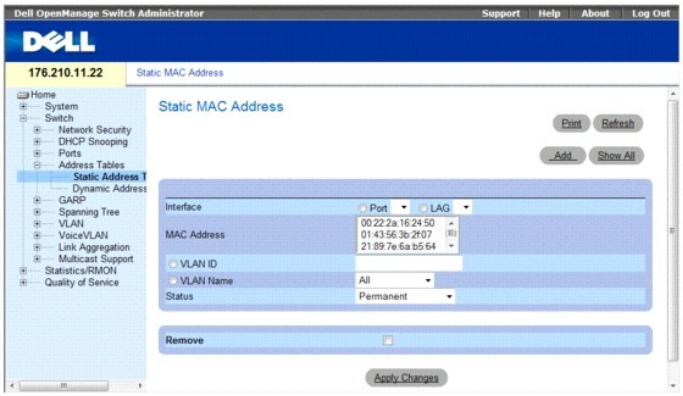
- Просмотр динамических адресов

Определение статических адресов

На странице Static MAC Address (Статический MAC-адрес) приведен список всех статических MAC-адресов. Статические адреса можно добавлять и удалять со страницы Static MAC Address (Таблица статических MAC-адресов). Кроме того, можно определить несколько MAC-адресов для одного порта.

Чтобы открыть страницу Static MAC Address (Статический MAC-адрес), выберите **Switch** (Коммутатор)→ **Address Tables** (Таблицы адресов)→ **Static Address Table** (Таблица статических адресов) на панели дерева.

Рис. 7-29. Страница Static MAC Address (Статические MAC-адреса)



Страница Static MAC Address (Статические MAC-адреса) содержит следующие поля:

- **Interface (Интерфейс)**. Порт или группа LAG, для которых назначены статические MAC-адреса.
- **MAC Address (MAC-адрес)**. MAC-адрес из текущего списка статических адресов.
- **VLAN ID (Идентификатор сети VLAN)**. Идентификатор сети VLAN, связанной с MAC-адресом.
- **VLAN Name (Имя сети VLAN)**. Имя сети VLAN, определяемое пользователем.
- **Status (Состояние)**. Состояние MAC-адреса. Возможные значения:
  - **Secure (Защита)**. Используется для определения статических MAC-адресов для блокированных портов.
  - **Permanent (Постоянный)**. Показывает, что MAC-адрес является постоянным.
  - **Delete on Reset (Удаляется при перезагрузке)**. Показывает, что MAC-адрес удаляется при перезагрузке устройства.
  - **Delete on Timeout (Удалить по истечении времени ожидания)**. Показывает, что MAC-адрес удаляется по истечении времени ожидания.

Чтобы предотвратить удаление статических MAC-адресов при выполнении сброса модуля устройства Ethernet, убедитесь, что порт, связанный с MAC-адресом, заблокирован.

- **Remove (Удалить)**. Когда этот флажок установлен, MAC-адрес удаляется из таблицы статических MAC-адресов. **(Static MAC Address Table)**. Возможные значения:
  - **Флажок установлен**. Удаляет выбранный MAC-адрес.
  - **Флажок снят**. Оставляет выбранный MAC-адрес.

Добавление статического MAC-адреса

1. Откройте страницу Static MAC Address (Статический MAC-адрес).
2. Нажмите кнопку **Add** (Добавить).

   Откроется страница Add Static MAC Address (Добавление статического MAC-адреса).

   Рис. 7-30. Добавление статического MAC-адреса

3. Заполните поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Новый статический адрес будет добавлен в **Static MAC Address Table** (Таблицу статических MAC-адресов), а устройство обновлено.

Изменение статического MAC-адреса в таблице статических адресов

1. Откройте страницу **Static MAC Address** (Статический MAC-адрес).
2. Выберите интерфейс.
3. Измените поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

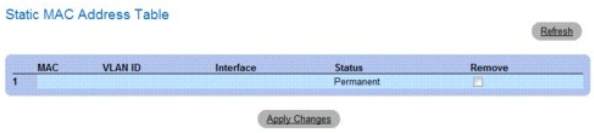
   Статический MAC-адрес будет изменен, а устройство обновлено.

Удаление статического адреса из таблицы статических адресов

1. Откройте страницу **Static MAC Address** (Статический MAC-адрес).
2. Выберите интерфейс.
3. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **Static MAC Address Table** (Таблица статических MAC-адресов).

Рис. 7-31. Таблица статических MAC-адресов



4. Выберите запись таблицы.
5. Установите флажок **Remove** (Удалить).
6. Нажмите кнопку **Apply Changes** (Применить изменения).

   Выбранный статический адрес будет удален, а устройство обновлено.

Настройка параметров статических адресов с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для настройки параметров статических адресов, как показано на странице Static MAC Address (Статический MAC-адрес).

Таблица 7-16. Команды консоли для настройки статических адресов

Команда консоли	Описание
bridge address *mac-адрес* [**permanent** | **delete-on-reset** | **delete-on-timeout** | **secure**] {**ethernet** *interface* | **port-channel** *port-channelномер-канала-порта*}	Добавляет статический MAC-адрес станции-источника в таблицу связей.
show bridge address-table [**vlan** *vlan*] [**ethernet** *interface* | **port-channel** *номер_канала_порта*]	Отображает записи базы данных, содержащей сведения о пересылке данных через мосты.

Далее приведен пример команд консоли.

```
console(config-if)#bridge address 00:60:70:4C:73:FF permanent ethernet g8

console# show bridge address-table
```

```
Aging time is 300 sec
```

vlan	mac address	port	type
----	------------	----	--------
1	00:60:70:4C:73:FF	1/e8	dynamic
1	00:60:70:8C:73:FF	1/e8	dynamic
200	00:10:0D:48:37:FF	1/e9	static

Просмотр динамических адресов

На странице Dynamic Address Table (Таблица динамических адресов) приведены сведения по запросу данных в таблице динамических адресов, в том числе типа интерфейса, MAC-адреса, VLAN и таблицы сортировки. Пакеты, которые пересылаются по адресам, хранящимся в таблице адресов, пересылаются непосредственно на эти порты. Dynamic Address Table (Таблица динамических адресов) содержит информацию о сроке хранения, после которого динамические MAC-адреса удаляются, а также параметры для запросов и просмотра списка динамических адресов. Таблица текущих адресов содержит параметры динамических адресов, по которым пакеты передаются непосредственно на порты.

Чтобы открыть страницу Dynamic Address Table (Таблица динамических адресов), выберите **Switch** (Коммутатор)→ **Address Tables** (Таблицы адресов)→ **Dynamic** (Динамический)→ **MAC Address** (MAC-адрес) на панели дерева.

Рис. 7-32. Страница Dynamic Address Table (Таблица динамических адресов)

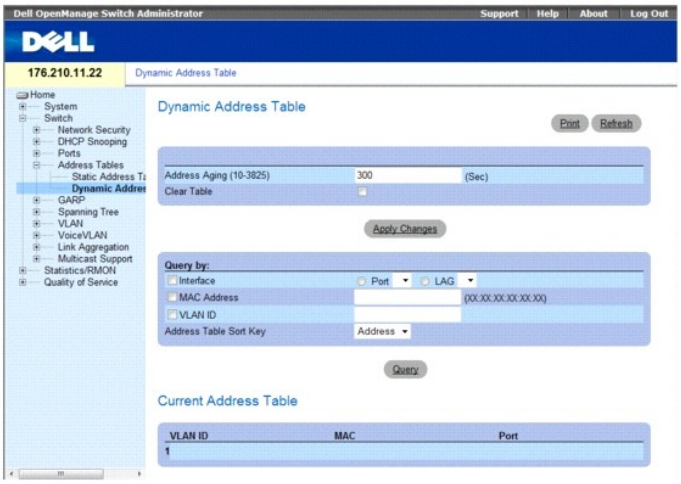


Таблица динамических адресов (Dynamic Address Table) содержит следующие поля:

- **Address Aging (10-3825) (Срок хранения адреса)**. Определяет временной интервал в секундах, в течение которого MAC-адрес остается в таблице динамических адресов (Dynamic Address Table) перед удалением, когда не обнаруживается трафик от источника. Значение по умолчанию: 300 секунд.
- **Clear Table (Очистить таблицу)**. Очистить таблицу динамических адресов.
  - **Флажок установлен**. Очищает таблицу динамических адресов.
  - **Флажок снят**. Оставляет таблицу динамических адресов.

Query By (Запрос по)

В разделе **Query By** (Запрос по), осуществляется выбор опции сортировки динамических адресов в таблице:

- **Port (По порту)**. Определяет интерфейс, для которого будет выполнен запрос по таблице. Можно выбрать один из двух типов интерфейсов.
- **MAC Address (MAC-адрес)**. Определяет MAC-адрес, для которого будет выполнен запрос по таблице.
- **VLAN ID (Идентификатор сети VLAN)**. Идентификатор VLAN, для которой будет выполнен запрос по таблице.

- **Address Table Sort Key (Ключ для сортировки таблицы адресов)**. Определяет, по какому полю сортируется таблица динамических адресов. Таблица динамических адресов может быть отсортирована по адресу, сети VLAN или интерфейсу.

Переопределение срока хранения

1. Откройте страницу Dynamic Address Table (Таблица динамических адресов).
2. Определите поле **Address Aging** (Срок хранения).
3. Нажмите кнопку **Apply Changes** (Применить изменения).

   Срок хранения будет изменен, а устройство обновлено.

Опрос таблицы динамических адресов

1. Откройте страницу Dynamic Address Table (Таблица динамических адресов).
2. Определите, по какому параметру нужно выполнить запрос таблицы **Dynamic Address Table** (Таблица динамических адресов).

   Записи запрашивать по полю **Port** (Порт), **MAC Address** (MAC-адрес) или **VLAN ID** (Идентификатор сети VLAN).
3. Нажмите кнопку **Query** (Запрос).

   Произойдет запрос таблицы динамических адресов (Dynamic Address Table) и результат будет выведен на просмотр.

Сортировка таблицы динамических адресов

1. Откройте страницу Dynamic Address Table (Таблица динамических адресов).
2. В раскрывающемся меню **Address Table Sort Key** (Ключ сортировки таблицы адресов) выберите поле, по которому будут отсортированы адреса - по адресу, идентификатору VLAN или интерфейсу.
3. Нажмите кнопку **Query** (Запрос).

   Dynamic Address Table (Таблица динамических адресов) отсортирована.

Опрос и сортировка динамических адресов с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для указания срока годности, опроса и сортировки динамических адресов, как они отображаются в таблице динамических адресов (Dynamic Address Table).

Таблица 7-17. Команды консоли для опроса и сортировки динамических адресов

Команда консоли	Описание
bridge aging-time секунды	Задает срок хранения для таблиц адресов.
show bridge address-table [[**vlan** *vlan*] [] [**ethernet** *interface* | | **port-channel** номер_канала_порта]]	Отображает классы динамически созданных записей базы данных, содержащей сведения о пересылке данных через мосты.

Далее приведен пример команд консоли.

```
console (config)# bridge aging-time 250

console (config)# console(config)# end

console# show bridge address-table
```

Aging time is 250 sec

vlan	mac address	port	type
----	-----------	----	----
1	00:60:70:4C:73:FF	1/e8	dynamic
1	00:60:70:8C:73:FF	1/e8	dynamic

200	00:10:0D:48:37:FF	1/e8	static

Настройка протокола GARP

Протокол GARP (Generic Attribute Registration Protocol) - это протокол общего назначения, регистрирующий любые возможности связи в сети или сведения о принадлежности. Протокол GARP определяет набор устройств, заинтересованных в данном атрибуте сети, например VLAN или адрес многоадресной передачи.

При настройке GARP выполняйте следующие инструкции:

- Время отключения должно быть больше или равно трехкратному времени соединения.
- Время полного отключения должно быть больше времени отключения.
- Устанавливает те же значения таймера GARP для всех устройство подключенных к уровню 2. Если таймеры GARP установлены по-разному на устройствах Layer 2, приложение GARP не сможет правильно работать.

Чтобы открыть страницу **GARP**, выберите Switch (Коммутатор) → **GARP** на панели дерева.

В этом разделе имеются следующие тематические подразделы:

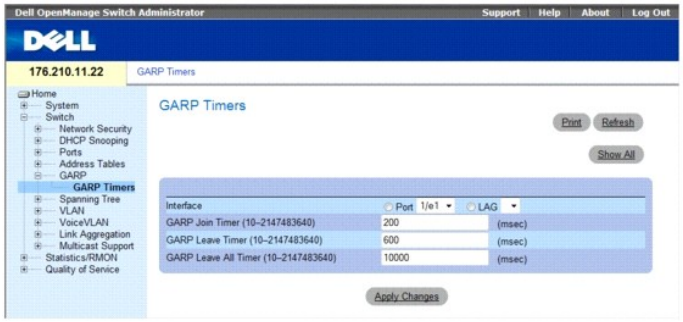
- Определение таймеров GARP

Определение таймеров GARP

Страница **GARP Timers** (Таймеры GARP) содержит поля для включения протокола GARP на устройстве.

Чтобы открыть страницу **GARP Timers** (Таймеры GARP), выберите Switch (Коммутатор)→ **GARP**→ **GARP Timers** (Таймеры GARP) на панели дерева.

Рис. 7-33. Страница GARP Timers (Таймеры GARP)



Страница GARP Timers (Таймеры GARP) содержит следующие поля:

- **Interface (Интерфейс)**. Определяет, где включен таймер - для порта или группы LAG.
- **GARP Join Timer (10 - 2147483640) (Таймер подключения)**. Время в миллисекундах, в течение которого, пересылаются блоки протокола данных (PDU). Значение по умолчанию: 200 мс.
- **GARP Leave Timer (10 - 2147483640) (Таймер отключения GARP)**. Время (в миллисекундах), в течение которого устройство ожидает, прежде чем выйти из состояния GARP. Отсчет времени Leave Time (Время отключения) активируется при отправке/получении сообщения Leave All Time (Время полного отключения) и отменяется при получении сообщения Join (Соединение). Время отключения должно быть больше или равно трехкратному времени соединения. Значение по умолчанию: 600 мсек.
- **GARP Leave All Timer (10 - 2147483640) (Таймер полного отключения GARP)**. Время (в миллисекундах), в течение которого все устройства ожидают, прежде чем выйти из состояния GARP. Время полного отключения должно быть больше времени отключения. Значение по умолчанию: 10000 мсек.

Определение таймеров GARP

1. Откройте страницу **GARP Timers** (Таймеры GARP).
2. Выберите интерфейс.
3. Заполните поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

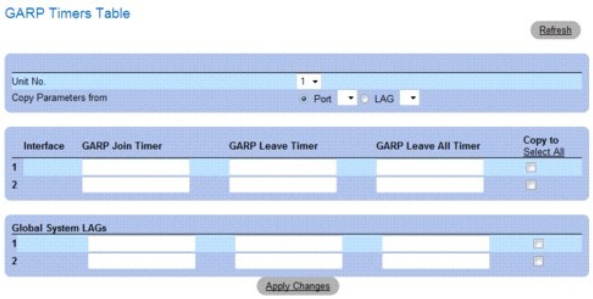
Параметры GARP будут сохранены на устройстве.

Копирование параметров в таблицу таймеров GARP

1. Откройте страницу **GARP Timers** (Таймеры GARP).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется таблица **GARP Timers Table** (Таблица таймеров GARP).

   Рис. 7-34. Таблица таймеров GARP



3. Выберите интерфейс в поле **Copy Parameters from** (Копировать параметры из) из выпадающего меню **Port** (Порт) или **LAG**.

   Определения для интерфейса будут скопированы в выбранный интерфейс. См. шаг 4.

4. Установите флажок в поле **Copy to** (Копировать в) для определения интерфейсов, для которых будут скопированы параметры таймера GARP, из поля **Copy Parameters from** (Скопировать параметры из), или выберите **Select All** (Выбрать все) для копирования определений во все порты или группы LAG.
5. Нажмите кнопку **Apply Changes** (Применить изменения).

   Параметры будут скопированы в выбранные порты или группы LAG в GARP Timers Table (Таблица таймеров GARP), а устройство обновлено.

Определение таймеров GARP с помощью команд консоли

В этой таблице приведены команды консоли для определения таймеров GARP, как показано на странице **Garp Timers** (Таймеры GARP).

Таблица 7-18. Команды консоли для определения таймеров GARP

Команда консоли	Описание
garp timer {join | leave | leaveall} время	Задает значения таймеров GARP для времени соединения, отключения и полного отключения приложений GARP.

Далее приведен пример команд консоли.

```
console(config)# interface ethernet 1/e1

console(config-if)# garp timer leave 900

console(config-if)# end

console# show gvrp configuration ethernet 1/e11



GVRP Feature is currently Disabled on the device.

Maximum VLANs: 223
```

Port (s)	GVRP-Status	Registration	Dynamic VLAN Creation	Timers (milliseconds) Join	Leave	Leave All
1/e11	Disabled	Normal	Enabled	200	900	10000

Настройка протокола STP

Протокол STP (Spanning Tree Protocol) предоставляет древовидную топологию для любого расположения мостов. STP обеспечивает также единственный путь между конечными станциями сети и исключает циклы.

Циклы появляются, когда между хостами существует несколько альтернативных маршрутов. Циклы в расширенной сети могут привести к тому, что мосты будут пересылать трафик неограниченно, в результате чего увеличится трафик и снизится производительность сети.

Устройство поддерживает следующие версии протоколов STP:

- **Classic STP (Классический STP)**. Обеспечивает единственный путь между конечными станциями сети и исключает циклы. Дополнительную информацию о настройке классического STP см. в разделе Определение общих параметров STP.
- **Rapid STP (Быстрый STP)**. Выявляет и использует топологию сети, обеспечивая лучшую сходимость для протокола STP без образования циклов пересылки. Если для устройства включен протокол RSTP, но на соседнем устройстве работает протокол STP, то локальное устройство будет использовать протокол STP.

  Дополнительную информацию о настройке быстрого STP см. в разделе **Настройка протокола RSTP**.

- **Multiple STP (Множественный STP (MSTP))**. Предоставляет полную связность для пакетов, назначаемых любым VLAN. Множественный STP базируется на RSTP. Кроме того, по протоколу MSTP передаются пакеты, назначенные разным VLAN через разные области MST. Если на устройстве работает протокол MSTP, области MST действуют как одиночный мост. Однако, если на соседнем устройстве работает протокол RSTP, а на локальном устройстве - протоколы STP, RSTP, и MSTP, то оба устройства могут нормально взаимодействовать.

  Дополнительную информацию о настройке MSTP см. в разделе **Настройка протокола MST**.

Чтобы открыть страницы **Spanning Tree** выберите **Switch** (Коммутатор)→ **Spanning Tree** на панели дерева.

В этом разделе имеются следующие тематические подразделы:

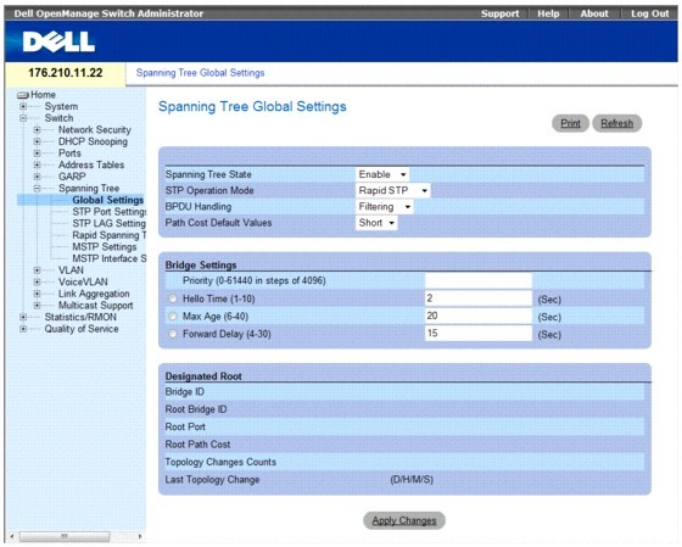
- Определение общих параметров STP
- Определение параметров STP для порта
- Определение параметров STP для LAG
- Определение протокола RSTP
- Настройка протокола Multiple Spanning Tree
- Определение параметров интерфейса MSTP

Определение общих параметров STP

На странице Spanning Tree Global Settings (Общие параметры STP) приведены параметры для включения протокола STP на устройстве.

Чтобы открыть страницу **Spanning Tree Global Settings** (Общие параметры STP), выберите **Switch** (Коммутатор)→ **Spanning Tree**→ **Global Settings** (Общие параметры) на панели дерева.

Рис. 7-35. Общие параметры STP



Страница Spanning Tree Global Settings (Общие параметры STP) содержит следующие поля:

- **Spanning Tree State (Состояние Spanning Tree)**. Включает или отключает протокол STP для устройства. Возможные значения:
  - **Enable (Включить)**. Включает протокол STP
  - **Disable (Отключить)**. Отключает протокол STP
- **STP Operation Mode (Режим работы STP)**. Режим включения протокола STP на устройстве. Возможные значения:
  - **Classic STP (Классический STP)**. Включает классический STP на устройстве. Это значение по умолчанию.
  - **Rapid STP (Быстрый STP)**. Включает быстрый STP на устройстве.
  - **Multiple STP (Протокол MSTP)**. Включает множественный STP на устройстве.
- **BPDU Handling (Обработка элементов данных протокола моста)**. Определяет метод управления элементами данных пакетов протокола *Bridge Protocol Data Unit* (BPDU), если протокол STP для порта/устройства отключен. BPDU используется для передачи информации протокола STP. Возможные значения:
  - **Filtering (Фильтр)**. Фильтрация пакетов BPDU, если протокол Spanning Tree отключен для интерфейса. Это значение по умолчанию.
  - **Flooding (Лавина)**. Отправка пакетов BPDU «лавиной», если протокол Spanning Tree отключен для интерфейса.
- **Path Cost Default Values (Метод определения стоимости пути)**. Определяет метод, используемый для назначения стоимости пути по умолчанию для портов STP. Возможные значения:
  - **Short (Короткий)**. Определяет диапазон от 1 до 65,535 для стоимости пути порта. Это значение по умолчанию.
  - **Long (Длинный)**. Определяет диапазон от 1 до 200 000 000 для стоимости пути порта.

Стоимость пути по умолчанию назначается для разных интерфейсов в зависимости от выбранного метода.

Интерфейс	Длинный	Short
LAG	20000	4
1000 Мбит/с	20000	4
100 Мбит/с	200000	19
10 Мбит/с	2000000	100

Установки моста

- **Priority (0-61440 in steps of 4096) (Приоритет от 0 до 61440 с шагом 4096)**. Значение приоритета для моста. Когда коммутаторы или мосты работают по протоколу STP, каждому из них назначается приоритет. После обмена пакетами BPDU устройство с низшим значением приоритета становится корневым мостом. Значение по умолчанию: 32768. Значение приоритета моста предоставляется с шагом 4096. Например, 4096, 8192, 12288 и т.д.
- **Hello Time (1-10) (Интервал приветствия)**. Определяет интервал приветствия для устройства. Это интервал отправки конфигурационных сообщений с корневого моста (в секундах). Значение по умолчанию: 2 секунды.
- **Max Age (6-40) (Максимальное время)**. Определяет максимальное время для устройства. Это максимальное время (в секундах), которое мост ожидает перед отправкой конфигурационного сообщения. Значение по умолчанию: 20 секунд.
- **Forward Delay (4-30) (Задержка пересылки)**. Определяет задержку пересылки для устройства. Это время, которое мост находится в состояниях распознавания (learning) и прослушивания (listening) перед пересылкой пакетов. Значение по умолчанию: 15 секунд.

Назначенный корень

- **Bridge ID (Идентификатор моста)**. Идентификатор приоритета и MAC-адрес моста.
- **Root Bridge ID (Идентификатор корневого моста)**. Идентификатор приоритета и MAC-адрес корневого моста.
- **Root Port (Корневой порт)**. Номер порта, предлагающего путь от данного моста к корневому с наименьшими затратами. Этот параметр имеет значение, если мост не является корневым.
- **Root Path Cost (Стоимость пути до корневого)**. Стоимость пути от данного моста до корневого.
- **Topology Changes Counts (Количество изменений топологии)**. Указывает общее количество изменений состояния STP.
- **Last Topology Change (Последнее изменение топологии)**. Время, прошедшее после инициализации или перенастройки моста и последнего изменения топологии. Время отображается в формате Д/Ч/М/С, например, 2Д/5Ч/10М/4С.

Определение общих параметров STP

1. Откройте страницу.
2. Выберите значение **Enable** (Включить) в поле **Spanning Tree State** (Состояние Spanning Tree).
3. Выберите режим **STP** в поле **STP Operation Mode** (Режим работы STP) и определите настройки моста.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   STP включен для этого устройства.

Изменение общих параметров STP

1. Откройте страницу.
2. Определите поля в диалоговом окне.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

   Параметры протокола STP будут изменены, а устройство обновлено.

Определение общих параметров протокола STP с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для определения общих параметров STP, как отображается на странице Spanning Tree Global Settings (Общие параметры STP).

Таблица 7-19. Команды консоли для определения общих параметров протокола STP

Команда консоли	Описание
spanning-tree	Включает функциональные возможности протокола STP.
spanning-tree mode {stp | rstp | mstp}	Настраивает режим работы протокола STP.
spanning-tree priority приоритет	Настраивает приоритет протокола STP.
spanning-tree hello-time секунды	Настраивает время Hello Time для моста протокола STP, определяющее, как часто устройство выполняет широковещательную передачу сообщений «Hello» другим устройствам.
spanning-tree max-age секунды	Настраивает максимальное время для моста протокола STP.
spanning-tree forward-time секунды	Настраивает время пересылки для моста протокола STP, определяющее, как долго порт находится в состоянии прослушивания и распознавания перед переключением в состояние пересылки.
show spanning-tree [ethernet *интерфейс* | **port-channel** *номер_канала_порта*] [**instance** *идентификатор_экземпляра*]	Отображает конфигурацию протокола STP.
show spanning-tree [detail] [**active** | **blockedports**] [**instance** *идентификатор_экземпляра*]	Отображает подробную информацию протокола STP об активных или заблокированных портах.
show spanning-tree mst- configuration	Отображает идентификатор конфигурации MST протокола STP.

Далее приведен пример команд консоли.

```
console(config)# spanning-tree

console(config)# spanning-tree mode rstp

console(config)# spanning-tree priority 12288
```

```
console(config)# spanning-tree hello-time 5

console(config)# spanning-tree max-age 12

console(config)# spanning-tree forward-time 25

console(config)# exit

console# show spanning-tree
```

Spanning tree enabled mode MSTP

Default port cost method: Short

Gathering information .....

MST 0 Vlans Mapped: 16-4094

CST Root ID Priority 20480

Address 00:30:ab:00:00:08

Path Cost 4

Root Port ch2

This switch is the IST master

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32768

Address 00:00:00:16:00:64

Max hops 20

Name	State	Prio.Nbr	Cost	Sts	Role	PortFast	Type
----	-----	-------	----	---	----	-------	----
1/e2	enabled	128.2	100	DSBL	Dsbl	No	P2p Intr
1/e3	enabled	128.3	100	DSBL	Dsbl	No	P2p Intr
1/e4	enabled	128.4	100	DSBL	Dsbl	No	P2p Intr
1/e5	enabled	128.5	19	FRW	Desg	Yes	P2p Intr
1/e6	enabled	128.6	100	DSBL	Dsbl	No	P2p Intr
1/e7	enabled	128.7	100	DSBL	Dsbl	No	P2p Intr
1/e8	enabled	128.8	100	DSBL	Dsbl	No	P2p Intr
1/e9	enabled	128.9	100	DSBL	Dsbl	No	P2p Intr
1/e10	enabled	128.10	100	DSBL	Dsbl	No	P2p Intr
1/e11	enabled	128.11	19	DSBL	Desg	Yes	P2p Intr

```
console# show spanning-tree active
```

Spanning tree enabled mode MSTP

Default port cost method: Short

Gathering information .....

MST 0 Vlans Mapped: 16-4094

CST Root ID Priority 20480

Address 00:30:ab:00:00:08

Path Cost 4

Root Port ch2

This switch is the IST master

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32768

Address 00:00:00:16:00:64

Max hops 20

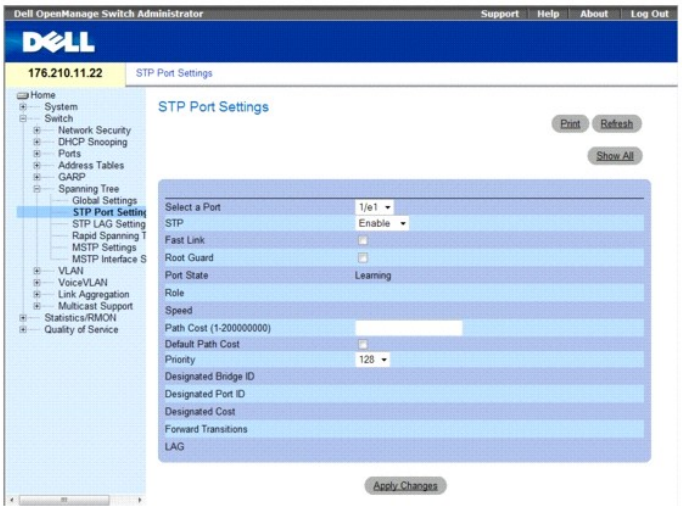
Name	State	Prio.Nbr	Cost	Sts	Role	PortFast	Type
----	-----	-------	----	---	----	-------	----
1/e5	enabled	128.2	19	FRW	Desg	Yes	P2p Intr
1/e7	enabled	128.7	19	DSCR	Altn	No	P2p Bound (STP)
1/e11	enabled	128.11	19	FRW	Desg	Yes	P2p Intr
1/e15	enabled	128.15	19	FRW	Desg	No	P2p Intr
1/e22	enabled	128.22	19	FRW	Desg	Yes	P2p Intr

Определение параметров STP для порта

Чтобы назначать свойства STP для отдельных портов, используйте страницу STP Port Settings (Параметры STP для порта).

Чтобы открыть страницу STP Port Settings (Параметры STP для порта), выберите **Switch** (Коммутатор)→ **Spanning Tree** (Протокол STP)→ **Port Settings** (Параметры порта) на панели дерева.

Рис. 7-36. Страница STP Port Settings (Параметры STP для порта)



Страница STP Port Settings (Параметры порта STP) содержит следующие поля:

- **Select a Port (Выбор порта)**. Указывает номер порта, для которого необходимо изменить параметры STP.
- **STP (Протокол STP)**. Включает или отключает протокол STP для порта. Возможные значения:
  - **Enable (Включить)**. Протокол STP для порта включен.
  - **Disable (Выключить)**. Протокол STP для порта выключен.
- **Fast Link (Быстрая связь)**. Включает режим быстрой связи для порта. Если режим быстрой связи для порта включен, то для параметра **Port State** (Состояние порта) автоматически устанавливается состояние **Forwarding** (Пересылка) сразу после появления связи. Режим Fast Link (Быстрая связь) оптимизирует время, которое требуется протоколу STP для сходимости. Для сходимости протокола STP в больших сетях может потребоваться от 30 до 60 секунд. Возможные значения:
  - **Флажок установлен**. Режим быстрой связи включен.
  - **Флажок снят**. Режим быстрой связи выключен.
- **Root Guard (Защита корня)**. Предотвращает назначение устройств за пределами ядра сети в качестве корня по протоколу STP.
  - **Флажок установлен**. Защита корня для порта включена.
  - **Флажок снят**. Защита корня для порта выключена.
- **Port State (Состояние порта)**. Показывает текущее состояние протокола STP для порта. Если этот параметр включен, он определяет, какое действие пересылки выполняется для трафика. Ниже перечислены возможные состояния порта.
  - **Disabled (Отключено)**. Протокол STP отключен на этом порте. Порт будет передавить весь трафик при распознавании MAC-адреса.
  - **Blocking (Блокирование)**. Порт в данный момент заблокирован, и его нельзя использовать для передачи трафика или распознавания MAC-адресов. Параметр Blocking (Блокирование) отображается, когда включен режим Classic STP (Классический STP).
  - **Listening (Прослушивание)**. Порт в данный момент находится в режиме прослушивания. Порт не может ни пересылать трафик, ни распознавать MAC-адреса.
  - **Learning (Распознавание)**. Порт в данный момент находится в режиме распознавания. Порт не может пересылать трафик, но может распознавать новые MAC-адреса.
  - **Forwarding (Пересылка)**. Порт в данный момент находится в режиме пересылки. Порт может пересылать трафик и распознавать новые MAC-адреса.
- **Role (Роль)**. Указывает роль порта, назначаемого алгоритмом STP для указания для путей STP. Возможные значения:
  - **Root (Корневой)**. Предоставляет путь с наименьшими затратами для пересылки пакетов в корневой коммутатор.
  - **Designated (Назначенный)**. Указывает порт или группу LAG, с помощью которых назначенный коммутатор подключен к LAN.
  - **Alternate (Альтернативный)**. Предлагает альтернативный путь к корневому коммутатору из корневого интерфейса.
  - **Backup (Резервный)**. Предлагает резервный путь к указанному пути порта к «листьям» протокола STP. Резервные порты требуются только в том случае, когда два порта соединены в петлю с помощью соединения «точка-точка». Резервные порты также необходимы,

когда LAN имеет два или более соединений к сегменту с общим доступом.

- **Disabled (Отключено)**. Указывает, что порт не участвует в соединении по протоколу STP.

- **Speed (Скорость)**. Скорость, на которой работает порт.
- **Path Cost (1-200000000) (Стоимость пути)**. Доля, которую этот порт вносит в стоимость пути к корню. Стоимость пути может иметь большее или меньшее значение и используется для пересылки трафика в случае переопределения маршрута пути.
- **Default Path Cost (Стоимость пути по умолчанию)**. Указывает, что устройство использует метод определения стоимости пути по умолчанию. Возможные значения:
  - **Флажок установлен**. Устройство использует метод определения стоимости пути по умолчанию.
  - **Флажок снят**. Устройство использует метод определения стоимости пути, указанный в поле Path Cost (Стоимость пути).
- **Priority (Приоритет)**. Значение приоритета для порта. Значение приоритета влияет на выбор порта, когда мост имеет два порта, соединенных в петлю. Значение приоритета находится в диапазоне: 0-240. Значения приоритета предоставляются с шагом 16.
- **Designated Bridge ID** (Идентификатор назначенного моста) - идентификатор приоритета и MAC-адрес назначенного моста.
- **Designated Port ID** (Идентификатор назначенного порта) - приоритет и интерфейс назначенного порта.
- **Designated Cost** (Назначенная стоимость) - стоимость порта, участвующего в топологии STP. Порты с меньшей стоимостью блокируются с меньшей вероятностью, когда STP определяет циклы.
- **Forward Transitions (Передача при пересылке)**. Показывает, сколько раз порт изменял свое состояние с **Forwarding** (Пересылка) на **Blocking** (Блокирование).
- **LAG** - группа LAG, с которой связан порт.

Включение STP для порта

1. Откройте страницу Spanning Tree **Port Settings** (Настройки порта STP).
2. Выберите порт.
3. Выберите значение **Enabled** (Включен) в поле **STP**.
4. Определите параметры полей **Fast Link** (Быстрая связь), **Root Guard** (Защита корня), **Path Cost** (Стоимость пути), **Default Path Cost** (Стоимость пути по умолчанию, и **Priority** (Приоритет).
5. Нажмите кнопку **Apply Changes** (Применить изменения).

   Протокол STP будет включен на этом порте.

Изменение параметров STP для порта

1. Откройте страницу Spanning Tree Port Settings (Настройки порта STP).
2. Выберите порт.
3. Измените соответствующие поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

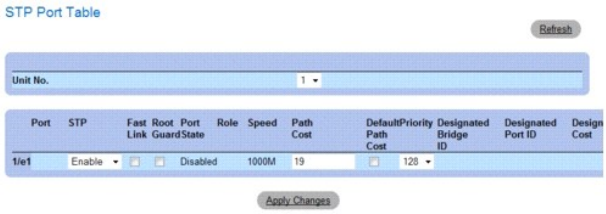
   Параметры STP для порта будут изменены, а устройство обновлено.

Отображение таблицы STP для порта

1. Откройте страницу Spanning Tree Port Settings (Настройки порта STP).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **STP Port Table** (Таблица STP для порта).

   Рис. 7-37. Таблица портов STP



Определение параметров STP для порта с помощью команд консоли

В следующей таблице приведены команды консоли, соответствующие полям для определения параметров STP для порта на странице **STP Port Settings** (Параметры STP для порта).

Таблица 7-20. Команды консоли для определения параметров STP для порта

Команда консоли	Описание
spanning-tree disable	Отключает протокол STP на определенном порте.
spanning-tree cost cost*стоимость*	Настройка стоимости пути для порта.
spanning-tree port-priority priority*приоритет*	Настраивает приоритет порта.
show **show spanning-tree [ethernet** *интерфейс* [| **port-channel** port-channel-number] [interface | **номер_канала_порта] [instance** *идентификатор_экземпляра*]]	Отображает конфигурацию протокола STP.
spanning-tree portfast	Включает режим быстрой связи.
spanning-tree guard root	Включение функции Root Guard на всех экземплярах STP для данного интерфейса.
show spanning-tree [detail] [active | **blockedports**] [**instance** *идентификатор_экземпляра*]	Отображает подробную информацию протокола STP об активных или заблокированных портах.
show spanning-tree mst- configuration	Отображает идентификатор конфигурации MST протокола STP.

Далее приведен пример команд консоли.

```
console> enable

console# configure

Console(config)# interface ethernet 1/e1

Console(config-if)# spanning-tree disable

Console(config-if)# spanning-tree cost 35000

Console(config-if)# spanning-tree port-priority 96

Console(config-if)# spanning-tree portfast

Console(config-if)# exit

Console(config)# exit

Console# show spanning-tree ethernet 1/e15
Port 1/e15 enabled
State: многоадресного                    Role: Designated
Port id: 128.15                          Port cost: 19
Type: P2p (configured: Auto) Internal Port Fast: No (configured: No)
Designated bridge Priority : 32768       Address: 00:00:00:16:00:64
Designated port id: 128.15               Designated path cost: 4
Guard root: Disabled
Number of transitions to forwarding state: 2
BPDU: sent 483, received 1037

console# show spanning-tree ethernet 1/e15 instance 12
Port 1/e15 enabled
```

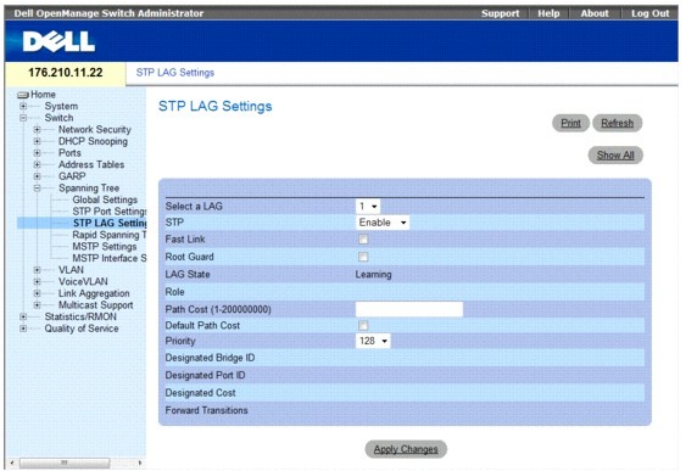
State: discarding			Role: alternate	
Port id: 128.15			Port cost: 19	
Type: P2p (configured: Auto) Internal Port Fast: No (configured: No)				
Designated bridge Priority : 32768			Address: 00:00:b0:07:07:49	
Designated port id: 128.11			Designated path cost: 0	
Guard root: Disabled				
Number of transitions to forwarding state: 3				
BPDU: sent 482, received 1035				

Определение параметров STP для LAG

Чтобы назначить параметры STP для объединенных портов, используйте страницу STP LAG Settings (Параметры STP для LAG).

Чтобы открыть страницу **STP LAG Settings** (Параметры STP для LAG), выберите **Switch** (Коммутатор)→ **Spanning Tree**→ (Протокол STP)→ **LAG Settings** (Параметры LAG) на панели дерева.

Рис. 7-38. Страница STP LAG Settings (Параметры STP для LAG)



Страница **Spanning Tree LAG Settings (Общие параметры STP LAG)** содержит следующие поля:

- **Select a LAG (Выбор LAG)**. Номер LAG, для которого необходимо изменить параметры STP.
- **STP (Протокол STP)**. Включает или отключает протокол STP для группы LAG. Возможные значения:
  - **Enable (Включить)**. Протокол STP для группы LAG включен.
  - **Disable (Выключить)**. Протокол STP для группы LAG выключен.
- **Fast Link (Быстрая связь)**. Включает режим быстрой связи для LAG. Если режим быстрой связи для группы LAG включен, то **LAG State** (Состояние LAG) автоматически переводится в состояние **Forwarding** (Пересылка) сразу после появления связи. Режим Fast Link (Быстрая связь) оптимизирует время, которое требуется протоколу STP для сходимости. Для сходимости протокола STP в больших сетях может потребоваться от 30 до 60 секунд. Возможные значения:
  - **Флажок установлен**. Режим быстрой связи включен.
  - **Флажок снят**. Режим быстрой связи выключен.
- **Root Guard (Защита корня)**. Предотвращает назначение устройств за пределами ядра сети в качестве корня по протоколу STP.
  - **Флажок установлен**. Защита корня для порта включена.
  - **Флажок снят**. Защита корня для порта выключена.
- **LAG State** (Состояние LAG) - текущее состояние протокола STP для группы LAG. Если этот параметр включен, действие пересылки, которое выполняется с трафиком, определяется по состоянию LAG. Если мост выявляет неполадки в работе группы LAG, то она переводится в состояние **Broken** (Оборвано). Ниже указаны возможные состояния LAG.
  - **Disabled (Отключено)**. Протокол STP отключен для LAG. LAG будет передавить весь трафик при распознавании MAC-адресов.
  - **Blocking (Блокирование)**. Группа LAG в данный момент заблокирована и не может использоваться для передачи трафика или распознавания MAC-адресов.
  - **RSTP Discarding State (Состояние отбраковывания RSTP)**. В этом состоянии порт не определяет MAC-адреса и не переадресовывает фреймы.
  - Это состояние является объединенным режимом состояний блокировки и определения, являющихся режимами работы протокола STP (802.1.D).

- **Listening (Прослушивание)**. LAG находится в режиме прослушивания и не может использоваться для передачи трафика или распознавания MAC-адресов.
- **Learning (Распознавание)**. LAG находится в режиме распознавания и не может пересылать трафик, но может распознавать новые MAC-адреса.
- **Forwarding (Пересылка)**. LAG находится в режиме передачи и может пересылать трафик и распознавать новые MAC-адреса.
- **Broken** (Оборвано) - LAG функционирует неправильно, и ее нельзя использовать для пересылки трафика.

- **Role (Роль)**. Указывает роль группы LAG, назначаемой алгоритмом STP для указания для путей STP. Возможные значения:
  - **Root (Корневой)**. Предоставляет путь с наименьшими затратами для пересылки пакетов в корневой коммутатор.
  - **Designated (Назначенный)**. Указывает группу LAG, с помощью которой назначенный коммутатор подключен к LAN.
  - **Alternate (Альтернативный)**. Предлагает альтернативную группу LAG к корневому коммутатору из корневого интерфейса.
  - **Backup (Резервный)**. Предлагает резервный путь к указанному пути порта к «листьям» протокола STP. Резервные порты требуются только в том случае, когда два порта соединены в петлю с помощью соединения «точка-точка». Резервные порты также необходимы, когда LAN имеет два или более соединений к сегменту с общим доступом.
  - **Disabled (Отключено)**. Указывает, что группа LAG не участвует в соединении по протоколу STP.
- **Path Cost (1-200000000)** (Стоимость пути) - доля, которую эта группа LAG вносит в стоимость пути к корню. Стоимость пути может иметь большее или меньшее значение и используется для пересылки трафика в случае переопределения маршрута пути. Стоимость пути может иметь значения от 1 до 200000000.
- **Default Path Cost (Стоимость пути по умолчанию)**. Указывает, что устройство использует метод определения стоимости пути по умолчанию. Возможные значения:
  - **Флажок установлен**. Устройство использует метод определения стоимости пути по умолчанию.
  - **Флажок снят**. Устройство использует метод определения стоимости пути, указанный в поле Path Cost (Стоимость пути).
- **Priority** (Приоритет) - значение приоритета для группы LAG. Значение приоритета влияет на выбор LAG, если на мосту порты соединены в петлю. Значения приоритета находятся в диапазоне 0-240 с шагом 16.
- **Designated Bridge ID** (Идентификатор назначенного моста) - идентификатор приоритета и MAC-адрес назначенного моста.
- **Designated Port ID** (Назначенный порт) - идентификатор интерфейса выбранного порта.
- **Designated Cost** (Назначенная стоимость) - стоимость порта, участвующего в топологии STP. Порты с меньшей стоимостью блокируются с меньшей вероятностью, когда STP определяет циклы.
- **Forward Transitions (Передача при пересылке)**. Показывает, сколько раз **LAG State** (Состояние LAG) изменялось с **Forwarding** (Пересылка) на **Blocking** (Блокирование).

Изменение параметров STP для группы LAG

1. Откройте страницу **Spanning Tree LAG Settings** (Настройки STP группы LAG).
2. Выберите LAG в раскрывающемся меню **Select a LAG** (Выбор LAG).
3. Выполните необходимые изменения в полях.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Параметры STP для группы LAG будут изменены, а устройство обновлено.

Отображение таблицы STP для группы LAG

1. Откройте страницу STP LAG Settings (Параметры STP для LAG).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **STP LAG Table** (Таблица STP для группы LAG).

Рис. 7-39. Таблица STP для группы LAG

Определение параметров STP для LAG с помощью команд консоли

В следующей таблице приведены команды консоли для определения параметров STP для LAG.

Таблица 7-21. Команды консоли для определения параметров STP для LAG

Команда консоли	**Описание**
`spanning-tree`	Включает STP.
`spanning-tree disable`	Отключает протокол STP для определенной группы LAG.
`spanning-tree cost стоимость`	Настраивает стоимость пути для группы LAG.
spanning-tree guard root	Включение функции Root Guard на всех экземплярах STP для данного интерфейса.
`spanning-tree port-priority приоритет`	Настраивает приоритет порта.
`show spanning-tree [show spanning-tree` **[ethernet** *интерфейс* `interface | |` **port-channel** `номер_канала_порта] [][`**instance** *`идентификатор_экземпляра`*`]]`	Отображает конфигурацию протокола STP.
show spanning-tree [detail] [active | blockedports] [instance *идентификатор_экземпляра*]	Отображает подробную информацию протокола STP об активных или заблокированных портах.

Далее приведен пример команд консоли.

```
console(config)# interface port-channel 1

console(config-if)# spanning-tree disable

console(config-if)# spanning-tree cost 35000

console(config-if)# spanning-tree port-priority 96

console(config-if)# spanning-tree portfast
```

Определение протокола RSTP

Если классический протокол spanning tree не позволяет выполнить пересылку циклов Layer 2 в общей топологии сети, период сходимости может достигать 30-60 секунд. Эта задержка позволяет определить возможные циклы, а также распространить данные об изменениях состояния.

Протокол RSTP (Rapid Spanning Tree Protocol) выявляет и использует топологию сети, обеспечивая лучшую сходимость для протокола STP без образования циклов пересылки.

Чтобы открыть страницу **Rapid Spanning Tree (RSTP)**, выберите **Switch** (Коммутатор)→ **Spanning Tree** → **Rapid Spanning Tree** (Протокол RSTP) на панели дерева.

Рис. 7-40. Страница Rapid Spanning Tree (RSTP)

Страница Spanning Tree RSTP содержит следующие поля:

- **Interface (Интерфейс)**. Порт или группа LAG, для которого выводятся настройки RSTP для просмотра и редактирования.
- **State (Состояние)**. Отключает протокол RSTP для выбранного интерфейса.
- **Role (Роль)**. Указывает роль порта, назначаемого алгоритмом STP для указания для путей STP. Возможные значения:

- **Root (Корневой)**. Предоставляет путь с наименьшими затратами для пересылки пакетов в корневой коммутатор.
- **Designated (Назначенный)**. Указывает порт или группу LAG, с помощью которых назначенный коммутатор подключен к LAN.
- **Alternate (Альтернативный)**. Предлагает альтернативный путь к корневому коммутатору из корневого интерфейса.
- **Backup (Резервный)**. Предлагает резервный путь к указанному пути порта к «листьям» протокола STP. Резервные порты требуются только в том случае, когда два порта соединены в петлю с помощью соединения «точка-точка». Резервные порты также необходимы, когда LAN имеет два или более соединений к сегменту с общим доступом.
- **Disabled (Отключено)** - указывает, что порт не участвует в соединении по протоколу STP.

- **Mode (Режим)**. Указывает текущий режим протокола STP. Режим протокола STP выбирается на странице **Spanning Tree Global Settings** (Общие параметры STP). Возможные значения:
  - **Classic STP (Классический STP)**. Указывает, что для устройства включен классический режим протокола STP.
  - **Rapid STP (быстрый STP)**. Указывает, что для устройства включен быстрый режим протокола STP.
  - **Multiple STP (Множественный STP)**. Указывает, что для устройства включен множественный режим протокола STP.
- **Fast Link Operational Status** (Рабочее состояние быстрой связи) - указывает, включен или выключен режим быстрой связи для порта или LAG. Если для интерфейса включен режим быстрой связи, то он автоматически переводится в состояние пересылки. Возможные значения:
  - **Enable (Включен)**. Режим быстрой связи включен.
  - **Disable (Выключить)**. Режим быстрой связи выключен.
  - **Auto (Автоматический)**. Режим быстрой связи включается через несколько секунд после того, как интерфейс становится активным.
- **Point-to-Point Admin Status (Состояние администрирования соединения «точка-точка»)**. Показывает, что включен режим соединения «точка-точка» или разрешает устройству совершить такое соединение. Возможные значения:
  - **Enable (Включить)**. Включает соединение «точка-точка» для устройства или задает автоматический режим такого соединения для устройства. Чтобы установить связь через соединение «точка-точка», PPP сначала посылает пакеты LCP (Link Control Protocol) и настройки для проверки соединения канала передачи данных. После установки соединения согласовывается дополнительное оборудование в соответствии с требованиями протокола LCP, PPP источника посылает пакеты Network Control Protocols (NCP) для выбора и настройки одного или нескольких уровней протокола уровня сети. После настройки каждого из выбранных протоколов уровня сети пакеты с каждого протокола уровня сети могут посылаться по каналу связи. Канал остается настроенным для связи до тех пор, пока он не будет закрыт с помощью пакетов LCP или NCP или не произойдет некоторое внешнее событие. Это реальный тип соединения порта коммутатора. Он может отличаться от административного состояния.
  - **Disable (Выключено)**. Выключает соединение «точка-точка».
  - **Auto (Автоматический)**. Устройство автоматически устанавливает соединение «точка-точка».
- **Point-to-Point Operational Status** (Рабочее состояние соединения «точка-точка») - показывает рабочее состояние соединения «точка-точка».
- **Activate Protocol Migrational (Активировать миграцию протокола)**. PPP разрешено посылать пакеты LCP (Link Control Protocol) для проверки и настройки соединения по передачи данных. Возможные значения:
  - **Флажок установлен**. Миграция протокола включена.
  - **Флажок снят**. Миграция протокола выключена.

Определение параметров RSTP

1. Откройте страницу Spanning Tree RSTP Settings (Параметры RSTP).
2. Выберите интерфейс.
3. Определите поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

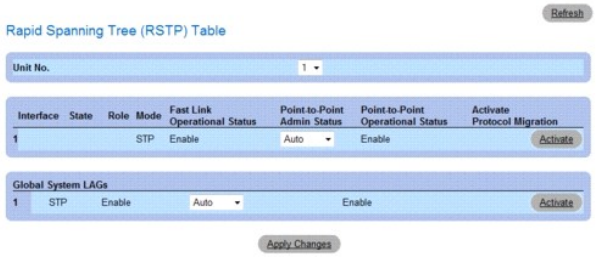
   Параметры RSTP будут определены, а устройство обновлено.

Отображение таблицы Rapid Spanning Tree (RSTP)

1. Откройте страницу Rapid Spanning Tree (RSTP).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **Rapid Spanning Tree (RSTP) Table** (Таблица Rapid Spanning Tree (RSTP)).

   Рис. 7-41. Таблица Rapid Spanning Tree (RSTP)



Определение параметров Rapid STP с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для определения параметров Rapid RSTP, как показано на странице Rapid Spanning Tree (RSTP).

Таблица 7-22. Команды консоли для определения параметров Rapid STP

Команда консоли	**Описание**
spanning-tree link-type {point-to-point | shared}	Переопределяет тип связи по умолчанию.
spanning tree mode {**stp** | **rstp** | **mstp**}	Настраивает работающий в данный момент протокол STP.
clear spanning-tree detected-protocols [**ethernet** *interface* | **port-channel** *port-channel-number*]	Перезапускает процесс миграции протоколов.
show spanning-tree [ethernetинтерфейс*port-channel***номер_канала_порта**	Отображает конфигурацию протокола STP.

Далее приведен пример команд консоли.

```
console(config)# interface ethernet 1/e5

console(config-if)# spanning-tree link-type shared

console(config-if)# spanning tree mode rstp
```

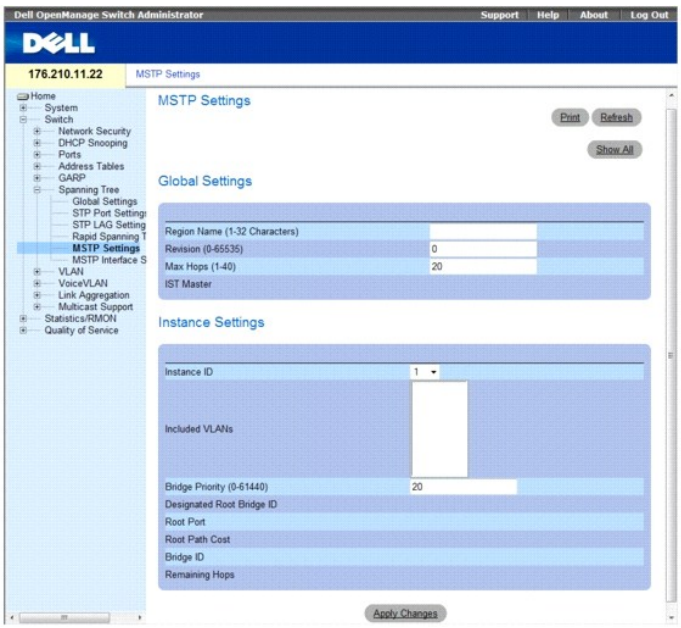
Настройка протокола Multiple Spanning Tree

Протокол MSTP сопоставляет сети VLAN в экземплярах STP. Данный протокол обеспечивает другой сценарий выравнивания нагрузки. Например, при блокировке порта A в одном экземпляре STP этот порт переходит в *состояние пересылки* в другом экземпляре STP.

Кроме того, пакеты, назначенные разным VLAN, передаются через разные пути в областях MST. Областями являются один или несколько мостов Multiple Spanning Tree, по которым передаются кадры.

Чтобы открыть страницу **MSTP Settings** (Параметры MSTP), выберите **Switch** (Коммутатор)→ **Spanning Tree** (Протокол STP)→ **MSTP Settings** (Настройка области MSTP) на панели дерева.

Рис. 7-42. Страница MSTP Settings (Параметры MSTP)



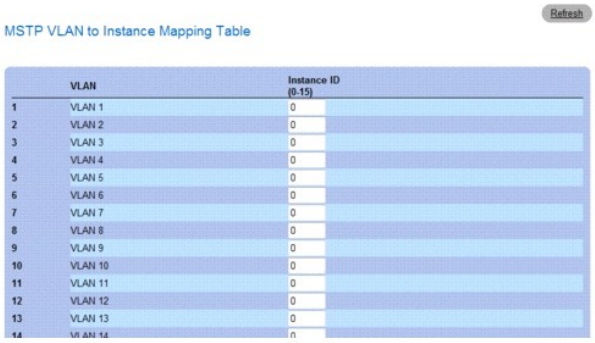
Страница **MSTP Settings** (Параметры MSTP) содержит следующие поля:

- **Region Name (1-32)** (Имя области) - указывает имя области MSTP, определяемое пользователем.
- **Revision (0-65535)** (Версия) - указывает 16-битное число без знака, определяющее версию текущей настройки MST. Номер версии необходим для настройки MST. Возможные значения поля: 0-65535.
- **Max Hops (1-40)** (Максимальное число узлов) - указывает общее число узлов, возникающих в определенной области, перед тем как пакеты BPDU будут отброшены. После того как пакеты BPDU будут отброшены, срок хранения информации о порте истечет. Возможные значения поля: 1-40. Значение по умолчанию: 2 узла.
- **IST Master (Мастер IST)**. Указывает идентификатор мастера Internal Spanning Tree. IST Master (Мастер IST) - корень указанного экземпляра 0.
- **Instance ID (Идентификатор экземпляра)** - определяет экземпляр протокола MSTP. Диапазон значений поля: 1-15.
- **Included VLANs (Включаемые VLAN)**. Отображает сети VLAN, привязанные к данному экземпляру. Каждая сеть VLAN принадлежит одному экземпляру.
- **Bridge Priority (0-61440) (Приоритет моста)**. Указывает приоритет устройства для выбора экземпляра протокола STP. Диапазон изменения поля 0-61440 с шагом 4096.
- **Designated Root Bridge ID (Идентификатор назначенного корневого моста)**. Указывает идентификатор моста, который является корневым для выбранного экземпляра.
- **Root Port (Корневой порт)**. Указывает корневой порт выбранного экземпляра.
- **Root Path Cost (Стоимость пути к корю)**. Указывает стоимость пути выбранного экземпляра.
- **Bridge ID (Идентификатор моста)**. Указывает идентификатор моста выбранного экземпляра.
- **Remaining Hops (Осталось узлов)**. Указывает оставшееся число узлов до следующей сети назначения.

Отображение страницы MSTP VLAN to Instance Mapping Table (Таблица привязки экземпляра к MSTP VLAN)

1. Откройте страницу **Spanning Tree** **MSTP Settings** (Параметры MSTP).
2. Выберите **Show All** (Показать все), чтобы открыть **таблицу привязки экземпляра к MSTP VLAN** (MSTP VLAN to Instance Mapping Table).

Рис. 7-43. Страница MSTP VLAN to Instance Mapping Table (Таблица привязки экземпляра к MSTP VLAN)



Определение экземпляров MST с помощью команд консоли

В следующей таблице показаны эквивалентные команды консоли для определения групп экземпляров MST, в том виде, как они показаны на странице **Spanning Tree** **MSTP Settings** (Параметры MSTP).

Таблица 7-23. Команды консоли для экземпляров MSTP

Команда консоли	**Описание**
spanning-tree mst configuration	Включает режим настройки MST.
instance *идентификатор_экземпляра* {**add** | **remove**} **vlan** *диапазон_vlan*	Привязывает VLAN к экземпляру MST.
name *строка*	Задает имя настройки.
revision *значение*	Задает номер версии настройки.
spanning-tree mst *идентификатор_экземпляра* **port-priority** *приоритет*	Устанавливает приоритет для порта.
spanning-tree mst *идентификатор_экземпляра* **priority** *приоритет*	Устанавливает приоритет устройства для указанного экземпляра протокола STP.
spanning-tree mst max-hops *число_узлов*	Устанавливает число узлов в области MST перед тем, как пакеты BPDU будут отброшены и срок хранения информации о порте истечет.
spanning-tree mst *идентификатор_экземпляра* **стоимость** *стоимость*	Устанавливает стоимость пути порта для вычислений MST.
exit	Выход из режима настройки области MST с сохранением изменений.
abort	Выход из режима настройки области MST без сохранения изменений.
show {**current** | **pending**}	Отображает текущую или незаконченную настройку области MST.

Далее приведен пример команд консоли.

```
console(config)# spanning-tree mst configuration

console(config-mst)# instance 1 add vlan 10-20

console(config-mst)# name region1

console(config-mst)# revision 1

console(config)# spanning-tree mst configuration

console(config-mst)# instance 2 add vlan 21-30

console(config-mst)# name region1

console(config-mst)# revision 1

console(config-mst)# show pending

Pending MST configuration

Имя: Region1

Revision: 1

Instance Vlans Mapped

-------- ------------
```

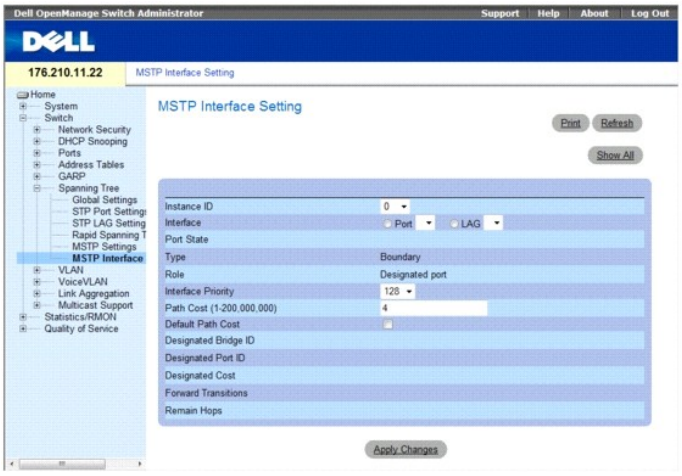
```
0 1-9,31-4094

1 10-20

2 21-30
```

Определение параметров интерфейса MSTP

На странице MSTP Interface Settings (Параметры интерфейса MSTP) содержатся параметры, позволяющие назначить параметры MSTP для определенных интерфейсов.

Чтобы открыть страницу **MSTP Interface Settings** (Параметры MSTP), выберите **Switch** (Коммутатор)→ **Spanning Tree** (Протокол STP)→ **MSTP Interface Settings** (Параметры интерфейса MSTP) на панели дерева.

Рис. 7-44. MSTP Interface Settings (Параметры интерфейса MSTP)



Страница **MSTP Interface Settings** (Параметры интерфейса MSTP) содержит следующие поля:

- **Instance ID (Идентификатор экземпляра)**. Перечисляет экземпляры MSTP, настроенные на устройстве. Возможные значения поля: 0-15.
- **Interface (Интерфейс)**. Назначает порты или LAG для выбранного экземпляра MSTP.
- **Port State(Состояние порта)**. Указывает, включен или выключен порт в определенном экземпляре.
- **Type (Тип)**. Указывает, является ли порт для MSTP двухточечным или он подключен к концентратору, а также является ли порт внутренним для области MSTP или граничным. Порт главного устройства обеспечивает соединяемость области MSTP с внешним корнем CIST. Граничный порт соединяет мосты MST с сетями LAN во внешней области. Если порт является граничным, параметр также указывает, работает ли устройство на другом конце линии в режиме RSTP или STP.
- **Role (Роль)**. Указывает роль порта, назначаемого алгоритмом STP для указания для путей STP. Возможные значения:
  - **Root** (Корневой) - предоставляет путь с наименьшими затратами для пересылки пакетов в корневое устройство.
  - **Designated (Назначенный)**. Указывает порт или группу LAG, с помощью которых назначенное устройство подключено к LAN.
  - **Alternate (Альтернативный)**. Предлагает альтернативный путь к корневому устройству из корневого интерфейса.
  - **Backup (Резервный)**. Предлагает резервный путь к указанному пути порта к «листьям» протокола STP. Резервные порты требуются только в том случае, когда два порта соединены в петлю с помощью соединения «точка-точка». Резервные порты также необходимы, когда LAN имеет два или более соединений к сегменту с общим доступом.
  - **Disabled (Отключено)**. Указывает, что порт не участвует в соединении по протоколу STP.
- **Interface Priority (Приоритет интерфейса) .** Определяет приоритет интерфейса для указанного экземпляра. Значение по умолчанию: 128.
- **Path Cost (Стоимость пути)**. Указывает долю, которую порт вносит в экземпляр протокола STP. Возможные значения поля: 1-200000000.
- **Default Path Cost (Стоимость пути по умолчанию)**. Указывает, что устройство использует метод определения стоимости пути по умолчанию. Возможные значения:
  - **Флажок установлен**. Устройство использует метод определения стоимости пути по умолчанию.
  - **Флажок снят**. Устройство использует метод определения стоимости пути, установленный пользователем.
- **Designated Bridge ID** (Идентификатор назначенного моста) - номер идентификатора моста, связывающего соединение или общую LAN с корнем.
- **Designated Port ID** (Идентификатор назначенного порта) - номер идентификатора порта на назначенном мосту, связывающем соединение или общую LAN с корнем.
- **Designated Cost** (Назначенная стоимость) - стоимость пути от соединения или общей LAN к корню.

- **Forward Transitions** (Передача при пересылке) - показывает, сколько раз порт изменял свое состояние на **forwarding** (пересылка).
- **Remain Hops** (Осталось узлов) - указывает оставшееся число узлов до следующей сети назначения.

Определение параметров интерфейса MSTP

1. Откройте страницу **MSTP Interface Settings** (Параметры интерфейса MSTP).
2. Выберите интерфейс.
3. Определите поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

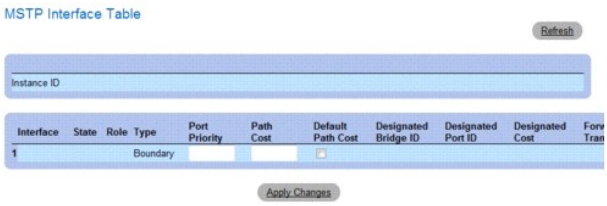
   Параметры RSTP будут определены, а устройство обновлено.

Просмотр страницы MSTP Interface Table (Таблица интерфейса MSTP)

1. Откройте страницу **MSTP Interface Settings** (Параметры интерфейса MSTP).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **MSTP Interface Table** (Таблица интерфейса MSTP) .

Рис. 7-45. Страница MSTP Interface Table (Таблица интерфейса MSTP)



Определение интерфейса MSTP с помощью команд консоли

В следующей таблице показаны эквивалентные команды консоли для определения интерфейсов MSTP, в том виде, в котором они показаны на странице **Spanning Tree** **MSTP Interface Settings** (Параметры MSTP).

Таблица 7-24. Команды консоли для интерфейса MSTP

Команда консоли	**Описание**
spanning-tree mst *идентификатор_экземпляра* **стоимость** *стоимость*	Устанавливает стоимость пути порта для вычислений MST.
spanning-tree mst *идентификатор_экземпляра* **priority** *приоритет*	Устанавливает приоритет устройства для указанного экземпляра протокола STP.
show spanning-tree mst- configuration	Отображает настройку MST.

Далее приведен пример команд консоли.

console# **show spanning-tree mst-configuration**		
Gathering information		
Current MST configuration		
Имя: Gili		
Revision: 65000		
Instance	Vlans Mapped	State
---------	------------------------	----------
0	16-4094	enabled
1	1	enabled
2	2	enabled

3	3	enabled
4	4	enabled
5	5	enabled
6	6	enabled
7	7	enabled
8	8	enabled
9	9	enabled
10	10	enabled
11	11	enabled
12	12	enabled
13	13	enabled
14	14	enabled
15	15	enabled

Настройка сетей VLAN

VLAN - это логические подгруппы сети, созданные программным, а не аппаратным путем. Группы VLAN объединяют пользовательские станции и сетевые устройства в одну группу независимо от того, к какому физическому сегменту LAN они подключены. Сети VLAN позволяют сделать более эффективным поток сетевого трафика в пределах подгрупп. Группы VLAN, управляемые с помощью программы, уменьшают время реализации изменений, добавлений и перемещений в сети.

Для доступа к онлайновой системе помощи для текущей страницы, нажмите ссылку ниже.

Минимальное число портов в VLAN не ограничено. Группы VLAN могут объединяться по модулям, по устройствам, по стеку или любым другим логическим соединениям, поскольку группы VLAN определяются на уровне программы, а не с помощью физических атрибутов.

Сети VLAN работают на уровне Layer 2. Поскольку они изолируют трафик внутри себя, для обеспечения трафика между группами VLAN необходим маршрутизатор уровня Layer 3, поддерживающий соответствующий уровень протокола. Маршрутизаторы уровня Layer 3 идентифицируют сегменты и координируют их с сетями VLAN. Группы VLAN - это широковещательные и многоадресные домены. Широковещательный и многоадресный трафик передается только в той сети VLAN, где он создается.

Маркировка сетей VLAN обеспечивает способ передачи информации VLAN между группами VLAN. При маркировке VLAN к заголовкам пакета присоединяется метка размером 4 байта. Метка VLAN указывает, к какой сети VLAN принадлежит пакет. Метки VLAN присоединяются к пакету на конечной станции или сетевом устройстве. Метки VLAN также содержат сведения о приоритете сетей VLAN.

Маркировка пакетов QinQ позволяет сетевым администраторам добавлять дополнительные метки на предварительно помеченные пакеты. Клиентские сети VLAN настраиваются при использовании QinQ. Добавление дополнительных меток на пакеты помогает расширить пространство VLAN. Дополнительная метка является для каждого клиента идентификатором VLAN (VLAN ID), что обеспечивает частный характер сетевого трафика и его изолированность. Идентификатор VLAN ID назначается для порта клиента в сети поставщика услуг. Затем для назначенного порта предоставляются дополнительные услуги для пакетов с двойными метками. Это позволяет администраторам расширять обслуживание пользователей VLAN.

Совместное использование сетей VLAN и протокола GVRP позволяет менеджерам сети объединять узлы сети в широковещательные домены. Широковещательный и многоадресный трафик ограничивается только передающей группой.

Чтобы открыть страницу **VLAN**, выберите **Switch**→ (Коммутатор)→ **VLAN** на панели дерева.

В этом разделе имеются следующие тематические подразделы:

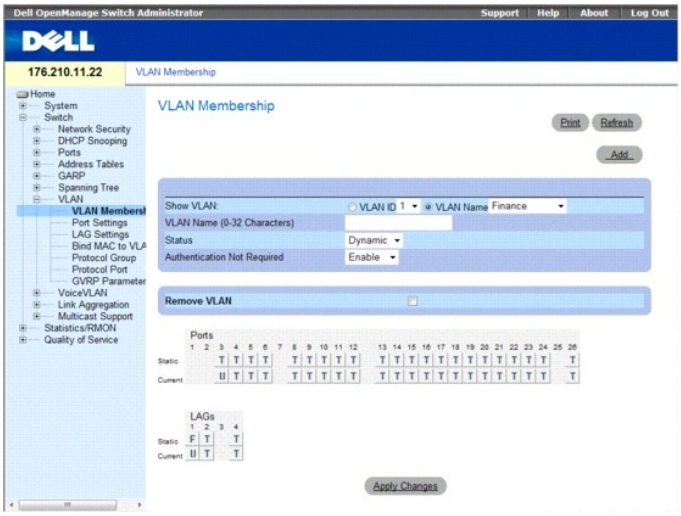
- Определение принадлежности к группе VLAN
- Определение параметров портов VLAN
- Определение параметров VLAN групп LAG
- Привязка MAC-адреса к сетям VLAN
- Определение групп протоколов VLAN
- Добавление интерфейсов к группам протоколов
- Настройка параметров GVRP

Определение принадлежности к группе VLAN

Страница **VLAN Membership** (Принадлежность VLAN) содержит поля для определения групп VLAN. Устройство поддерживает привязку идентификаторов VLAN 4094 к группам 256 VLAN. Все порты должны иметь определенный идентификатор PVID. Если не указано другое значение, то используется значение по умолчанию VLAN PVID. VLAN номер 1 - группа VLAN по умолчанию. Ее нельзя удалить из системы.

Чтобы открыть страницу VLAN Membership (Принадлежность VLAN), выберите **Switch** (Коммутатор)→ **VLAN** → **VLAN Membership** (Принадлежность VLAN) на панели дерева.

Рис. 7-46. Принадлежность VLAN



Страница **VLAN Membership** (Принадлежность VLAN) содержит следующие поля:

- **Show VLAN (Отобразить VLAN)**. Выводит информацию по конкретной группе VLAN в соответствии с идентификатором VLAN или именем VLAN.
- **VLAN Name (Имя сети VLAN, 0-32 символа)**. Имя сети VLAN, определенное пользователем.
- **Status (Состояние)**. Тип VLAN. Возможные значения:
  - **Dynamic (Динамическая)**. Показывает, что группа VLAN была динамически создана при использовании протокола GVRP.
  - **Static (Статическая)**. Показывает, что группа VLAN определена пользователем.
- **Authentication Not Required (Проверка подлинности не требуется)**. Указывает, могут ли неавторизованные пользователи получить доступ к сети VLAN. Возможные значения:
  - **Enable (Включить)** . Предоставляет неавторизованным пользователям доступ к сетям VLAN.
  - **Disable (Выключить)** . Закрывает неавторизованным пользователям доступ к сетям VLAN.
- **Remove VLAN (Удалить VLAN)**. Когда установлен этот параметр, VLAN удаляется из таблицы принадлежности VLAN.
  - **Флажок установлен**. Удаляет VLAN.
  - **Флажок снят**. Оставляет VLAN в таблице принадлежности VLAN.

Добавление новых сетей VLAN

1. Откройте страницу **VLAN Membership** (Принадлежность VLAN).
2. Нажмите кнопку **Add** (Добавить).

   Откроется страница Create New VLAN (Создание новой VLAN).

   Рис. 7-47. Create New VLAN (Создание новой VLAN)

3. Введите идентификатор и имя VLAN.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Новая группа VLAN будет добавлена, а устройство обновлено.

Изменение групп принадлежности VLAN

1. Откройте страницу **VLAN Membership** (Принадлежность VLAN).
2. Выберите сеть VLAN в раскрывающемся списке **Show VLAN** (Отобразить VLAN).
3. Выполните необходимые изменения в полях.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Информация о принадлежности VLAN будет изменена, а устройство обновлено.

Таблица принадлежности портов VLAN

Таблица портов VLAN содержит таблицу портов для назначения портов в группы VLAN. Принадлежность портов к VLAN определяется путем переключения параметров **Port Control** (Управление портом). Порты могут иметь следующие значения:

Таблица 7-25. Таблица принадлежности портов VLAN

Управление портом	Описание
T	Интерфейс входит в VLAN. Все пакеты, пересылаемые интерфейсом, помечаются. Пакеты содержат информацию о VLAN.
U	Интерфейс входит в VLAN. Пакеты, пересылаемые интерфейсом, не помечаются.
F	Интерфейсу отказано в принадлежности VLAN.
Пусто	Интерфейс не входит в VLAN. Пакеты, связанные с интерфейсом, не пересылаются.

В **VLAN Port Membership Table** (Таблица принадлежности портов VLAN) отображаются порты и состояния портов, а также группы LAG.

Назначение портов в группу VLAN

1. Откройте страницу **VLAN Membership** (Принадлежность VLAN).
2. Нажмите кнопку **VLAN ID** (Идентификатор VLAN) или **VLAN Name** (Имя VLAN) и выберите VLAN в раскрывающемся меню.
3. Выберите порт на странице **Port Membership Table** (Таблица портов сети VLAN) и назначьте значение для порта.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Порт будет назначен в группу VLAN, а устройство будет обновлено.

Удаление VLAN

1. Откройте страницу **VLAN Membership** (Принадлежность VLAN).
2. Нажмите кнопку **VLAN ID** (Идентификатор VLAN) или **VLAN Name** (Имя VLAN) и выберите VLAN в раскрывающемся меню.
3. Установите флажок **Remove VLAN** (Удалить VLAN).
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Выбранная группа VLAN будет удалена, а устройство будет обновлено.

Определение групп принадлежности VLAN с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для определения принадлежности групп VLAN, как показано на странице **VLAN Membership** (Принадлежность VLAN).

Таблица 7-26. Команды консоли для определения принадлежности VLAN

Команда консоли	Описание
vlan database	Включает режим настройки VLAN.
vlan {диапазон_vlan}	Создает VLAN.

name строка	Добавляет имя в VLAN.

Далее приведен пример команд консоли.

```
console(config)# vlan database

console(config-vlan)# vlan 1972

console(config-vlan)# end

console(config)# interface vlan 1972

console(config-if)# name Marketing

console(config-if)# end
```

Назначение портов в VLAN с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для назначения портов для групп VLAN.

Таблица 7-27. Команды консоли для назначения портов в группы VLAN

Команда консоли	Описание
switchport general acceptable-frame-types tagged-only	Отбрасывает входящие непомеченные кадры.
switchport forbidden vlan {add список_vlan | remove список_vlan}{ | }	Запрещает добавление указанных VLAN для порта.
switchport mode {access | trunk | general	Настраивает режим принадлежности VLAN для порта.
switchport access vlan *идентификатор_vlan*	Настраивает идентификатор порта VLAN, если интерфейс работает в режиме доступа.
switchport trunk allowed vlan {add *список_сетей_vlan* | **remove** *список_сетей_vlan*}	Добавляет или удаляет группы VLAN из порта, работающего в режиме транк.
switchport trunk native vlan *идентификатор_vlan*	Определяет принадлежность порт указанной группе VLAN и идентификатор VLAN как «идентификатор порта по умолчанию VLAN (PVID)».
switchport general allowed vlan add *список_сетей_vlan* [tagged | untagged]	Добавляет или удаляет группы VLAN из порта, работающего в общем режиме.
switchport general pvid идентификатор_vlan	Настраивает идентификатор порта PVID, если интерфейс работает в общем режиме.

Далее приведен пример команд консоли.

```
console(config)# vlan database

console(config-vlan)# vlan 23-25

console(config-vlan)# end

console(config)# interface vlan 23

console(config-if)# name Marketing

console(config-if)# end

console(config)# interface ethernet 1/e8

console(config-if)# switchport mode access

console(config-if)# switchport access vlan 23

console(config-if)# end

console(config)# interface ethernet 1/e9

console(config-if)# switchport mode trunk

console(config-if)# switchport mode trunk allowed vlan add 23-25

console(config-if)# end

console(config)# interface ethernet 1/e11
```

```
console(config-if)# switchport mode general

console(config-if)# switchport general allowed vlan add 23,25 tagged

console(config-if)# switchport general pvid 25
```

Определение параметров портов VLAN

Страница **VLAN Port Settings** (Параметры VLAN для порта) содержит поля для управления портами, входящими в группу VLAN. Идентификатор Port Default VLAN ID (PVID) настраивается на странице **VLAN Port Settings** (Параметры VLAN для порта). Все непомеченные пакеты, поступающие на устройство, маркируются идентификатором PVID портов.

Чтобы открыть страницу **VLAN Port Settings** (Параметры VLAN для порта), выберите **Switch** (Коммутатор)→ **VLAN**→ **Port Settings** (Параметры порта) на панели дерева.

Рис. 7-48. Страница VLAN Port Settings (Параметры порта VLAN)

Страница **VLAN Port Settings** (Параметры порта VLAN) содержит следующие поля:

- **Port (Порт)**. Номер порта, входящего в VLAN.
- **Port VLAN Mode (Режим порта VLAN)**. Режим работы порта. Возможные значения:
  - **Customer (Настраиваемый)**. Порт принадлежит к группе VLAN. Когда порт находится в режиме Customer (Настраиваемый), дополнительная метка является для каждого клиента идентификатором VLAN (VLAN ID), что обеспечивает частный характер сетевого трафика и его изолированность.
  - **General (Общий)**. Порт принадлежит нескольким группам VLAN, каждая из них определена пользователем как помеченная или непомеченная (дуплексный режим 802.1Q).
  - **Access (Доступен)**. Порт принадлежит к одной непомеченной группе VLAN. Когда порт находится в режиме доступа (Access), типы пакетов, которые принимаются на порт, нельзя назначить. Невозможно включить или отключить входящий фильтр на порте доступа.
  - **Trunk (Транк)**. Порты принадлежат группе VLAN, в которой все порты помечаются (кроме одного порта, который может остаться непомеченным).
- **Dynamic (Динамический)**. Назначает порт MAC-адресу, подключенному к порту, и определенном на основе сети VLAN.
  - **Флажок установлен**. Этот порт может быть зарегистрирован в динамической сети VLAN.
  - **Флажок снят**. Этот порт не может быть зарегистрирован в динамической сети VLAN.
- **PVID (1-4095)**. Присваивает идентификатор VLAN непомеченным пакетам. Возможны следующие значения: 1-4095. VLAN 4095 определяется в соответствии со стандартом и принятой практикой в отрасли, как «discard VLAN». Пакеты, определенные в эту группу «Игнорируемая VLAN», опускаются.
- **Frame Type (Тип кадра)**. Тип пакетов, принимаемый портом. Возможные значения:
  - **Admit Tag Only (Разрешить только помеченные)**. Порт принимает только помеченные пакеты.
  - **Admit All (Разрешить все)**. Порт принимает и помеченные, и непомеченные пакеты.
- **Ingress Filtering (Фильтрация на входе)**. При фильтрации на входе отклоняются пакеты, предназначенные для групп VLAN, к которым не принадлежит определенный порт.
  - **Enable (Включить)**. Фильтрация на входе включена.
  - **Disable (Выключить)**. Фильтрация на входе для указанного порта выключена.
- **Current Reserved VLAN (Текущая резервная группа VLAN)**. Группа VLAN, в настоящее время выделенная системой в качестве резервной группы VLAN.
- **Reserve VLAN for Internal Use (Резервная группа VLAN для внутреннего использования)**. Группа VLAN, выбранная пользователем в качестве резервной группы VLAN, если она не используется системой.

Назначение параметров порта

1. Откройте страницу **VLAN Port Settings** (Параметры VLAN для порта).
2. Выберите порт, для которого необходимо назначить параметры, в раскрывающемся списке **Port** (Порт).
3. Введите значения в необходимые поля
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Параметры порта VLAN будут определены, а устройство будет обновлено.

Отображение таблицы портов VLAN

1. Откройте страницу **VLAN Port Settings** (Параметры VLAN для порта).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **VLAN Port Table** (Таблица портов VLAN).

Рис. 7-49. VLAN Port Table (Таблица портов VLAN)

Определение параметров VLAN групп LAG

На странице **VLAN LAG Settings** (Параметры группы LAG сети VLAN) приведены параметры для управления группами LAG, входящими в состав VLAN. Сети VLAN состоят из отдельных портов или групп LAG. Непомеченные пакеты, поступающие на устройство, помечаются с помощью идентификатора групп LAG в соответствии с идентификатором PVID.

Чтобы открыть страницу **VLAN LAG Setting** (Параметры группы LAG сети VLAN), выберите **Switch** (Коммутатор)→ **VLAN**→ **LAG Settings** (Параметры группы LAG) на панели дерева.

Рис. 7-50. Страница VLAN LAG Setting (Параметры группы LAG сети VLAN)

Страница **VLAN LAG Settings** (Параметры группы LAG сети VLAN) содержит следующие поля:

- **LAG** - номер LAG, входящей в сеть VLAN.
- **LAG VLAN Mode (Режим LAG VLAN)**. Режим VLAN LAG. Возможные значения:
  - **Customer (Настраиваемый)**. Группа LAG принадлежит к сети VLAN. Если группа LAG находится в режиме Customer (Настраиваемый), дополнительная метка является для каждого клиента идентификатором VLAN (VLAN ID), что обеспечивает частный характер сетевого трафика и его изолированность.

- **General (Общий)**. Порт принадлежит нескольким группам VLAN, каждая из них определена пользователем как помеченная или непомеченная (дуплексный режим 802.1Q).
- **Access (Доступна)**. Группа LAG принадлежит одной непомеченной группе VLAN.
- **Trunk (Транк)**. Группа LAG принадлежат группе VLAN, в которой все порты помечаются (кроме одного порта, который может остаться непомеченным).

- **Dynamic (Динамический)**. Назначает группу LAG MAC-адресу, подключенному к порту, и определенном на основе сети VLAN. Возможные значения:
  - **Флажок установлен**. Группа LAG может быть зарегистрирована в динамической сети VLAN.
  - **Флажок снят**. Группа LAG может быть зарегистрирована в динамической сети VLAN.
- **PVID (1-4095)** . Присваивает идентификатор VLAN непомеченным пакетам. Возможные значения: 1-4095. VLAN 4095 определяется в соответствии со стандартом и принятой практикой в отрасли, как «discard VLAN». Пакеты, определенные в эту группу VLAN, опускаются.
- **Frame Type (Тип кадра)**. Тип пакетов, принимаемый группой LAG. Возможные значения:
  - **Admit Tag Only (Разрешить только помеченные)**. Группа LAG принимает только помеченные пакеты.
  - **Admit All (Разрешить все)**. Группа LAG принимает и помеченные, и непомеченные пакеты.
- **Ingress Filtering (Фильтрация на входе)**. Включает или отключает фильтрацию на входе для LAG. При фильтрации на входе отклоняются пакеты, предназначенные для групп VLAN, к которым не принадлежит определенная группа LAG. Возможные значения:
  - **Enable (Включить)**. Фильтрация на входе для группы LAG включена.
  - **Disable (Выключить)**. Фильтрация на входе для группы LAG выключена.
- **Current Reserve VLAN (Текущая резервная группа VLAN)**. Группа VLAN в настоящее время выделенная в качестве резервной группы VLAN.
- **Reserve VLAN for Internal Use (Резервная группа VLAN для внутреннего использования)**. Группа VLAN, назначенная в качестве резервной группы VLAN после выполнения сброса устройства.

Назначение параметров группы LAG группы VLAN:

1. Откройте страницу VLAN LAG Settings (Параметры группы LAG сети VLAN).
2. Выберите LAG в раскрывающемся меню **LAG** и заполните поля на странице.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

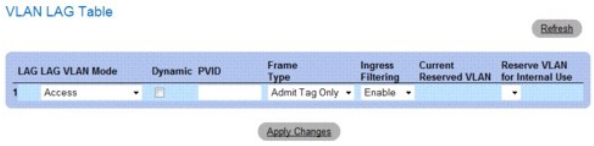
   Параметры группы LAG сети VLAN будут определены, а устройство обновлено.

Отображение таблицы групп LAG для VLAN

1. Откройте страницу VLAN LAG Settings (Параметры группы LAG сети VLAN).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница VLAN LAG Table (Таблица групп LAG для VLAN).

   Рис. 7-51. Таблица групп LAG для VLAN



3. Чтобы изменить параметры LAG, изменяйте значения полей в таблице для любой из групп LAG.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Параметры группы LAG сети VLAN будут определены, а устройство обновлено.

Назначение групп LAG в сети VLAN с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для назначения групп LAG группам VLAN, как показано на странице VLAN LAG Settings (Параметры группы LAG VLAN).

Таблица 7-28. Команды консоли для назначения групп LAG VLAN

Команда консоли	Описание
switchport mode {access | trunk | general}	Настраивает режим принадлежности LAG VLAN.
switchport trunk native vlan *идентификатор_vlan*	Определяет принадлежность порта указанной группе VLAN, а также определяет идентификатор VLAN как «идентификатор по умолчанию VLAN (PVID) для группы LAG».
switchport general pvid *идентификатор_vlan*	Настраивает идентификатор LAG VLAN ID (PVID), если интерфейс работает в общем режиме.
switchport general allowed vlan add *список_vlan* [**tagged** | **untagged**]	Добавляет или удаляет группы VLAN из группы LAG, работающей в общем режиме.
switchport general acceptable-frame-type tagged-only	Отбрасывает непомеченные входящие пакеты.
switchport access vlan dynamic	Привязывает MAC-адрес к сети VLAN.
switchport general ingress-filtering disable	Отключает фильтрацию на входе для LAG.

Далее приведен пример команд консоли.

```
console(config)# interface port-channel 1

console(config-if)# switchport mode access

console(config-if)# switchport access vlan 2

console(config-if)# exit

console(config)# interface port-channel 2

console(config-if)# switchport mode general

console(config-if)# switchport general allowed vlan add 2-3 tagged

console(config-if)# switchport general pvid 2

console(config-if)# switchport general acceptable-frame-type tagged-only

console(config-if)# switchport general ingress-filtering disable

console(config-if)# exit

console(config)# interface port-channel 3

console(config-if)# switchport mode trunk

console(config-if)# switchport trunk native vlan 3

console(config-if)# switchport trunk allowed vlan add 2
```

Привязка MAC-адреса к сетям VLAN

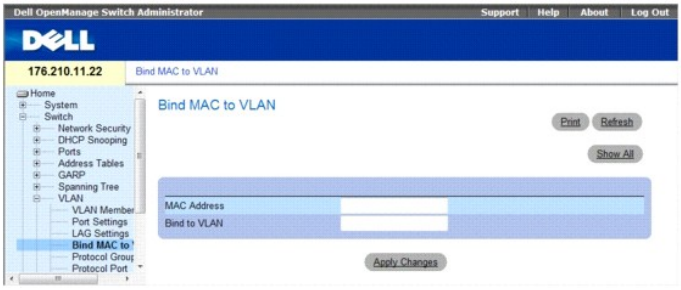
Привязка MAC-адреса к сетям VLAN обеспечивает назначение порта в зависимости от MAC-адресов. После того, как сеть VLAN назначена MAC-адресу и MAC-адрес для порта определен, этот порт присоединяется к привязке к VLAN. Если MAC-адрес устарел, этот порт исключается из сети VLAN. Только динамические сети VLAN могут быть привязаны к MAC-адресам.

ПРИМЕЧАНИЕ. Функция привязки MAC-адреса сети VLAN (MAC to VLAN Assignment) не поддерживается теми версиями, в которые встроена функция динамического назначения VLAN (DVA). Функция DVA обеспечивает ту же функциональность, что и назначение MAC-адреса сети VLAN, но выполняет эту функцию стандартным образом.

Чтобы привязать MAC-адреса сети VLAN, необходимо обеспечить, чтобы порты VLAN были динамическими, а не статическими.

Чтобы открыть страницу **Bind MAC to VLAN** (Привязка MAC-адреса сети VLAN), выберите **Switch** (Коммутатор)→ **VLAN**→ **Bind MAC to VLAN** (Привязка MAC-адреса сети VLAN).

Рис. 7-52. Привязка MAC-адреса сети VLAN



Страница **Bind MAC to VLAN** (Привязка MAC-адреса сети VLAN) содержит следующие поля:

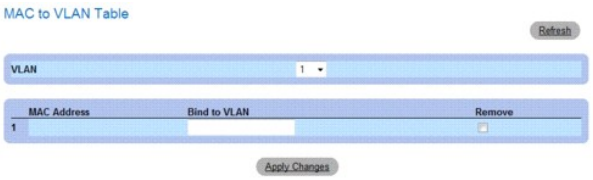
- **MAC Address (MAC-адрес)**. указывает MAC-адреса, которые привязываются сети VLAN.
- **Bind to VLAN (Привязать к сети VLAN)**. Указывает сеть VLAN, к которой производится привязка MAC-адреса. Возможные значения: 1-4094.

Отображение таблицы привязки MAC-адреса сети VLAN:

1. Откройте страницу **Bind MAC to VLAN** (Привязка MAC-адреса сети VLAN).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется таблица **MAC to VLAN Table** (Привязка MAC-адреса сети VLAN).

Рис. 7-53. Таблица привязки MAC-адреса сети VLAN



Удаление привязки адреса MAC к сети VLAN:

1. Откройте страницу **Bind MAC to VLAN** (Привязка MAC-адреса сети VLAN).
2. Нажмите кнопку **Show All** (Показать все). Откроется таблица **MAC to VLAN Table** (Привязка MAC-адреса сети VLAN).
3. Выберите нужную сеть VLAN, или выберите параметр **All** (Все), чтобы показать все привязки сетям VLAN.
4. Удалите флажок из поля **Remove** (Удалить) возле нужной связи.
5. Нажмите кнопку **Apply Changes** (Применить изменения).

Привязка MAC-адреса сети VLAN с помощью команд консоли:

В следующей таблице приведены эквивалентные команды консоли для привязки MAC-адреса сети VLAN.

Таблица 7-29. Команды консоли для привязки MAC-адреса сети VLAN

Команда консоли	Описание
`mac-to-vlan mac-address vlan-id`	Привязывает MAC-адрес к сети VLAN.
`switchport access vlan dynamic`	Выполняет настройку частных сетей VLAN.
`show mac-to-vlan`	Отображает базу данных привязки MAC-адреса сети VLAN
`no mac-to-vlan mac-address`	Удаляет привязку MAC-адреса сети VLAN.

Далее приведен пример команд консоли.

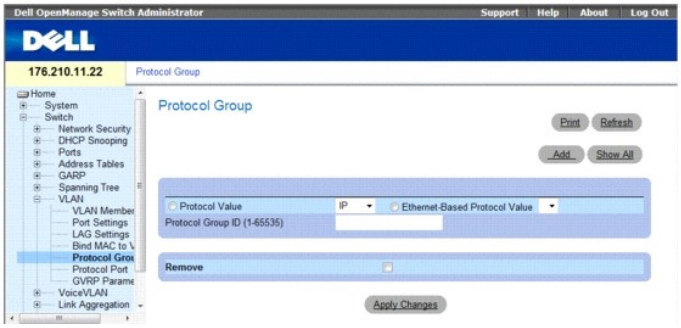
```
console(config-vlan)# mac-to-vlan 0060.704c.73ff 123

console(config-vlan)#exit

console(config)# exit

console# show vlan mac-to-vlan

MAC Address VLAN

------------ ------

0060.704c.73ff 123
```

Определение групп протоколов VLAN

На странице **Protocol Group** (Группа протокола) приведены параметры для настройки типов кадров для определенных групп протоколов.

Чтобы открыть страницу **Protocol Group** (Группа протоколов), выберите **Switch** (Коммутатор)→ **VLAN**→ **Protocol Group** (Группа протоколов) на панели дерева.

Рис. 7-54. Страница Protocol Group (Группа протокола)



- **Protocol Value (Значение протокола)**. Отображает значение протокола, определенного пользователем. Возможные опции таковы:
  - **Protocol Value (Значение протокола)**. Определенное пользователем имя протокола. Допустимые значения поля: **IP**, **IPX** и **ARP**.
  - **Ethernet-Based Protocol Value** . Тип группы протокола Ethernet.
- **Идентификатор группы протокола (1-65535)**. Идентификационный номер группы VLAN.
- **Remove** (Удалить) - при установке этого флажка удаляется групповая привязка «кадр-протокол», если группа протоколов, которая должна быть удалена, не настроена на этом порту протокола.
  - **Флажок установлен**. Удаляет отображение группы протокола.
  - **Флажок снят**. Сохраняет отображение группы протокола.

Назначение протокола группе

1. Откройте страницу **Protocol Group** (Группа протоколов).
2. Нажмите кнопку **Add** (Добавить).

   Откроется страница **Assign Protocol To Group** (Назначение протокола группе).

   Рис. 7-55. Назначение протокола группе

3. Заполните поля на этой странице.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Будет назначена группа протоколов, а устройство обновлено.

Назначение параметров группе протоколов VLAN

1. Откройте страницу **Protocol Group** (Группа протоколов).
2. Заполните поля на этой странице.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

   Параметры группы протоколов VLAN будут определены, а устройство обновлено.

Удаление протоколов из таблицы группы протоколов

1. Откройте страницу **Protocol Group** (Группа протоколов).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница Protocol Group Table (Таблица группы протоколов).

Рис. 7-56. Таблица Protocol Group (Группа протоколов)

3. Установите флажок **Remove** (Удалить) для тех групп протоколов, которые необходимо удалить.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Протокол будет удален, а устройство обновлено.

Определение групп протоколов VLAN с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для настройки групп протоколов.

Таблица 7-30. Команды консоли для определения групп протоколов VLAN

Команда консоли	Описание
map protocol *протокол [инкапсуляция]* **protocols-group** *группа*	Выполняет привязку протокола к группе протоколов. Группы протоколов используются для назначения группы VLAN, основанной на протоколах.

Следующий пример протокол ip-arp назначается для группы «213»:

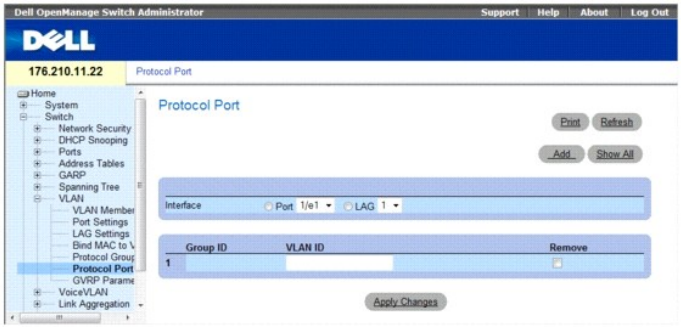
```
Console (config)# vlan database

Console (config-vlan)# map protocol ip-arp protocols-group 213
```

Добавление интерфейсов к группам протоколов

Страница **Protocol Port** (Порт протокола) используется для добавления интерфейса в группу протоколов.

Чтобы открыть страницу **Protocol Port** (Порт протокола), выберите **Switch** (Коммутатор)→ **VLAN**→ **Protocol Port** (Порт протокола) на панели дерева.

Рис. 7-57. Страница Protocol Port (Порт протокола)



- **Interface (Интерфейс)**. Номер порта или группы LAG добавляемых в группу протоколов.
- **Group ID (Идентификатор группы)**. Идентификатор группы протоколов, в которую добавляется интерфейс. Идентификатор группы протоколов определяется в таблице группы протоколов.
- **VLAN ID (Идентификатор сети VLAN)**. Связывает интерфейс с идентификатором VLAN, определенным пользователем. Идентификатор VLAN определяется на странице **Create a New VLAN** (Создание новой VLAN). Порт протокола может быть добавлен с использованием идентификатора VLAN или имени VLAN. Возможны следующие значения: 1-4095. VLAN 4095 определяется в соответствии со стандартом и принятой практикой в отрасли, как «discard VLAN».
- **Remove (Удалить)**. Указывает на удаление выбранного интерфейса из группы протокола.
  - **Флажок установлен**. Удаляет выбранный интерфейс.
  - **Флажок снят**. Оставляет выбранный интерфейс.

Добавление нового порта протокола к сети VLAN

Порты протокола можно определить только на портах, которые определены как общие (**General**) на странице **VLAN Port Settings** (Параметры VLAN для порта).

1. Откройте страницу **Protocol Port** (Порт протокола).
2. Нажмите кнопку **Add** (Добавить).

   Откроется страница **Assign Protocol Port To VLAN** (Назначение порта протокола сети VLAN).

   Рис. 7-58. Назначение порта протокола сети VLAN

3. Введите значения в полях диалогового окна.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

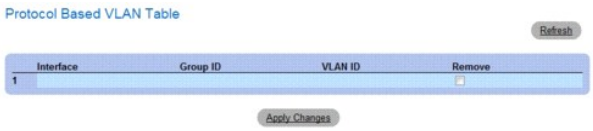
   Новая группа протоколов VLAN будет добавлена в **Protocol Port Table** (Таблица группы протоколов), а устройство обновлено.

Вывод на просмотр протоколов, назначенных портам

1. Откройте страницу **Protocol Port** (Порт протокола).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется **таблица сетей VLAN на основе протокола** (Protocol Based VLAN Table).

   Рис. 7-59. Таблица сетей VLAN на основе протокола



Определение портов протокола с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для определения портов протокола.

Таблица 7-31. Команды консоли для определения портов протокола

Команда консоли	Описание
switchport general map protocols-group *group* vlan *идентификатор_vlan*	Определяет правило классификации на основе протокола.

В следующем примере определяется правило классификации на основе протокола группы протоколов 1 для VLAN 8:

```
Console (config-if)# switchport general map protocols-group 1 vlan 8
```

Настройка параметров GVRP

Протокол GVRP (GARP VLAN Registration Protocol) специально предусмотрен для автоматического распределения информации о принадлежности VLAN между мостами, поддерживающими VLAN. Протокол GVRP позволяет таким мостам автоматически определять группы VLAN для назначения портов мостам, не настраивая отдельно каждый мост, и регистрировать принадлежность к VLAN.

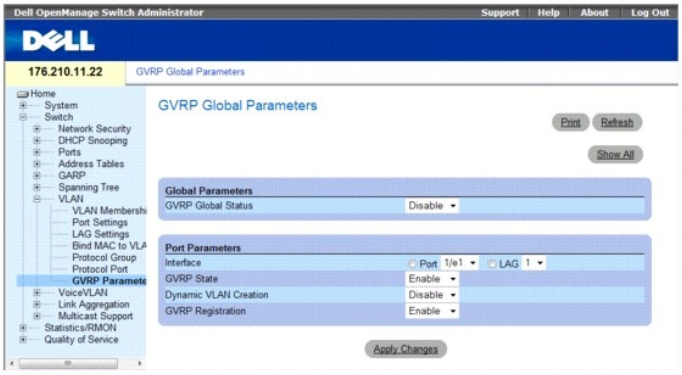
Чтобы гарантировать правильную работу протокола GVRP, рекомендуется установить для максимального количества групп VLAN с протоколом GVRP значение, которое существенно больше суммы:

- количества всех статических групп VLAN, настроенных на данных момент или ожидающих настройки;
- количества всех динамических VLAN, входящих в протокол GVRP, настроенных на данных момент (начальное количество динамических сетей VLAN с протоколом GVRP равно 128) или ожидающих настройки.

Страница GVRP Global Parameters (Общие параметры GVRP) позволяет глобально включить GVRP.Протокол GVRP можно также включить для отдельных интерфейсов.

Чтобы открыть страницу **GVRP Global Parameters** (Общие параметры GVRP), выберите **Switch** (Коммутатор)→ **VLAN** → **GVRP Parameters** (Параметры GVRP) на панели дерева.

Рис. 7-60. Страница GVRP Global Parameters (Общие параметры GVRP)



Страница GVRP Global Parameters (Общие параметры GVRP) содержит следующие поля:

Global Parameters (Общие параметры)

- **GVRP Global Status (Общий статус GVRP)**. Указывает, включен ли протокол GVRP на устройстве. Возможные значения:
  - **Enable (Включен)**. Включает протокол GVRP на выбранном устройстве.
  - **Disable (Выключен)**. Выключает протокол GVRP на выбранном устройстве. GVRP по умолчанию отключен.

Параметры порта

- **Interface (Интерфейс)**. Порт или группа LAG, для которого выводятся настройки GVRP для редактирования.
- **GVRP State (Состояние GVRP)**. Указывает, включен ли протокол GVRP на интерфейсе. Возможные значения:
  - **Enabled (Включен)**. Включает протокол GVRP на выбранном интерфейсе.
  - **Disabled (Выключен)**. Выключает протокол GVRP на выбранном интерфейсе.
- **Dynamic VLAN Creation (Создание динамической сети VLAN)**. Указывает, что на интерфейсе включено создание динамической сети VLAN. Возможные значения:
  - **Enabled (Включено)**. На интерфейсе включено создание динамической сети VLAN.
  - **Disabled (Выключено)**. На интерфейсе выключено создание динамической сети VLAN.
- **GVRP Registration (Регистрация GVRP)**. Указывает, включена ли регистрация сети VLAN через протокол GVRP на данном интерфейсе. Возможные значения:
  - **Enabled (Включено)**. Регистрация сети VLAN через протокол GVRP на данном интерфейсе включена.
  - **Disabled (Выключено)**. Регистрация сети VLAN через протокол GVRP на данном интерфейсе выключена.

Включение GVRP на устройстве

1. Откройте страницу **GVRP Global Parameters** (Общие параметры GVRP).
2. Выберите значение **Enable** (Включить) в поле **GVRP Global Status** (Общее состояние GVRP).
3. Нажмите кнопку **Apply Changes** (Применить изменения).

   Протокол GVRP будет включен на этом устройстве.

Включение регистрации группы VLAN по протоколу GVRP

1. Откройте страницу **GVRP Global Parameters** (Общие параметры GVRP).
2. Выберите значение Enable (Включить) в поле GVRP Global Status (Общее состояние GVRP).
3. Для необходимого интерфейса выберите значение **Enable** (Включить) в поле GVRP State (Состояние GVRP).
4. Выберите значение **Enable** (Включить) в поле **GVRP Registration** (Регистрация GVRP).
5. Нажмите кнопку **Apply Changes** (Применить изменения).

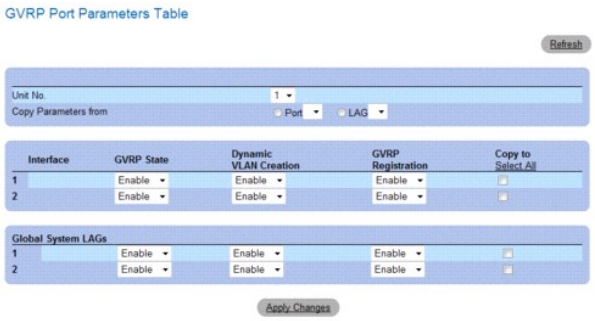
   Регистрация сети VLAN по протоколу GVRP будет включена для порта, а устройство будет обновлено.

Отображение таблицы параметров GVRP

1. Откройте страницу **GVRP Global Parameters** (Общие параметры GVRP).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется таблица **GVRP Port Parameters Table** (Таблица параметров порта GVRP).

Рис. 7-61. Таблица параметров порта GVRP



Помимо полей окна **GVRP Global Parameters** (Общие параметры GVRP), таблица **GVRP Port Parameters Table** (Таблица параметров порта GVRP) содержит следующее поле:

Copy Parameters from (Копировать параметры из). указывает порт или группу LAG, из которого нужно скопировать параметры и назначить их другому интерфейсу.

Настройка протокола GVRP с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для настройки GVRP, как показано на странице **GVRP Global Parameters** (Общие параметры GVRP).

Таблица 7-32. Команды консоли для настройки общих параметров протокола GVRP

Команда консоли	Описание
gvrp enable (global**)**	Включает протокол GVRP для системы в целом.
gvrp enable (interface)	Включает протокол GVRP для интерфейса.
gvrp vlan-creation-forbid	Включает или отключает динамическое создание VLAN.
gvrp registration-forbid	Отменяет регистрацию всех динамических сетей VLAN и предотвращает динамическую регистрацию VLAN для порта.
show gvrp configuration [**ethernet** *интерфейс*| **port-channel** *номер_канала_порта*]	Отображает сведения о конфигурации протокола GVRP, в том числе значения таймеров, разрешен ли протокол GVRP или динамическое создание сети VLAN, а также какие порты работают по протоколу GVRP.
show gvrp error-statistics [**ethernet** *интерфейс*| **port-channel** *номер_канала_порта*]	Отображает статистику ошибок протокола GVRP.
show gvrp statistics [**ethernet** *интерфейс*| **port-channel** *номер_канала_порта*]	Отображает статистику протокола GVRP.
clear gvrp statistics [**ethernet** *интерфейс*| **port-channel** *номер_канала_порта*]	Сбрасывает всю статистику протокола GVRP.

Далее приведен пример команд консоли.

```
console(config)# gvrp enable

console(config)# interface ethernet 1/e1

console(config-if)# gvrp enable

console(config-if)# gvrp vlan-creation-forbid

console(config-if)# gvrp registration-forbid

console(config-if)# end

console# show gvrp configuration

GVRP Feature is currently Enabled on the device (Для данного устройства функция GVRP в настоящее время включена)

Maximum VLANs: 223
```

Port(s)	GVRP- Status	Registration	Dynamic VLAN Creation	Timers (milliseconds) Join	Leave	Leave All
-------	------	------------	--------	--------------	-----	-----
1/e11	Enabled	Forbidden	Disabled	200	900	10000
1/e12	Disabled	Normal	Enabled	200	600	10000

Настройка голосовых сетей VLAN

Голосовая VLAN позволяет сетевым администраторам совершенствовать службу VoIP путем настройки портов на передачу голосового трафика IP с IP-телефонов на определенную сеть VLAN. Трафик VoIP имеет предварительно настроенный префикс OUI в исходном MAC-адресе. Сетевые администраторы могут выполнить настройку сетей VLAN, на которые пересылается голосовой IP-трафик. Трафик, не являющийся трафиком VoIP, выпадает из голосовой VLAN в автоматическом режиме безопасности голосовой VLAN. Голосовая VLAN также обеспечивает функционирование службы QoS (Качество обслуживания) для VoIP, что способствует тому, что качество голоса не ухудшается, если IP-трафик принимается неравномерно. Система поддерживает одну голосовую сеть VLAN.

Существуют два режима работы IP-телефонов:

- IP-телефон настраивается с поддержкой VLAN и обязательной пометкой пакетов при всех видах связи.

- При запрещенном режиме VLAN телефон будет использовать непомеченные пакеты. Телефон использует непомеченные пакеты во время получения начального IP-адреса через DHCP. Но затем телефон начинает использовать голосовую VLAN и посылает помеченные пакеты.

Раздел включает следующие темы:

- Страница определения параметров голосовой сети VLAN
- Определение параметров голосовой сети VLAN для порта
- Определение префиксов OUI

В этом разделе имеются следующие тематические подразделы:

- Определение общих параметров голосовой сети VLAN
- Определение параметров голосовой сети VLAN для порта
- Определение префиксов OUI

Определение общих параметров голосовой сети VLAN

Страница **Voice VLAN Global Parameters** (Общие параметры голосовой сети VLAN) содержит параметры которые применяются для всех голосовых VLAN на устройстве.

Чтобы открыть страницу **Voice VLAN Global Parameters** (Общие параметры голосовой сети VLAN) щелкните **Switch** (Коммутатор)→ **Voice VLAN** (Голосовая VLAN)→ **Global Parameters** (Общие параметры) на панели дерева.

Рис. 7-62. Страница Voice VLAN Global Parameters (Общие параметры голосовой сети VLAN)

- **Voice VLAN Status** (Состояние голосовой VLAN) - показывает, включена ли голосовая VLAN на устройстве. Возможные значения:
  - **Enable** (Включено) - включает голосовую VLAN на устройстве.
  - **Disable** (Отключено) - отключает голосовую VLAN на устройстве. Это значение по умолчанию.
- **Voice VLAN ID** (Идентификатор голосовой VLAN) - определяет идентификатор голосовой VLAN.
- **Class of Service** (Класс обслуживания) - включает добавление пометки CoS к непомеченным пакетам полученным в сети голосовой VLAN. Возможные значения от 0 до 7, где 0 означает наименьший приоритет, а 7 - высший.
- **Remark CoS (Метка CoS)**. Указывает, что Метка CoS всегда включена.
- **Voice VLAN Aging Time** (Срок действия голосовой VLAN) - указывает время, прошедшее с момента истечения срока действия последнего префикса OUI IP-телефона для указанного порта. Срок действия порта закончится после истечения срока действия связи и голоса. Время по умолчанию - один день. Формат поля - день:часы:минуты. Началом срока действия считается момент удаления MAC-адреса из таблицы «Dynamic MAC Address» (Динамические MAC-адреса) по истечении срока его действия. Время по умолчанию - 300 сек. Дополнительную информацию о сроке действия MAC-адресов см. в «Defining Aging Time» (Определение срока действия).

Configuring Voice VLAN Global Parameters (Настройка общих параметров голосовой сети VLAN):

1. Откройте страницу **Voice VLAN Global Parameters** (Общие параметры голосовой сети VLAN).
2. Заполните поля на этой странице.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

   Общие параметры голосовой сети VLAN будут определены, а устройство обновлено.

Определение общих параметров голосовой сети VLAN с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для определения Voice VLAN global parameters (Общие параметры голосовой сети VLAN).

Таблица 7-33. Voice VLAN Global Parameters (Общие параметры голосовой сети VLAN) Команды консоли

Команда консоли	**Описание**
voice vlan id *vlan-id* ***no voice vlan id***	Чтобы включить голосовую сеть VLAN и настроить идентификатор голосовой сети VLAN, используйте команду voice vlan id в режиме настройки общих параметров. Чтобы отключить голосовую сеть VLAN, используйте форму no этой команды.
voice vlan cos *cos* no voice vlan cos	Чтобы настроить класс обслуживания голосовой сети VLAN, используйте команду voice vlan cos в режиме настройки общих параметров. Чтобы восстановить значение по умолчанию, используйте форму no этой команды.
voice vlan aging-timeout ***minutes*** no voice aging-timeout	Чтобы установить тайм-аут срока использования голосовой VLAN, используйте команду voice vlan aging-timeout в режиме глобальной конфигурации. Чтобы восстановить значение по умолчанию, используйте форму no этой команды.
voice vlan enable	В режиме настройки интерфейса используйте команду voice vlan enable для включения автоматической настройки голосовой сети VLAN для порта. Чтобы отключить автоматическую настройку голосовой сети VLAN, используйте форму no этой команды.
show voice vlan [ethernet *interface* | port-channel *номер_порта-канала*]	В режиме EXEC используйте команду show voice vlan, чтобы отобразить состояние голосовой сети VLAN.

Switch# show voice vlan Aging timeout: 1440 minutes OUI table			
MAC Address - Prefix	Description		
00:E0:BB	3COM		
00:03:6B	Cisco		
00:E0:75	Veritel		
00:D0:1E	Pingtel		
00:01:E3	Siemens		
00:60:B9	NEC/Philips		
00:0F:E2	Huawei-3COM		
Voice VLAN VLAN ID: 8 CoS: 6 Remark: Yes			
Interface	Enabled	Secure	Activated
------	------	------	------
1/e1	Yes	Yes	Yes
1/e2	Yes	Yes	Yes
1/e3	Yes	Yes	Yes
1/e4	Yes	Yes	Yes
1/e5	No	No	-
1/e6	No	No	-
1/e7	No	No	-
1/e8	No	No	-
1/e9	No	No	-

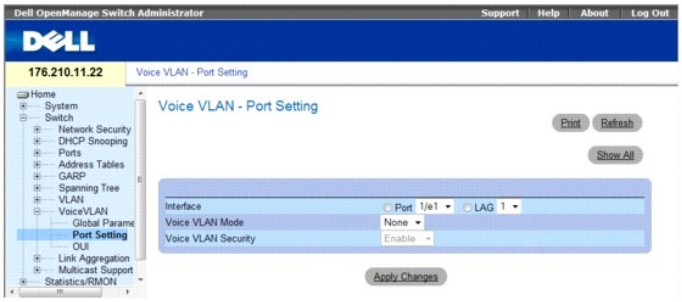
Ниже приведен пример команд консоли:

Определение параметров голосовой сети VLAN для порта

Страница VLAN Port Settings (Параметры голосовой сети VLAN для порта) содержит поля для добавления портов или групп LAG в голосовую сеть VLAN.

Чтобы открыть страницу **Voice VLAN Port Setting** (Параметры голосовой сети VLAN для порта), щелкните **Switch** (Коммутатор)→ **Voice VLAN** (Голосовая сеть VLAN)→ **Port Setting** (Параметры порта) на панели дерева.

Рис. 7-63. Voice VLAN Port Setting (Параметры голосовой сети VLAN для порта)



- **Interface (Интерфейс)**. Означает определенный порт или группу LAG, к которой применяются параметры голосовой сети VLAN.
- **Voice VLAN Mode (Режим голосовой сети VLAN)**. Определяет режим голосовой сети VLAN. Возможные значения:
  - ***None (Нет)***. Выключает выбранный порт/группу LAG в голосовой сети VLAN.
  - ***Static (Статический)*** - поддерживает текущие параметры голосовой сети VLAN для порта/группы LAG. Это значение по умолчанию.
  - ***Auto (Авто)***. Означает, что если трафик с MAC-адресом IP-телефонов передается для порта/группы LAG, порт/группа LAG присоединяется к голосовой сети VLAN. Порт/группа LAG в голосовой сети VLAN устаревает, если MAC-адрес IP-телефонов (с префиксом OUI) устаревает и превышает заданное значение. Если префикс OUI MAC-адреса IP-телефонов был добавлен вручную для порта/группы LAG в голосовой сети VLAN, пользователь может добавить его в голосовую сеть VLAN только в ручном режиме, но не в режиме Auto (Авто).
- **Voice VLAN Port/LAG Security** (Безопасность портов/групп LAG голосовой сети VLAN) - означает, что безопасность портов/групп LAG в голосовой сети VLAN включена. Безопасность порта гарантирует, что пакеты, приходящие с нераспознанными префиксами OUI, отбрасываются.
  - ***Enable (Включено)***. Включение безопасности порта в голосовой сети VLAN.
  - ***Disable (Отключено)***. Отключение безопасности порта в голосовой сети VLAN. Это значение по умолчанию.

Настройка параметров порта

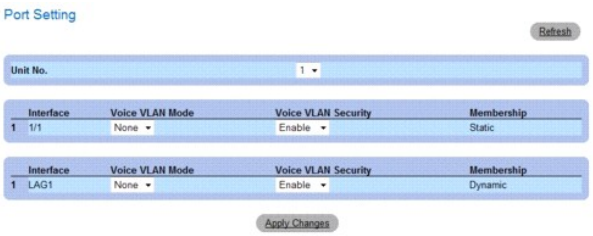
1. Откройте страницу **Voice VLAN Port Settings** (Параметры голосовой сети VLAN для порта).
2. Выберите порт или группу LAG.
3. Выполните необходимые изменения в полях.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Параметры будут изменены, а устройство обновлено.

Отображение таблицы параметров порта

1. Откройте страницу **Voice VLAN Port Settings** (Параметры голосовой сети VLAN для порта).
2. Нажмите кнопку **Show All** (Показать все). Откроется таблица параметров порта.

Рис. 7-64. Таблица параметров голосовой сети VLAN для порта



В таблице параметров голосовой сети VLAN для порта имеется поле **Membership** (Принадлежность), в котором указывается, является элемент голосовой сети VLAN статическим или динамическим. Значение поля Dynamic (Динамическая) означает, что принадлежность VLAN была динамически создана при использовании протокола GARP. Значение поля Static (Статическая) показывает, что принадлежность VLAN определена пользователем.

3. Выберите номер устройства.
4. Выполните необходимые изменения в полях.
5. Нажмите кнопку **Apply Changes** (Применить изменения).

Определение параметров голосовой сети VLAN для порта с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для определения параметров голосовой сети VLAN для порта.

Таблица 7-34. Команды консоли для определения параметров голосовой сети VLAN для порта

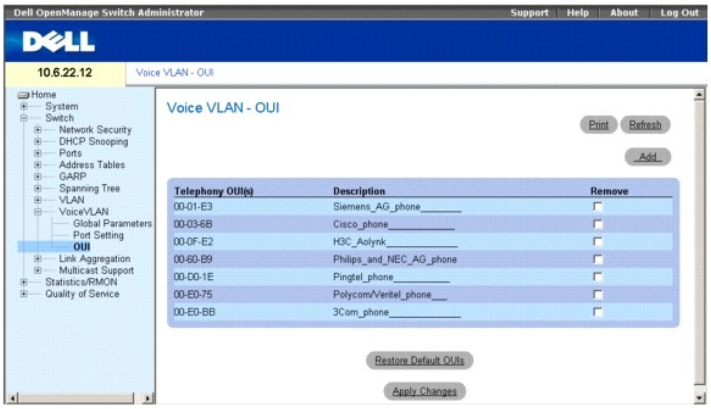
Команда консоли	Описание
voice vlan secure ***no voice vlan secure***	Команда настройки интерфейса voice vlan secure используется для настройки режима безопасности для голосовой сети VLAN. Чтобы отключить режим безопасности, используйте форму no этой команды.

Определение префиксов OUI

На странице **Voice VLAN OUI** (Префикс OUI голосовой сети VLAN) перечисляются уникальные идентификаторы организации (OUI), относящиеся к голосовой сети VLAN. В первых трех байта MAC-адреса содержится идентификатор производителя. В последних трех байтах содержится уникальный идентификатор станции. Используя префиксы OUI, администраторы сети могут добавлять MAC-адреса определенных производителей в таблицу OUI. После добавления префиксов OUI весь трафик, полученный на портах голосовой сети VLAN со специального IP-телефона с указанным OUI, направляется в голосовую сеть VLAN.

Чтобы открыть страницу **Voice VLAN OUI** (Префикс OUI голосовой сети VLAN), щелкните **Switch** (Коммутатор)→ **Voice VLAN** (Голосовая сеть VLAN)→ **OUI** на панели дерева.

Рис. 7-65. Voice VLAN OUI (Префикс OUI голосовой сети VLAN)



- **Telephony OUI(s)** (Телефонные префиксы OUI) - перечислены префиксы OUI, которые в настоящий момент включены в голосовой сети VLAN. Следующие префиксы OUI включены по умолчанию:
  - 00-01-E3 . телефон Siemens AG
  - 00-03-6B . телефон Cisco
  - 00-0F-E2 . устройство H3C Aolynk
  - 00-60-B9 . телефоны Philips и NEC AG
  - 00-D0-1E . телефон Pingtel
  - 00-E0-75 . телефон Polycom/Veritel
  - 00-E0-BB . телефон 3COM
- **Description** (Описание) - предоставляет описание OUI размером до 32 символов.
- **Remove** (Удалить) - когда установлен этот флажок, удаляется префикс OUI из списка Telephony OUI (Телефонные префиксы OUI). Возможные

значения:

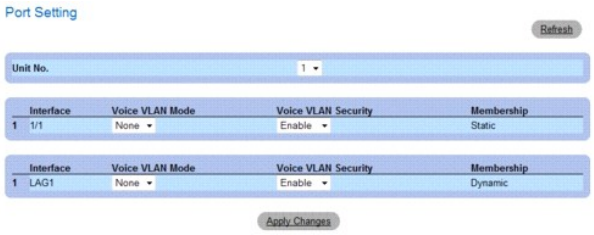
- ***Флажок установлен*** - удаление выбранного префикса OUI.
- ***Флажок снят*** - оставляет текущий префикс OUI в списке Telephony OUI (Телефонные префиксы OUI). Это значение по умолчанию.

- **Restore Default OUIs** (Восстановить значения OUI по умолчанию) - восстанавливает значения OUI по умолчанию.

Добавление префиксов OUI

1. Откройте страницу **Voice VLAN OUI** (Префикс OUI голосовой сети VLAN).
2. Нажмите кнопку **Add** (Добавить). Откроется страница Add OUI (Добавление префикса OUI).

Рис. 7-66. Страница Voice VLAN Add OUI (Префикс OUI голосовой сети VLAN)



3. Заполните поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Добавятся префиксы OUI.

Удаление префиксов OUI

1. Откройте страницу **Voice VLAN OUI** (Префикс OUI голосовой сети VLAN).
2. Установите флажок **Remove** (Удалить) рядом с префиксом OUI, который необходимо удалить.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Выбранные префиксы OUI будут удалены.

Восстановление префиксов OUI по умолчанию

1. Откройте страницу **Voice VLAN OUI** (Префикс OUI голосовой сети VLAN).
2. Щелкните **Restore Default OUIs** (Восстановить значения OUI по умолчанию).

Префиксы OUI по умолчанию будут восстановлены.

Определение префиксов OUI голосовой сети VLAN с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для определения Voice VLAN OUIs (Префиксов OUI голосовой сети VLAN).

Таблица 7-35. Команды консоли для определения префиксов OUI голосовой сети VLAN

Команда консоли	Описание
voice vlan oui-table {add *префикс_mac-адреса* ***[description*** *текст]* ***| remove*** *префикс_mac-адреса}*	Чтобы настроить таблицу префиксов OUI голосовой сети, используйте команду voice vlan oui-table в режиме общей настройки. Чтобы восстановить значение по умолчанию, используйте форму no этой команды.

no voice vlan oui-table	

Объединение портов

Объединение каналов оптимизирует использование портов, связывая между собой группу портов и формируя одну объединенную группу каналов LAG. Объединение портов увеличивает пропускную способность между устройствами, увеличивает гибкость портов и обеспечивает избыточность каналов.

Устройство поддерживает статические группы LAG и группы LAG с протоколом LACP. Группы LAG протокола LACP согласовывают объединенные каналы портов с LACP-портами других устройств. Если порты других устройств также являются LACP-портами, устройства формируют из них группу LAG.

При объединении портов выполняйте следующие инструкции:

- Все порты в группе LAG должны быть одинакового типа.
- VLAN не должна быть настроена для этого порта.
- Порт не должен быть назначен для другой группы LAG.
- Режим автоматического согласования не должен быть настроен для этого порта.
- Порт должен работать в дуплексном режиме.
- Все порты в группе LAG должны иметь одинаковые режимы входного фильтра и пометки.
- Все порты в группе LAG должны иметь одинаковые режимы обратного давления и управления потоком.
- Все порты в группе LAG должны иметь одинаковые приоритеты.
- Все порты в группе LAG должны иметь одинаковые типы трансивера.
- Устройство поддерживает до восьми портов на группу LAG и восьми групп LAG на систему.
- Порты могут быть сконфигурированы как LACP только в том случае, если они не являются частью предварительно настроенной группы LAG.

Порты, добавляемые в группу LAG, теряют индивидуальные настройки. Когда порты удаляются из группы LAG, для них применяются первоначальные настройки.

Устройство использует функцию хеширования, чтобы определить, какие пакеты и по какой части объединенного канала передаются. Функция хеширования выравнивает статическую загрузку на компоненты объединенного канала. Устройство рассматривает объединенный канал как один логический порт.

Объединенные порты можно связать в группы портов объединенного канала. Каждая группа состоит из портов с одинаковой скоростью, работающих в дуплексном режиме.

Порты в группе LAG могут содержать разные типы носителей, если порты работают с одной скоростью. Объединенные каналы можно настроить вручную или автоматически, включив протокол LACP (Link Aggregation Control Protocol) на соответствующих каналах.

В этом разделе имеются следующие тематические подразделы:

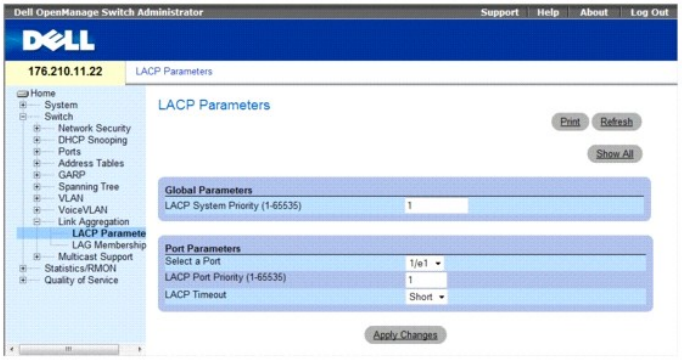
- Определение параметров протокола LACP
- Определение принадлежности к группе LAG

Определение параметров протокола LACP

Страница **LACP Parameters** (Параметры LACP) содержит поля, позволяющие настроить группы LAG по протоколу LACP. Объединенные порты можно связать в группы портов объединенного канала. Каждая группа состоит из портов с одинаковой скоростью. Объединенные каналы можно настроить вручную или установить автоматически, включив протокол LACP (Link Aggregation Control Protocol) на соответствующих каналах.

Чтобы открыть страницу **LACP Parameters** (Параметры LACP), выберите **Switch** (Коммутатор)→ **Link Aggregation** (Объединение каналов)→ **LACP Parameters** (Параметры LACP) на панели дерева.

Рис. 7-67. Страница LACP Parameters (Параметры LACP)



Страница **LACP Parameters** (Параметры LACP) содержит следующие поля:

- **LACP System Priority (1-65535) (Приоритет системы LACP (1-65535))** - значение приоритета LACP для общих параметров. Возможные значения: от 1 до 65535. Значение по умолчанию: 1.
- **Select a Port** (Выбор порта) - номер порта, для которого назначены значения времени ожидания и приоритета.
- **LACP Port Priority (1-65535)** (Приоритет порта LACP (1-65535)) - значение приоритета LACP для порта.
- **LACP Timeout** (Тайм-аут LACP) - административный тайм-аут LACP. Возможные значения:
  - **Short (Короткий)**. Определяет малое время ожидания.
  - **Long (Длинный)**. Определяет большое время ожидания.

Определение общих параметров объединенных каналов

1. Откройте страницу **LACP Parameters** (Параметры LACP).
2. Укажите значение поля **LACP System Priority** (Приоритет системы LACP).
3. Нажмите кнопку **Apply Changes** (Применить изменения).

   Параметры будут определены, а устройство обновлено.

Определение параметров портов объединенного канала

1. Откройте страницу **LACP Parameters** (Параметры LACP).
2. Введите значения в полях в области **Port Parameters** (Параметры порта).
3. Нажмите кнопку **Apply Changes** (Применить изменения).

   Параметры будут определены, а устройство обновлено.

Отображение таблицы параметров LACP

1. Откройте страницу **LACP Parameters** (Параметры LACP).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется таблица параметров LACP Parameters Table.

   Рис. 7-68. Таблица параметров LACP

Настройка параметров LACP с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для настройки параметров LACP, как показано на странице **LACP Parameters** (Параметры LACP).

Таблица 7-36. Команды консоли для настройки параметров LACP

Команда консоли	Описание
lacp system-priority *значение*	Настраивает приоритет системы.
lacp port-priority *значение*	Настраивает приоритет физических портов.
lacp timeout {**long** | **short**}	Задает административный тайм-аут LACP.
show lacp ethernet *интерфейс* [**parameters** | **statistics** | **protocol-state**]	Отображает информацию о протоколе LACP для порта Ethernet.

Далее приведен пример команд консоли.

```
Console (config)# lacp system-priority 120

Console (config)# interface ethernet 1/e11

Console (config-if)# lacp port-priority 247

Console (config-if)# lacp timeout long

Console(config-if)# end

Console# show lacp ethernet 1/e11 statistics

Port 1/e11 LACP Statistics:

LACP PDUs sent:2

LACP PDUs received:2
```

Определение принадлежности к группе LAG

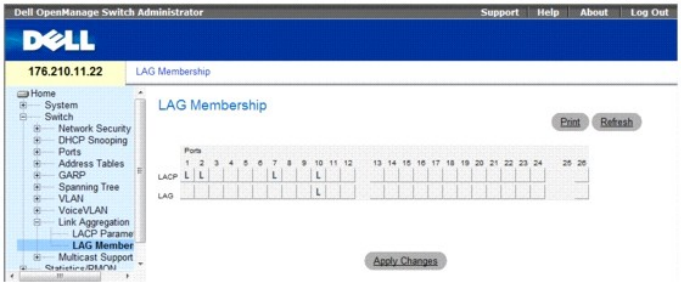
Устройство поддерживает 15 групп LAG на систему и 8 портов на каждую группу LAG, независимо от того, является ли устройство автономным или работает в стеке.

Если порт добавляется в группу LAG, он принимает все ее свойства. Если порт не может быть настроен параметрами LAG, то он не добавляется в группу LAG. В таком случае выдается сообщение об ошибке. Однако, если первый порт, который присоединяется к группе LAG, не может быть настроен с помощью ее параметров, то этот порт будет добавлен в группу LAG, но с установками по умолчанию. В таком случае выдается сообщение об ошибке. Однако, если этот порт является единственным портом в группе LAG, тогда группа будет работать с использованием параметров этого порта, а не определенных заранее параметров группы.

Используйте страницу **LAG Membership** (Членство в LAG) для назначения портов для группы LAG.

Чтобы открыть страницу **LAG Membership** (Принадлежность LAG), выберите **Switch** (Коммутатор)→ **Link Aggregation** (Объединение каналов)→ **LAG Membership** (Принадлежность LAG) на панели дерева.

Рис. 7-69. Страница LAG Membership (Принадлежность LAG)



Страница **LAG Membership** (Принадлежность VLAN) содержит следующие поля:

- **LACP** - добавляет порт в группу LAG, используя протокол LACP.
- **LAG** - добавляет порт в группу LAG и указывает LAG, к которой принадлежит порт.

Добавление портов в LAG или LACP

1. Откройте страницу **LAG Membership** (Принадлежность LAG).
2. В строке LAG (вторая строка) переключите кнопку на определенный номер, чтобы добавить или удалить порт из этого номера LAG.
3. В строке LACP (первая строка) переключите кнопку под номером порта, чтобы назначить либо LACP, либо статическую группу LAG.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Порт будет добавлен в группу LAG или LACP, а устройство обновлено.

Включение портов в группы LAG с помощью команд консоли

В следующей таблице приведены команды консоли, соответствующие полям для включения портов в группы LAG на странице **LAG Membership** (Принадлежность LAG).

Таблица 7-37. Команды консоли для определения принадлежности LAG

Команда консоли	Описание
channel-group номер_канала_порта mode {on | auto} { | }	Связывает порт с каналом порта. Для удаления конфигурации группы канала из интерфейса используйте форму по этой команды.
show interfaces port-channel *[номер_канала_порта]*	Отображает информацию о канале порта.

Далее приведен пример команд консоли.

```
console(config)# interface ethernet 1/e11

console(config-if)# channel-group 1 mode on
```

Поддержка пересылки многоадресного трафика

Пересылка многоадресного трафика позволяет пересылать один пакет по нескольким адресам. Служба многоадресной пересылки уровня 2 основана на устройстве уровня 2, который получает один пакет, адресованный определенным адресам многоадресной передачи. Она создает копии пакета и передает их на соответствующие порты.

- **Registered Multicast traffic (Зарегистрированный многоадресный трафик)**. Если обнаруживается трафик, адресованный зарегистрированной группе многоадресной передачи, он обрабатывается в зависимости от записей базы данных фильтрации многоадресного трафика, и переадресовывается на зарегистрированные порты.
- **Unregistered Multicast traffic (Незарегистрированный многоадресный трафик)**. Если обнаруживается трафик, адресованный незарегистрированной группе многоадресной передачи, он обрабатывается в зависимости от записей базы данных фильтрации многоадресного трафика. Установка по умолчанию для этого параметра - маршрутизация всего трафика (трафик в незарегистрированные группы).

Устройство поддерживает:

- **Forwarding L2 Multicast Packets** (Пересылка многоадресных пакетов L2) - включает пересылку многоадресных пакетов Layer 2. Фильтрация многоадресной рассылки Layer 2 включена по умолчанию и не настраивается пользователем.

Система поддерживает фильтр многоадресной рассылки для 256 групп многоадресной рассылки.

- **Filtering L2 Multicast Packets** (Фильтрация многоадресных пакетов L2) - включает пересылку пакетов Layer 2 на интерфейсы. Если фильтрация многоадресного трафика отключена, многоадресные пакеты «лавиной» рассылаются на все соответствующие порты.

Чтобы открыть страницу **Multicast Support** (Поддержка многоадресного трафика), выберите **Switch** (Коммутатор)→ **Multicast Support** (Поддержка многоадресного трафика) на панели дерева.

В этом разделе имеются следующие тематические подразделы:

- Определение общих параметров многоадресной передачи
- Добавление записей адресов многоадресной передачи моста
- Назначение параметров многоадресной пересылки всем
- Наблюдение по протоколу IGMP

Определение общих параметров многоадресной передачи

Переключение Layer 2 пересылает многоадресные пакеты на все соответствующие порты VLAN по умолчанию, при этом пакет рассматривается как одна многоадресная передача. Пересылка многоадресного трафика является эффективной, но не оптимальной, поскольку и несоответствующие порты получают пакеты многоадресной рассылки. Избыточные пакеты вызывают увеличение сетевого трафика. Фильтр многоадресной пересылки позволяет выполнять пересылку пакетов Layer 2 на набор портов.

Когда наблюдение на базе IGMP включено глобально для всей системы, все пакеты IGMP отправляются на процессор. Процессор анализирует входящие пакеты и определяет следующее:

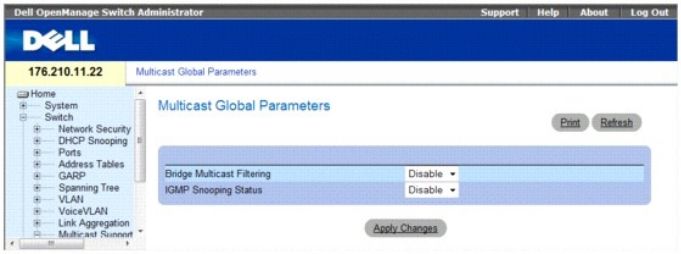
- Какие порты подключаются к какой из многоадресных групп.
- Какие порты имеют многоадресные маршрутизаторы, которые генерируют запросы IGMP.
- Какие протоколы маршрутизации переадресовывают пакеты и многоадресный трафик.

Порты, запрашивающие добавление в определенную группу многоадресной передачи, выдают отчет IGMP, в котором указано, что группа многоадресной передачи принимает записи. В результате этого создается база данных фильтров многоадресной передачи.

Страница **Global Parameters** (Общие параметры) содержит поля для включения отслеживания протокола IGMP на устройстве.

Чтобы открыть страницу **Global Parameters** (Общие параметры), выберите **Switch** (Протокол)→ **Multicast Support** (Поддержка многоадресного трафика)→ **Global Parameters** (Общие параметры) на панели дерева.

Рис. 7-70. Страница Global Parameters (Общие параметры)



Страница **Global Parameters** (Общие параметры) содержит следующие поля:

- **Bridge Multicast Filtering** (Фильтрация многоадресного трафика через мост) - включает или отключает фильтрацию многоадресного трафика через мост. Значение по умолчанию: отключено.
  - **Enable (Включено)**. Включает фильтрацию многоадресного трафика через мост.
  - **Disable (Выключено)**. Выключает фильтрацию многоадресного трафика через мост.
- **IGMP Snooping Status** (Состояние наблюдения по протоколу IGMP) - включает или отключает наблюдение по протоколу IGMP на устройстве. Значение по умолчанию: отключено. Наблюдение по протоколу IGMP может быть включено только в том случае, если включены **Global Parameters** (Общие параметры).
  - Enable (Включено). Включает наблюдение по протоколу IGMP.
  - Disable (Выключено) . Выключает наблюдение по протоколу IGMP.

Включение на устройстве фильтрации многоадресного трафика через мост

1. Откройте страницу **Global Parameters** (Общие параметры).
2. Выберите **Enable** (Включено) в поле **Bridge Multicast Filtering** (Фильтрация многоадресного трафика через мост).

3. Нажмите кнопку **Apply Changes** (Применить изменения).

   Фильтрация многоадресного трафика через мост включена.

Включение на устройстве наблюдения на базе IGMP

1. Откройте страницу **Global Parameters** (Общие параметры).
2. Выберите **Enable** (Включено) в поле **IGMP Snooping Status** (Состояние наблюдения на базе IGMP).
3. Нажмите кнопку **Apply Changes** (Применить изменения).

   Наблюдение на базе IGMP будет включено на этом устройстве.

Включение фильтрации многоадресного трафика и наблюдения на базе IGMP с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для включения фильтрации многоадресного трафика и наблюдения на базе IGMP, как показано на странице **Global Parameters** (Общие параметры).

Таблица 7-38. Команды консоли для включения фильтрации многоадресного трафика и наблюдения на базе IGMP

Команда консоли	Описание
bridge multicast filtering	Включает фильтрацию многоадресных адресов.
ip igmp snooping	Включает наблюдение по протоколу IGMP.

Далее приведен пример команд консоли.

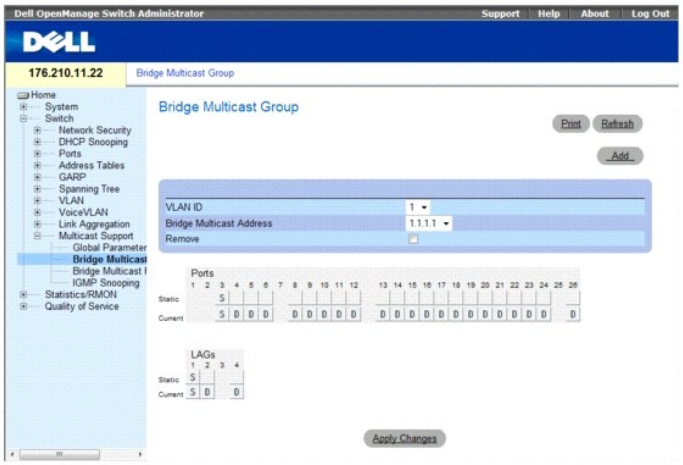
```
console(config)# bridge multicast filtering

console(config)# ip igmp snooping
```

Добавление записей адресов многоадресной передачи моста

На странице **Bridge Multicast Group** (Группа многоадресной передачи моста) показаны порты и группы LAG, связанные с группой службы многоадресной передачи, в таблицах **Ports** (Порт) и **LAG**. Таблицы Port и LAG также отражают принцип добавления порта или LAG в группу многоадресной передачи. Порты можно добавлять в существующую группу или в новые группы службы многоадресной передачи. Страница **Bridge Multicast Group** (Группа многоадресной передачи моста) позволяет создавать новые группы службы многоадресной передачи. На странице **Bridge Multicast Group** (Группа многоадресной передачи моста) также можно присвоить порты определенной группе многоадресной передачи.

Чтобы открыть страницу **Bridge Multicast Group** (Группа многоадресной передачи моста), выберите **Switch** (Коммутатор)→ **Multicast Support** (Поддержка многоадресного трафика)→ **Bridge Multicast Group** (Группа многоадресной передачи моста) на панели дерева.

Рис. 7-71. Страница Bridge Multicast Group (Группа многоадресной передачи моста)



Страница **Bridge Multicast Group** (Группа многоадресной передачи моста) содержит следующие поля:

- **VLAN ID (Идентификатор VLAN)**. Определяет VLAN и содержит информацию об адресе группы многоадресной передачи.
- **Bridge Multicast Address(Адрес многоадресной передачи моста)**. Идентифицирует MAC/IP-адрес группы многоадресной передачи.
- **Remove (Удалить)**. Удаление адреса многоадресной передачи моста.
  - **Флажок установлен**. Удаляет адрес многоадресной передачи моста.
  - **Флажок снят**. Оставляет адрес многоадресной передачи моста.
- **Ports (Порты)**. Порты, которые можно добавить в службу многоадресной передачи.
- **LAGs (Группы LAG)**. Группы LAG, которые можно добавить в службу многоадресной передачи.

В следующей таблице приведены параметры управления записями портов и групп LAG для IGMP:

Таблица 7-39. Параметры управления таблицей записей портов/LAG для IGMP

Управление портом	Описание
D	Показывает, что порт/группа LAG добавлена в группу многоадресной передачи динамически в строке *Current* (Текущий).
S	Связывает порт с многоадресной группой в качестве статического члена в строке *Static* (Статический). Порт/группа LAG присоединена к многоадресной группе статически в строке *Current* (Текущий).
F	Запрещено.
Пусто	Порт не связан с группой многоадресной передачи.

Добавление адресов многоадресной передачи моста

1. Откройте страницу **Bridge Multicast Group** (Группа многоадресной передачи моста).
2. Нажмите кнопку **Add** (Добавить).

   Откроется страница **Add Bridge Multicast Group** (Добавление группы многоадресной передачи моста).

   Рис. 7-72. Страница Add Bridge Multicast Group (Добавление группы многоадресной передачи моста)

3. Определите поля **VLAN ID** (Идентификатор VLAN) и **New Bridge Multicast Address** (Новый адрес многоадресной передачи моста).
4. Переключите порт на значение **S**, чтобы добавить его в выбранную группу многоадресной передачи.
5. Переключите порт на значение **F**, чтобы запретить добавление определенных адресов многоадресной передачи для определенного порта.
6. Нажмите кнопку **Apply Changes** (Применить изменения).

   Адрес многоадресной передачи моста будет добавлен в многоадресную группу, а устройство обновлено.

Определение портов для получения службы многоадресной пересылки

1. Откройте страницу **Bridge Multicast Group** (Группа многоадресной передачи моста).

2. Определите поля **VLAN ID** (Идентификатор VLAN) и **Bridge Multicast Address** (Адрес многоадресной передачи моста).
3. Переключите порт на значение **S**, чтобы добавить его в выбранную группу многоадресной передачи.
4. Переключите порт на значение **F**, чтобы запретить добавление определенных адресов многоадресной передачи для определенного порта.
5. Нажмите кнопку **Apply Changes** (Применить изменения).

   Порт будет назначен в группу многоадресной передачи, а устройство обновлено.

Назначение групп LAG для получения службы многоадресной пересылки

1. Откройте страницу **Bridge Multicast Group** (Группа многоадресной передачи моста).
2. Определите поля **VLAN ID** (Идентификатор VLAN) и **Bridge Multicast Address** (Адрес многоадресной передачи моста).
3. Переключите LAG на значение **S**, чтобы добавить его в выбранную группу многоадресной передачи.
4. Переключите LAG на значение **F**, чтобы запретить добавление определенных адресов многоадресной передачи для определенной группы LAG.
5. Нажмите кнопку **Apply Changes** (Применить изменения).

   Группа LAG будет назначена в группу многоадресной передачи, а устройство обновлено.

Управление записями службы многоадресной пересылки с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для управления записями службы многоадресной пересылки, как показано на странице **Bridge Multicast Group** (Группа многоадресной передачи моста).

Таблица 7-40. Команды консоли для управления записями службы многоадресной пересылки

Команда консоли	**Описание**
bridge multicast address {*mac_адрес_многоадресной_передачи* | *ip_адрес_многоадресной_передачи*}	Регистрирует адреса для многоадресной передачи на уровне MAC-адресов для таблицы мостов и добавляет в группу статические порты.
bridge multicast forbidden address {*mac_адрес_многоадресной_передачи* | *ip_адрес_многоадресной_передачи*}[**add** | **remove**] {**ethernet** *список_интерфейсов* | **port-channel** *список_номеров_каналов_портов*}	Запрещает добавление определенного адреса многоадресной передачи для определенных портов. Для возврата к значениям по умолчанию используйте форму no этой команды
show bridge multicast address-table [**vlan** *vlan-id*] [**address** {*mac-multicast-address* | *ip-multicast-address*}] [**format ip** | **mac**]	Отображает информацию таблицы MAC-адресов для многоадресной передачи.

Далее приведен пример команд консоли.

```
Console (config-if)# bridge multicast address 0100.5e02.0203

add ethernet 1/e11,1/e12

console(config-if)# end

console # show bridge multicast address-table
```

Vlan	MAC Address	Type	Ports
----	-----------	-----	----------
1	0100.5e02.0203	static	1/e11, 1/e12
19	0100.5e02.0208	static	1/e11-16
19	0100.5e02.0208	dynamic	1/e11-12
Forbidden ports for multicast addresses:			
Vlan	MAC Address	Ports	
----	-----------	----------	
1	0100.5e02.0203	1/e8	
19	0100.5e02.0208	1/e8	

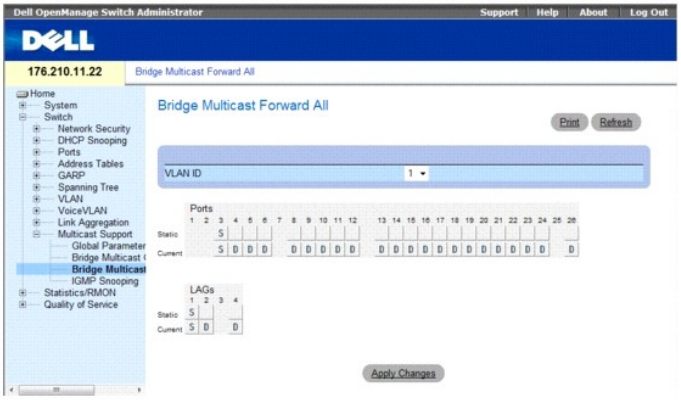
console # **show bridge multicast address-table format ip**			
Vlan	IP Address	Type	Ports
----	----------	-----	----------
1	224-239.130|2.2.3	static	1/e11, 1/e12
19	224-239.130|2.2.8	static	1/e11-16
19	224-239.130|2.2.8	dynamic	1/e11-12
Forbidden ports for multicast addresses:			
Vlan	IP Address	Ports	
----	----------	----------	
1	224-239.130|2.2.3	1/e8	
19	224-239.130|2.2.8	1/e8	

Назначение параметров многоадресной пересылки всем

Страница **Bridge Multicast Forward All** (Многоадресная передача моста всем) позволяет включить привязку портов или групп LAG к устройству, связанному с соседним маршрутизатором или коммутатором для многоадресной пересылки. После того как наблюдение по протоколу IGMP включено, многоадресные пакеты пересылаются соответствующему порту или группе VLAN.

Чтобы открыть страницу **Bridge Multicast Forward All**, выберите **Switch** (Коммутатор)→ **Multicast Support** (Поддержка многоадресного трафика)→ **Bridge Multicast Forward All** (Многоадресная передача моста всем) на панели дерева.

Рис. 7-73. Страница Bridge Multicast Forward All (Многоадресная передача моста всем)



Страница **Bridge Multicast Forward All** (Многоадресная передача моста всем) содержит следующие поля:

- **VLAN ID** (Идентификатор VLAN) - определяет VLAN.
- **Ports** (Порты) - порты, которые можно добавить в службу многоадресной передачи.
- **LAGs** (Группы LAG) - группы LAG, которые можно добавить в службу многоадресной передачи.

В таблице **Bridge Multicast Forward All Router / Port Control Settings Table** (Таблица параметров управления коммутатором/портами для многоадресной передачи моста всем) приведены параметры управления настройками маршрутизатора и портов.

Управление таблицей параметров управления коммутатором / портами для многоадресной передачи моста всем

В следующей mf,kbwt приведены параметры, используемые для установки портов.

Таблица 7-41. Таблица параметров управления коммутатором / портами для многоадресной передачи моста всем

Управление портом	Описание
D	Связывает порт с многоадресным маршрутизатором или коммутатором как динамический порт.
S	Связывает порт с многоадресным маршрутизатором или коммутатором как статический порт.
F	Запрещено.
Пусто	Порт не подключен к маршрутизатору или коммутатору многоадресной передачи.

Привязка порта к маршрутизатору или коммутатору многоадресной передачи

1. Откройте страницу **Bridge Multicast Forward All** (Многоадресная передача моста всем).
2. Определите поле **VLAN ID** (Идентификатор VLAN).
3. Выберите порт в таблице **Ports** (Порты) и назначьте значение для порта.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Порт не подключен к маршрутизатору или коммутатору многоадресной передачи.

Привязка группы LAG к маршрутизатору или коммутатору многоадресной передачи

1. Откройте страницу **Bridge Multicast Forward All** (Многоадресная передача моста всем).
2. Определите поле **VLAN ID** (Идентификатор VLAN).
3. Выберите порт в таблице **LAGs** (Группы LAG) и укажите значение LAG.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Группа LAG привязывается к маршрутизатору или коммутатору многоадресной передачи.

Управление группами LAG и портами, связанными с маршрутизаторами многоадресной передачи с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для управления группами LAG и портами, привязанными к маршрутизаторам многоадресной передачи, как показано на странице **Bridge Multicast Forward All** (Многоадресная передача моста всем).

Таблица 7-42. Команды консоли для управления группами LAG и портами, привязанными к маршрутизаторам многоадресной передачи

Команда консоли	Описание
show bridge multicast filtering *идентификатор_vlan*	Отображает настройку фильтра многоадресной передачи.
bridge multicast forward-all {**add** | **remove**} {**ethernet** *список_интерфейсов* | **port-channel** *список_номеров_каналов_портов*}	Разрешает пересылку всех многоадресных пакетов для порта. Для возврата к значениям по умолчанию используйте форму no этой команды

Далее приведен пример команд консоли.

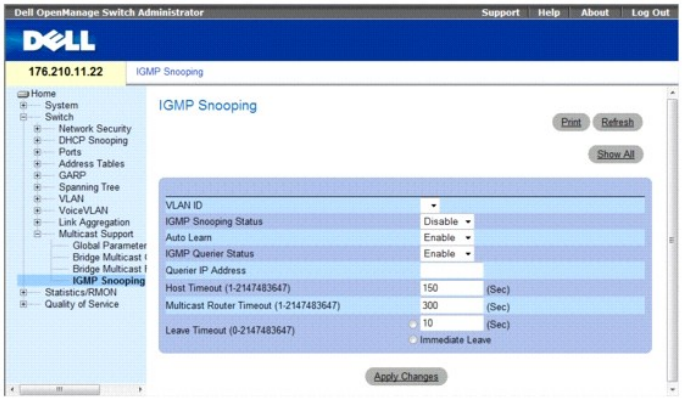
```
Console(config)# interface vlan 1

Console(config-if)# bridge multicast forward-all add ethernet 1/e3

Console(config-if)# end

Console# show bridge multicast filtering 1
```

```
Filtering: Enabled

VLAN:    Forward-All
Port     Static            Status
-------  ----------------  -----------
1/e11    Forbidden         Filter
1/e12    Forward           Forward(s)
1/e13    -                 Forward(d)
```

Наблюдение по протоколу IGMP

Страница **IGMP Snooping** (Наблюдение по протоколу IGMP) содержит поля для добавления записей IGMP. Чтобы открыть страницу **IGMP Snooping** (Наблюдение по протоколу IGMP), выберите **Switch** (Коммутатор)→ **Multicast Support** (Поддержка многоадресного трафика)→ **IGMP Snooping** (Наблюдение по протоколу IGMP) на панели дерева.

Рис. 7-74. Страница IGMP Snooping (Наблюдение по протоколу IGMP)



- **VLAN ID** (Идентификатор сети VLAN) - указывает идентификатор VLAN.
- **IGMP Snooping Status** (Состояние наблюдения по протоколу IGMP) - включает или отключает наблюдение по протоколу IGMP для VLAN.
- **Auto Learn** (Автоматическое распознавание) - включает или отключает автоматическое распознавание на устройстве.
- **IGMP Querier Status** (Состояние опрашивающего устройства IGMP) - включает или отключает опрашивающее устройство IGMP. Опрашивающее устройство IGMP имитирует работу маршрутизатора многоадресной передачи, обеспечивая отслеживание многоадресного домена Layer 2 даже при отсутствии маршрутизатора многоадресной передачи.
- **Querier IP Address** (IP-адрес опрашивающего устройства) - IP-адрес опрашивающего устройства. Используется, чтобы назначить использование адреса IP-интерфейса сети VLAN или определить уникальный IP-адрес, который будет использоваться в качестве адреса источника опрашивающего устройства.
- **Host Timeout (1-2147483647)** (Время ожидания хоста) - время, по истечении которого запись наблюдения по протоколу IGMP устаревает. Значение по умолчанию: 260 секунд.
- **Multicast Router Timeout (1-2147483647)** (Время ожидания многоадресного маршрутизатора) - время, по истечении которого запись многоадресного маршрутизатора устаревает. Значение по умолчанию: 300 секунд.
- **Leave Timeout (0-2147483647)** (Время старения) - время в секундах после получения сообщения портом и до истечения срока хранения. **User-defined** (Определено пользователем) позволяет определить интервал времени ожидания, а **Immediate Leave** (Немедленно) определяет время ожидания немедленного выхода. Значение по умолчанию: 10 секунд.

Включение на устройстве наблюдения на базе IGMP

1. Откройте страницу **IGMP Snooping** (Наблюдение по протоколу IGMP).
2. Выберите идентификатор VLAN для устройства, на котором будет включено наблюдение на базе протокола IGMP.
3. Выберите **Enable** (Включено) в поле **IGMP Snooping Status** (Состояние наблюдения на базе IGMP).
4. Заполните поля на этой странице.
5. Нажмите кнопку **Apply Changes** (Применить изменения).

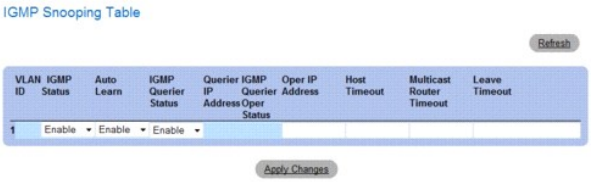
   Наблюдение на базе IGMP будет включено на этом устройстве.

Отображение таблицы наблюдения по протоколу IGMP

1. Откройте страницу **IGMP Snooping** (Наблюдение по протоколу IGMP).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **IGMP Snooping Table** (Таблица наблюдения по протоколу IGMP).

Рис. 7-75. Таблица наблюдения по протоколу IGMP



Настройка наблюдения по протоколу IGMP с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для настройки на устройстве IGMP Snooping (Наблюдение по протоколу IGMP):

Таблица 7-43. Команды консоли для настройки наблюдения по протоколу IGMP

Команда консоли	**Описание**
ip igmp snooping	Включает наблюдение по протоколу IGMP.
ip igmp snooping mrouter learn-pim-dvmrp	Включает автоматическое распознавание портов многоадресного маршрутизатора в контексте определенной VLAN.
ip igmp snooping host-time-out количество_секунд	Настраивает время ожидания хоста.
ip igmp snooping mrouter-time-out количество_секунд	Настраивает время ожидания маршрутизатора.
ip igmp snooping leave-time-out { | *immediate-leave*}	Настраивает время старения хоста.
ip igmp snooping querier enable no ip igmp snooping querier enable	Включает опрашивающее устройство, использующее протокол управления группами Интернета (Internet Group Management Protocol (IGMP)) в конкретной VLAN. Чтобы отключить устройство, используйте форму no этой команды.
ip igmp snooping querier address *ip-адрес* no ip igmp snooping querier address	Определяет IP-адрес источника, который должен использоваться опрашивающим устройством, выполняющим наблюдение на базе протокола IGMP. Для возврата к значениям по умолчанию используйте форму no этой команды
show ip igmp snooping groups [vlan] [address *идентификатор_vlanip_адрес_многоадресной_передачи*]	Отображает группы многоадресной передачи, полученные во время наблюдения по протоколу IGMP.
show ip igmp snooping interface *идентификатор_vlan*	Отображает конфигурацию наблюдения по протоколу IGMP.
show ip igmp snooping mrouter [**interface** *идентификатор_vlan*]	Отображает информацию о динамически распознаваемых интерфейсах многоадресного маршрутизатора.

Далее приведен пример команд консоли.

```
Console> enable

Console# config

Console (config)# ip igmp snooping

Console (config)# interface vlan 1

Console (config-if)# ip igmp snooping mrouter learn-pim-dvmrp

Console (config-if)# ip igmp snooping host-time-out 300

Console (config-if)# ip igmp snooping mrouter-time-out 200

Console (config-if)# exit

Console (config)# interface vlan 1

Console (config-if)# ip igmp snooping leave-time-out 60

Console (config-if)# exit

Console (config)# exit

Console # show ip igmp snooping groups

Vlan IP Address Querier Ports

----- ------------------ -------- -----
```

```
1 224-239.130|2.2.3 Yes g1, g2



Console # show ip igmp snooping interface 1000

IGMP Snooping is globally enabled


IGMP Snooping admin: Enabled

Hosts and routers IGMP version: 2

IGMP snooping oper mode: Enabled

IGMP snooping querier admin: Enabled

IGMP snooping querier oper: Enabled

IGMP snooping querier address admin:

IGMP snooping querier address oper: 172.16.1.1

IGMP snooping querier version admin: 3

IGMP snooping querier version oper: 2




IGMP host timeout is 300 sec

IGMP Immediate leave is disabled. IGMP leave timeout is 10 sec

IGMP mrouter timeout is 300 sec

Automatic learning of multicast router ports is enabled




Console # show ip igmp snooping mrouter
```

VLAN	Ports
----	------
1	g1

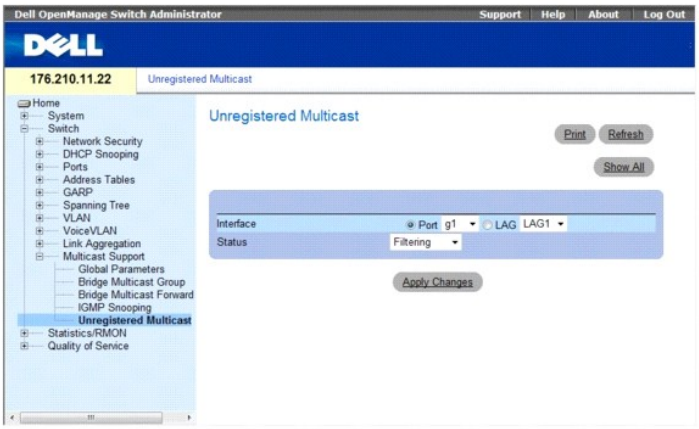
Незарегистрированная групповая передача

Кадры групповой (многоадресной) передачи обычно направляются на все порты VLAN. Если включен режим наблюдения по протоколу (IGMP Snooping), устройство получает информацию о наличии групп многоадресной передачи и проверяет, какие порты присоединились к этой группе многоадресной передачи. Группы многоадресной передачи могут также быть задействованы в статическом режиме. Это позволяет устройству направлять кадры многоадресной передачи (от зарегистрированной группы многоадресной передачи) только к портам, которые зарегистрированы в этой группе.

Страница **Unregistered Multicast** (Незарегистрированная многоадресная передача) содержит поля, которые предназначены для обработки кадров передачи, принадлежащих к незарегистрированным группам многоадресной передачи. Незарегистрированные группы многоадресной передачи - это группы, которые пока «неизвестны» устройству. Все кадры незарегистрированных групп по прежнему направляются на все порты VLAN. После установки для порта функции переадресации / фильтрации, конфигурация этого порта становится действительной для любой VLAN, членом которой он является (или будет являться).

Чтобы открыть страницу **Unregistered Multicast** (Незарегистрированная многоадресная передача), выберите **Switch** (Коммутатор)→ **Multicast Support** (Поддержка многоадресного трафика)→ **Unregistered Multicast** (Незарегистрированная многоадресная передача)на панели дерева.

Рис. 7-76. Незарегистрированная многоадресная передача



- **Interface (Интерфейс)**. Позволяет осуществить выбор порта или группы LAG.
- **Status (Состояние)**. Указывает состояние переадресации для выбранного интерфейса. Возможные значения:
  - **Forwarding (Переадресация)**. Обеспечивает переадресацию кадров незарегистрированного многоадресного трафика на указанный порт или канал порта. Это значение по умолчанию.
  - **Filtering (Фильтрация)**. Обеспечивает отфильтровывание кадров незарегистрированного многоадресного трафика выбранного интерфейса VLAN.

Установки состояния незарегистрированного многоадресного трафика интерфейса

1. Откройте страницу **Unregistered Multicast** (Незарегистрированная многоадресная передача).
2. Выберите интерфейс, для которого необходимо установить незарегистрированный многоадресный трафик.
3. В поле **Status** (Состояние) выберите состояние.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Состояние незарегистрированного многоадресного трафика установлено.

Отображается таблица незарегистрированного многоадресного трафика (Unregistered Multicast Table)

1. Откройте страницу **Unregistered Multicast** (Незарегистрированная многоадресная передача).
2. Нажмите кнопку **Show All** (Показать все).

   Отображается таблица незарегистрированного многоадресного трафика (Unregistered Multicast Table)

Рис. 7-77. Таблица незарегистрированного многоадресного трафика

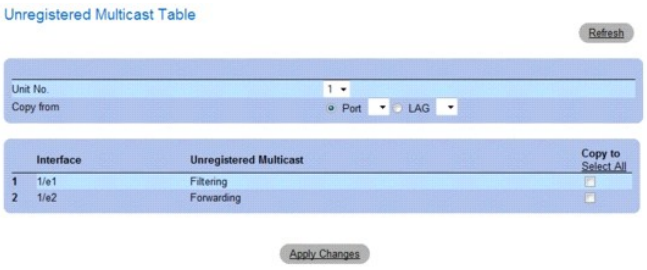


Таблица **Unregistered Multicast Table** (Таблица незарегистрированного многоадресного трафик) имеет следующие дополнительные поля:

- **Unit No. (Номер устройства)**. Выбор номера устройства стека.
- **Copy from (Копировать из)**. Копирует параметры из выбранного элемента.

Копирование установок незарегистрированного многоадресного с одного интерфейса на другой

1. Откройте страницу **Unregistered Multicast** (Незарегистрированная многоадресная передача).
2. Нажмите кнопку **Show All** (Показать все). Отображается таблица незарегистрированного многоадресного трафика (Unregistered Multicast Table)
3. Выберите интерфейс, из которого необходимо копировать параметры, в поле **Copy Parameters from** (Копировать параметры из).
4. Для каждого из интерфейсов, в который вы хотите скопировать параметры, установите галочку в клетке поля **Copy to** (Копировать в). В противном случае, выберите **Select All** (Выбрать все) для автоматического выбора всех интерфейсов.
5. Нажмите кнопку **Apply Changes** (Применить изменения).

   Параметры незарегистрированного многоадресного трафика скопированы с одного интерфейса на другой.

Настройка незарегистрированного многоадресного трафика командами консоли

В следующей таблице приведены эквивалентные команды консоли для настройки незарегистрированного многоадресного трафика на устройстве:

Таблица 7-44. Команды консоли для незарегистрированного многоадресного трафика

Команда консоли	Описание
bridge multicast unregistered (Незарегистрированная мостовая многоадресная передача)	Настраивает состояние переадресации незарегистрированных адресов многоадресного трафика.
show bridge multicast unregistered (Показать незарегистрированные мостовые передачи)	Отображает настройку фильтра незарегистрированной мостовой передачи.

Далее приведен пример команд консоли.

```
Console # show bridge multicast unregistered



Port Unregistered (незарегистрированный порт)

---- -------------

1/1   Forward

1/2   Filter

1/3   Filter
```

Назад на страницу Содержание

Назад на страницу Содержание

Просмотр статистики

Руководство пользователя систем Dell™ PowerConnect™ 35xx

- Просмотр таблиц
- Просмотр статистики удаленного мониторинга
- Просмотр диаграмм

На страницах **статистики** приведены ссылки на информацию для интерфейса, GVRP, Etherlike, RMON и использования устройства. Чтобы открыть страницу **статистики**, щелкните **Statistics** (Статистика) на панели дерева.

Команды CLI доступны не для всех страниц статистики.

Просмотр таблиц

Страница **Table Views** (Просмотр в виде таблиц) содержит ссылки для отображения статистики в табличном виде. Чтобы открыть страницу, щелкните **Statistics** (Статистика)→ **Table** (Таблица) на панели дерева.

В этом разделе имеются следующие тематические подразделы:

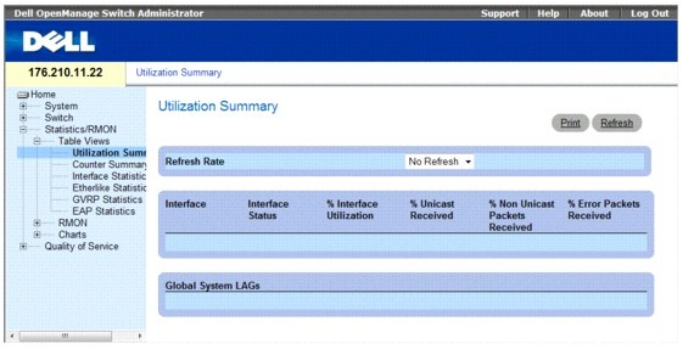
- Просмотр общих сведений по использованию
- Просмотр сводки по счетчикам
- Просмотр статистики интерфейса
- Просмотр статистики Etherlike
- Просмотр статистики протокола GVRP
- Просмотр статистики EAP
- Просмотр статистики протокола EAP с помощью команд консоли

Просмотр общих сведений по использованию

Страница Utilization Summary (Общие сведения по использованию) содержит статистику по использованию интерфейса. Это окно периодически обновляется в целях минимизации влияния на компьютеры с малым объемом памяти. В течение этого периода изображение на дисплее может искажаться.

Чтобы открыть страницу, щелкните **Statistics** (Статистика)→ **Table Views** (Просмотр в виде таблиц)→ **Utilization Summary** (Общие сведения по использованию) на панели дерева.

Рис. 8-1. Utilization Summary (Общие сведения по использованию)



Страница Utilization Summary (Общие сведения по использованию) содержит следующие поля:

- **Refresh Rate (Частота обновления)**. Период времени между обновлениями статистики интерфейса. Возможные значения:
  - **15 с**. Статистика интерфейса обновляется каждые 15 секунд.
  - **30 с**. Статистика интерфейса обновляется каждые 30 секунд.
  - **60 с**. Статистика интерфейса обновляется каждые 60 секунд.
  - **No Refresh (Нет обновления)**. Автоматическое обновление статистики интерфейса не происходит.

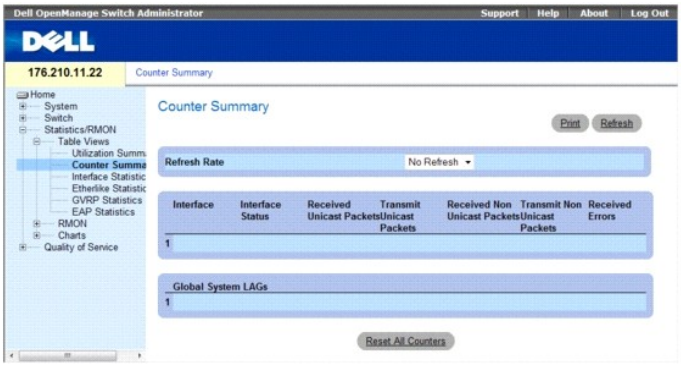
- **Interface (Интерфейс)**. Номер интерфейса.
- **Interface Status (Состояние интерфейса)**. Состояние интерфейса.
- **% Interface Utilization (% использования интерфейса)**. Процент использования сетевого интерфейса на основе дуплексного режима интерфейса. Диапазон значений этого параметра составляет от 0 до 200 %. Максимальное значение 200% для дуплексного соединения показывает, что полоса пропускания входящих и исходящих соединений на 100% используется трафиком, проходящим через интерфейс. Максимальное значение для полудуплексного соединения составляет 100%.
- **% Unicast Received (% полученных одноадресных пакетов)**. Процент полученных на интерфейс одноадресных пакетов.
- **% Non Unicast Packets Received (% полученных многоадресных пакетов)**. Процент полученных на интерфейс многоадресных пакетов.
- **% Error Packets Received (% полученных пакетов с ошибками)**. Процентное количество пакетов с ошибками, полученных на интерфейс.
- **Global System LAGs (Общие системные группы LAG)**. Указывает на текущее применение LAG.

Просмотр сводки по счетчикам

Страница Counter Summary (Сводка по счетчикам) содержит статистику по использованию порта в числовых суммах, а не в процентах.

Чтобы открыть страницу Counter Summary (Сводка по счетчикам) нажмите **Statistics/RMON** (Статистика/RMON)→ **Table Views** (Просмотр в виде таблиц)→ **Counter Summary** (Сводка по счетчикам) на панели дерева.

Рис. 8-2. Counter Summary (Сводка по счетчикам)



Страница Counter Summary (Сводка по счетчикам) содержит следующие поля:

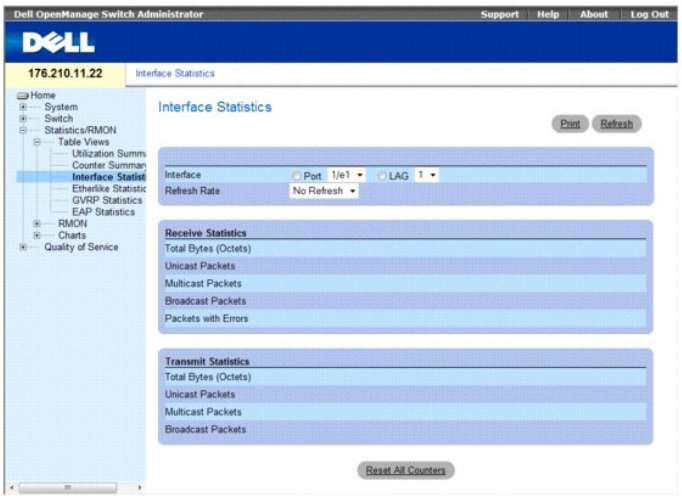
- **Refresh Rate (Частота обновления)**. Период времени между обновлениями статистики интерфейса. Возможные значения:
  - **15 с**. Статистика интерфейса обновляется каждые 15 секунд.
  - **30 с**. Статистика интерфейса обновляется каждые 30 секунд.
  - **60 с**. Статистика интерфейса обновляется каждые 60 секунд.
  - **No Refresh (Нет обновления)**. Автоматическое обновление статистики интерфейса не происходит.
- **Interface (Интерфейс)**. Номер интерфейса.
- **Interface Status (Состояние интерфейса)**. Состояние интерфейса.
- **Received Unicast Packets (Получено одноадресных пакетов)**. Число полученных на интерфейс одноадресных пакетов.
- **Transmit Unicast Packets (Передано одноадресных пакетов)**. Число переданных одноадресных пакетов из интерфейса.
- **Received Non Unicast Packets (Получено многоадресных пакетов)**. Число полученных на интерфейс многоадресных пакетов.
- **Transmit Non Unicast Packets (Передано многоадресных пакетов)**. Число переданных многоадресных пакетов из интерфейса.
- **Received Errors (Получено с ошибками)**. Число пакетов с ошибками, полученных на интерфейс.
- **Global System LAGs (Общие системные LAG)**. Выдает сводку по счетчиками общих системных групп LAG.

Просмотр статистики интерфейса

Страница Interface Statistics (Статистика интерфейса) содержит статистику по принятым и переданным пакетам. Поля для полученных и переданных пакетов идентичны.

Чтобы открыть страницу Interface Statistics (Статистика интерфейса), щелкните **Statistics/RMON** (Статистика/RMON)→ **Table Views** (Просмотр в виде таблиц)→ **Interface Statistics** (Статистика интерфейса) на панели дерева.

Рис. 8-3. Interface Statistics (Статистика интерфейса)



Страница Interface Statistics (статистика интерфейса) содержит следующие поля:

- **Interface (Интерфейс)**. Указывает, отображается статистика для порта или LAG.
- **Refresh Rate (Частота обновления)**. Период времени между обновлениями статистики интерфейса. Возможные значения:
  - **15 с**. Статистика интерфейса обновляется каждые 15 секунд.
  - **30 с**. Статистика интерфейса обновляется каждые 30 секунд.
  - **60 с**. Статистика интерфейса обновляется каждые 60 секунд.
  - **No Refresh (Нет обновления)**. Автоматическое обновление статистики интерфейса не происходит.

Статистика приема

- **Total Bytes (Octets) (Всего байт (октетов))**. Число октетов, принятых на выбранный интерфейс.
- **Unicast Packets (Одноадресные пакеты)**. Число одноадресных пакетов, полученных на выбранный интерфейс.
- **Multicast Packets (Многоадресные пакеты)**. Число многоадресных пакетов, полученных на выбранный интерфейс.
- **Broadcast Packets (Пакеты широковещательной рассылки)**. Число пакетов широковещательной рассылки, полученных на выбранный интерфейс.
- **Packets with Errors (Получено пакетов с ошибками)**. Число пакетов с ошибками, полученных на выбранный интерфейс.

Статистика передачи

- **Total Bytes (Octets) (Всего байт (октетов)**. Число октетов, переданных с выбранного интерфейса.
- **Unicast Packets (Одноадресные пакеты)**. Количество одноадресных пакетов, переданных с выбранного интерфейса.
- **Multicast Packets (Многоадресные пакеты)**. Количество многоадресных пакетов, переданных с выбранного интерфейса.
- **Broadcast Packets (Пакеты широковещательной рассылки)**. Число пакетов широковещательной рассылки, переданных с выбранного интерфейса.

Отображение статистики интерфейса

1. Откройте страницу Interface Statistics (Статистика интерфейса).
2. Выберите интерфейс в поле **Interface** (Интерфейс).

   Отображается **статистика интерфейса для выбранного интерфейса**.

Сброс счетчиков статистики интерфейса

1. Откройте страницу Interface Statistics (Статистика интерфейса).
2. Щелкните **Reset All Counters** (Сбросить все счетчики).

Произойдет сброс счетчиков статистики интерфейса

Просмотр статистики интерфейса с помощью команд консоли

Следующая таблица содержит команды CLI для просмотра статистики интерфейса.

Таблица 8-1. Команды консоли для статистики интерфейса

Команда консоли	Описание
show interfaces counters [**ethernet** (интерфейс) | **port-channel***interface- port-channel-number (номер_канала_порта)*]	Отображает трафик, видимый физическим интерфейсом.

Далее приведен пример команд консоли.

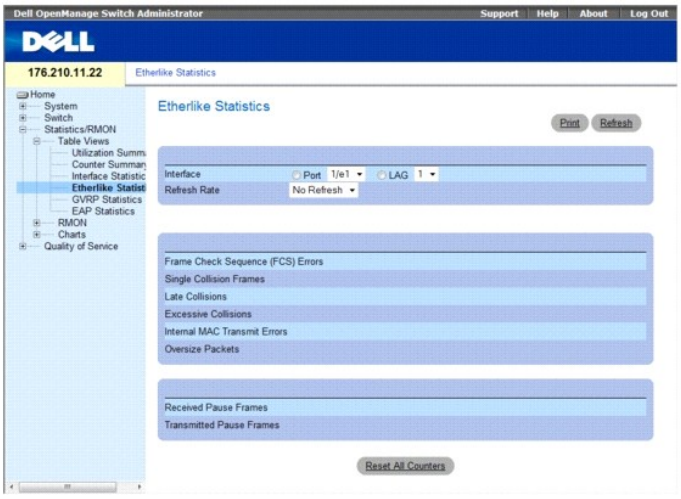
```
console> консоль включить

console# show interfaces counters

Port InOctets InUcastPkts InMcastPkts InBcastPkts

------. --------. ----------. ----------. ----------

1/e1 0 0 0 0

1/e2 0 0 0 0

1/e3 0 0 0 0

1/e4 0 0 0 0

1/e5 0 0 0 0

1/ e6 0 0 0 0

1/e7 0 0 0 0

1/e8 0 0 0 0

1/e9 0 0 0 0

1/e10 0 0 0 0
```

Просмотр статистики Etherlike

Страница Etherlike Statistics (Статистика Etherlike) содержит статистику ошибок интерфейса.

Чтобы открыть страницу Etherlike Statistics (Статистика интерфейса), щелкните **Statistics/RMON** (Статистика/RMON)→ **Table Views** (Просмотр в виде таблиц)→ **Etherlike Statistics** (Статистика интерфейса) на панели дерева.

Рис. 8-4. Etherlike Statistics (Статистика Etherlike)



Страница Etherlike Statistics (Статистика Etherlike) содержит следующие поля:

- **Interface (Интерфейс)**. Указывает, отображается статистика для порта или LAG.
- **Refresh Rate (Частота обновления)**. период времени между обновлениями статистики интерфейса. Возможные значения:
  - **15 с**. Статистика Etherlike обновляется каждые 15 секунд.
  - **30 с**. Статистика Etherlike обновляется каждые 30 секунд.
  - **60 с**. Статистика Etherlike обновляется каждые 60 секунд.
  - **No Refresh (Нет обновления)**. Автоматическое обновление статистики Etherlike не происходит.
- **Frame Check Sequence (FCS) Errors** (Ошибки последовательности проверки кадра). число ошибок последовательности проверки кадра, полученных на выбранный интерфейс.
- **Single Collision Frames (Кадры с одиночной коллизией)**. Число ошибок одиночных коллизий в кадрах, полученных на выбранный интерфейс.
- **Late Collisions (Последние коллизии)**. Число последних коллизий, полученных на выбранный интерфейс.
- **Internal MAC Transmit Errors (Внутренние ошибки передачи MAC)**. Число внутренних ошибок управления доступом к среде передачи (Internal MAC Transmit), полученных на выбранный интерфейс.
- **Oversize Packets (Превышение размера пакетов)**. Число слишком больших пакетов, полученных на выбранный интерфейс.
- **Receive Pause Frames (Принятые кадры паузы)**. Число ошибок паузы, полученных на выбранный интерфейс.
- **Transmitted Paused Frames (Переданные кадры паузы)**. Число ошибок паузы, переданных с выбранного интерфейса.

Отображение статистики Etherlike для интерфейса

1. Откройте страницу Etherlike Statistics (Статистика Etherlike).
2. Выберите интерфейс в поле **Interface** (Интерфейс).

Сброс статистики Etherlike

1. Откройте страницу Etherlike Statistics (Статистика Etherlike).
2. Щелкните **Reset All Counters** (Сбросить все счетчики).

   Произойдет сброс счетчиков статистики Etherlike.

Просмотр статистики Etherlike с помощью команд консоли

Следующая таблица содержит команды CLI для просмотра статистики Etherlike.

Таблица 8-2. Команды консоли статистики Etherlike

Команда консоли	Описание
show interfaces counters [**ethernet** *(интерфейс)*| **port-channel** *port-channel-number (номер_канала_порта)* **]**	Отображает трафик, видимый физическим интерфейсом.

Далее приведен пример команд консоли.

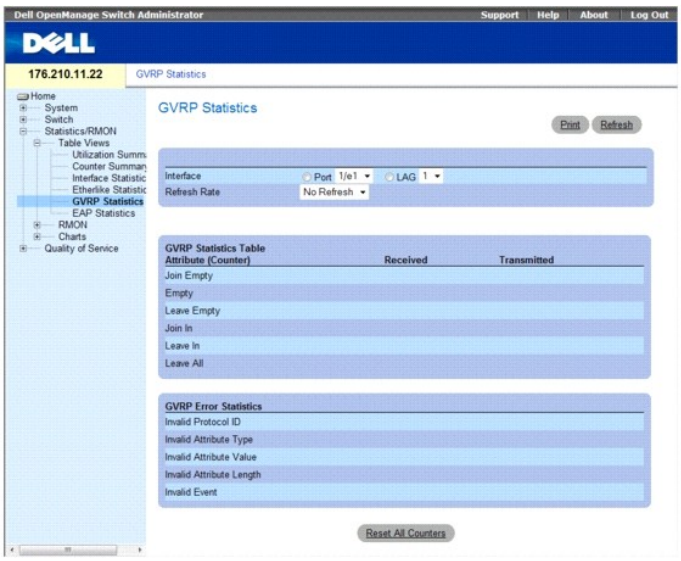
```
Console# show interfaces counters ethernet 1/e1

Port    IN Octets    InUcastPkts    InMcastPkts    InBcastPkts
----    ---------    -----------    -----------    -----------
1/e1    183892       1289           987            8

Port    OUT Octets   OutUcastPkts   OutMcastPkts   OutBcastPkts
----    ----------   ------------   ------------   ------------
1/e1    9188         9              8              0

FCS Errors: 8
Single Collision Frames: 0
Multiple Collision Frames: 0
SQE Test Errors: 0
Deferred Transmissions: 0
Late Collisions: 0
Excessive Collisions: 0
Internal MAC Tx Errors: 0
Carrier Sense Errors: 0
Oversize Packets: 0
Internal MAC Rx Errors: 0
Received Pause Frames: 0
Transmitted Pause Frames: 0
```

Просмотр статистики протокола GVRP

На странице GVRP Statistics (Статистика GVRP) показана статистика для протокола GVRP.

Чтобы открыть эту таблицу, щелкните **Statistics/RMON** (Статистика/RMON)→ **Table Views** (Просмотр в виде таблиц)→ **GVRP Statistics** (Статистика интерфейса) на панели дерева.

Рис. 8-5. GVRP Statistics (Статистика GVRP)



Страница GVRP Statistics (Статистика GVRP) содержит следующие поля:

- **Interface (Интерфейс)**. Указывает, отображается статистика для порта или LAG.
- **Refresh Rate (Частота обновления)**. Период времени между обновлениями статистики GVRP. Возможные значения:
  - **15 с**. Статистика GVRP обновляется каждые 15 секунд.
  - **30 с**. Статистика GVRP обновляется каждые 30 секунд.
  - **60 с**. Статистика GVRP обновляется каждые 60 секунд.
  - **No Refresh (Нет обновления)**. Автоматическое обновление статистики GVRP не происходит.

Таблица статистики GVRP

- **Join Empty (Объединить пустые)**. Статистика Join Empty протокола GVRP для устройства.
- **Empty (Пустая)**. Указывает число пустых статистик GVRP.
- **Leave Empty (Оставлять пустые)**. Статистика Leave Empty протокола GVRP для устройства.
- **Join In (Присоединять)**. Статистика Join In протокола GVRP для устройства.
- **Leave In (Оставлять)**. Статистика Leave In протокола GVRP для устройства.
- **Leave All (Оставлять все)**. Статистика Leave all протокола GVRP для устройства.

Статистика ошибок GVRP

- **Invalid Protocol ID (Недопустимый идентификатор протокола)**. Статистика Invalid Protocol ID протокола GVRP для устройства.
- **Invalid Attribute Type (Недопустимый тип атрибута)**. Статистика Invalid Attribute Type протокола GVRP для устройства.
- **Invalid Attribute Value (Недопустимое значение атрибута)**. Статистика Invalid Attribute Value протокола GVRP для устройства.
- **Invalid Attribute Length (Недопустимая длина атрибута)**. Статистика Invalid Attribute Length протокола GVRP для устройства.
- **Invalid Event (Недопустимые события)**. Статистика Invalid Events протокола GVRP для устройства.

Отображение статистики GVRP для порта

1. Откройте страницу GVRP Statistics (Статистика GVRP).
2. Выберите интерфейс в поле **Interface** (Интерфейс).

   Отображается статистика GVRP для выбранного интерфейса.

Сброс статистики GVRP

1. Откройте страницу GVRP Statistics (Статистика GVRP).
2. Щелкните **Reset All Counters** (Сбросить все счетчики).

   Произойдет сброс счетчиков статистики GVRP.

Просмотр статистики протокола GVRP с помощью команд консоли

В следующей таблице приведены команды консоли для просмотра статистики GVRP.

Таблица 8-3. Команды консоли для просмотра статистики GVRP

Команда консоли	Описание
show gvrp statistics [**ethernet** *interface (интерфейс)* | **port-channel** *port-channel-number (порт-канал-номер)*]	Отображает статистику протокола GVRP.
show gvrp error-statistics [**ethernet** *interface (интерфейс)* | **port-channel** *port-channel-number (номер_канала_порта)*]	Отображает статистику ошибок протокола GVRP.

Далее приведен пример команд консоли.

```
console# show gvrp statistics

GVRP statistics:

---------------

Legend:

rJE : Join Empty Received

rJIn : Join In Received

rEmp : Empty Received

rLIn : Leave In Received

rLE : Leave Empty Received

rLA : Leave All Received

sJE : Join Empty Sent

sJIn : Join In Sent

sEmp : Empty Sent

sLIn : Leave In Sent

sLE : Leave Empty Sent

sLA : Leave All Sent
```

```
Port rJE rJIn rEmp rLIn rLE rLA sJE sJIn sEmp sLIn sLE sLA

----. --. ---. ---. ---. --. --. --. --. --. ---. --. --

1/e1 0 0 0 0 0 0 0 0 0 0 0 0

1/e2 0 0 0 0 0 0 0 0 0 0 0 0

1/e3 0 0 0 0 0 0 0 0 0 0 0 00 0
```

```
Console# show gvrp error-statistics

GVRP error statistics:

---------------

Legend:

INVPROT : Invalid Protocol Id
```

INVPLEN : Invalid PDU Length

INVATYP : Invalid Attribute Type

INVALEN : Invalid Attribute Length

INVAVAL : Invalid Attribute Value

INVEVENT : Invalid Event

Port INVPROT INVATYP INVAVAL INVPLEN INVALEN INVEVENT

---. ------. ------. ------. -----. ------. -------

1/e1 0 0 0 0 0 0

1/e2 0 0 0 0 0 0

1/e3 0 0 0 0 0 0

1/e4 0 0 0 0 0 0

sLE : Leave Empty Sent

sLA : Leave All Sent

Port rJE rJIn rEmp rLIn rLE rLA sJE sJIn sEmp sLIn sLE sLA

---. --. ---. ---. ---. --. --. --. --. --. ---. --. --

1/e1 0 0 0 0 0 0 0 0 0 0 0 0

1/e2 0 0 0 0 0 0 0 0 0 0 0 0

1/e3 0 0 0 0 0 0 0 0 0 0 0 0

1/e4 0 0 0 0 0 0 0 0 0 0 0 0

1/e5 0 0 0 0 0 0 0 0 0 0 0 0

1/e6 0 0 0 0 0 0 0 0 0 0 0 0

1/e7 0 0 0 0 0 0 0 0 0 0 0 0

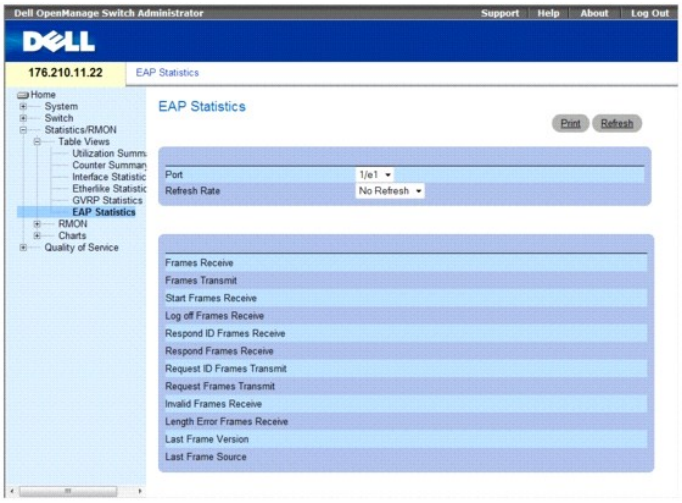
1/e8 0 0 0 0 0 0 0 0 0 0 0 0

Просмотр статистики EAP

Страница EAP Statistics (Статистика EAP) содержит сведения о пакетах EAP, полученных на определенный порт. Дополнительную информацию о EAP см. в разделе Port Based Authentication (Проверка подлинности на основе порта).

Чтобы открыть страницу EAP Statistics (Статистика EAP), выберите **Statistics / RMON** (Статистика/RMON)→ **Table Views** (Табличный вид)→ **EAP Statistics** (Статистика EAP) на панели дерева.

Рис. 8-6. Страница EAP Statistics (Статистика EAP)



Страница **EAP Statistics** (Статистика EAP) содержит следующие поля.

- **Port (Порт)**. Указывает порт, запрос которого происходит для отображения статистики EAP.
- **Refresh Rate (Частота обновления)**. Период времени между обновлениями статистики EAP. Возможные значения:
  - **15 с**. Статистика EAP обновляется каждые 15 секунд.
  - **30 с**. Статистика EAP обновляется каждые 30 секунд.
  - **60 с**. Статистика EAP обновляется каждые 60 секунд.
  - **No Refresh (Нет обновления)**. Автоматическое обновление статистики EAP не происходит.
- **Frames Receive (Получено кадров)**. Отображает количество полноценных кадров EAPOL, полученных на этом порте.
- **Frames Transmit (Передано кадров)**. Число кадров по протоколу EAPOL, переданных через порт.
- **Start Frames Receive (Получено начальных кадров)**. Число кадров Start по протоколу EAPOL, полученных на порте.
- **Log off Frames Receive (Получено кадров Log off)**. Число кадров Log off по протоколу EAPOL, полученных для порта.
- **Respond ID Frames Receive (Получено кадров с идентификаторами ответа)**. Число кадров Resp/Id по протоколу EAP, полученных на порте.
- **Respond ID Frames Receive (Получено кадров с идентификаторами ответа)**. Число кадров Resp/Id по протоколу EAP, полученных на порте.
- **Request ID Frames Transmit (Передано кадров с идентификатором запроса)**. Число кадров Requested ID по протоколу EAP, переданных через порт.
- **Request ID Frames Transmit (Передано кадров с идентификатором запроса)**. Число кадров Requested ID по протоколу EAP, переданных через порт.
- **Log off Frames Receive (Получено кадров Log off)**. Число нераспознанных кадров Log off по протоколу EAPOL, полученных для порта.
- **Length Error Frames Receive (Получено кадров с ошибкой длины)**. Число кадров по протоколу EAPOL с неверной длиной тела пакета, полученных на этом порте.
- **Last Frame Version (Версия последнего кадра)**. Номер версии протокола, указанный для последнего принятого кадра по протоколу EAPOL.
- **Last Frame Source (Источник последнего кадра)**. MAC-адрес источника, указанный для последнего принятого кадра по протоколу EAPOL.

Отображение статистики EAP для порта

1. Откройте страницу EAP Statistics (Статистика EAP).
2. Выберите интерфейс в поле **Interface** (Интерфейс).

   Отобразится статистика EAP интерфейса.

Для сброса статистики EAP:

1. Откройте страницу EAP Statistics (Статистика EAP).
2. Щелкните Reset All Counters (Сбросить все счетчики).

   Произойдет сброс счетчиков статистики EAP.

Просмотр статистики протокола EAP с помощью команд консоли

В следующей таблице приведены команды консоли для просмотра статистики интерфейса EAP.

Таблица 8-4. Команды консоли для просмотра статистики EAP

Команда консоли	Описание
show dot1x statistics	Отображает статистику 802.1X для указанного интерфейса.

Далее приведен пример команд консоли.

```
console# show dot1x statistics ethernet 1/e1

EapolFramesRx: 11

EapolFramesTx: 12
```

```
EapolStartFramesRx: 1

EapolLogoffFramesRx: 1

EapolRespIdFramesRx: 3

EapolRespFramesRx: 6

EapolReqIdFramesTx: 3

EapolReqFramesTx: 6

InvalidEapolFramesRx: 0

EapLengthErrorFramesRx: 0

LastEapolFrameVersion: 1

LastEapolFrameSource: 0008.3b79.8787
```

Просмотр статистики удаленного мониторинга RMON

С помощью удаленного мониторинга (RMON) администраторы сети могут осуществлять удаленный доступ к информации. Для того, чтобы открыть страницу **RMON**, нажмите на ссылку под строкой помощи для текущей страницы.

Щелкните **Statistics / RMON→ RMON** на панели дерева.

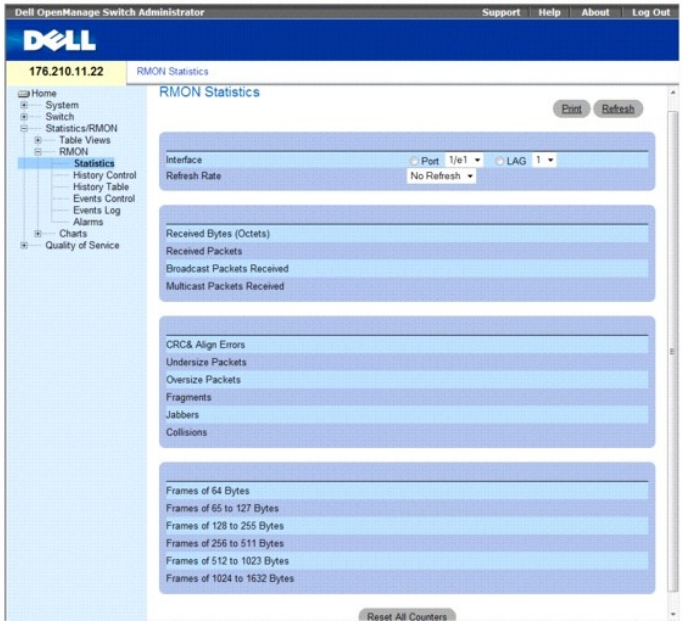
В этом разделе имеются следующие тематические подразделы:

- Просмотр группы статистики RMON
- Просмотр статистики управления журналом удаленного мониторинга
- Просмотр журнала удаленного мониторинга
- Определение событий удаленного мониторинга устройства
- Просмотр журнала событий удаленного мониторинга
- Определение сигналов устройств удаленного мониторинга

Просмотр группы статистики RMON

Страница **RMON Statistics** (Статистика RMON) используется для отображения информации по использованию устройства и возникающих на нем ошибок. Чтобы открыть страницу **RMON Statistics** (Сигналы удаленного мониторинга), щелкните **Statistics / RMON** (Статистика/RMON)→ **RMON**→ **Statistics** (Статистика) на панели дерева.

Рис. 8-7. RMON Statistics (Статистика RMON)



Страница **RMON Statistics** (Статистика RMON) содержит следующие поля:

- **Interface (Интерфейс)**. Указывает порт или LAG, для которых отображается статистика.
- **Refresh Rate (Частота обновления)**. Период времени между обновлениями статистики интерфейса.
- **Received Bytes (Octets) (Получено байт (октетов))**. Число байт, полученных на выбранный интерфейс.
- **Received Packets (Пакетов получено)**. Число байт, полученных на выбранный интерфейс.
- **Broadcast Packets Received (Получено широковещательных пакетов)**. Число хороших широковещательных пакетов, полученных на интерфейс с момента последнего обновления устройства. В это число не входят многоадресные пакеты.
- **Multicast Packets Received (Получено многоадресных пакетов)**. Число хороших многоадресных пакетов, полученных на интерфейс с момента последнего обновления устройства.
- **CRC & Align Errors (Ошибки контрольной суммы и выравнивания)**. Число ошибок контрольной суммы (CRC) и выравнивания, произошедших на интерфейсе с момента последнего обновления устройства.
- **Undersize Packets (Пакеты с размером меньше допустимого)**. Число пакетов с размером, меньше минимально допустимого (менее 64 октетов), полученных на интерфейс с момента последнего обновления устройства.
- **Oversize Packets (Превышение размера пакетов)**. Число пакетов с размером, больше максимально допустимого (более 1632 октетов), полученных на интерфейс с момента последнего обновления устройства.
- **Fragments (Фрагменты)**. Число фрагментов (пакеты размером менее 64 октетов, исключая биты кадров, но включая октеты FCS), полученных на интерфейс с момента последней очистки счетчиков.
- **Jabbers (Сбойные пакеты)**. Число сбойных пакетов (пакеты длиннее 1632 октетов), полученных на интерфейс с момента последнего обновления устройства.
- **Collisions (Коллизии)**. Число коллизий, полученных на интерфейс с момента последнего обновления устройства.
- **Frames of *xx* Bytes (Кадры из xx байт)**. Число *xx*-байтовых кадров, полученных на интерфейс с момента последнего обновления устройства.

Просмотр статистики интерфейса

1. Откройте страницу **RMON Statistics** (Статистика RMON).
2. Выберите тип и номер интерфейса в поле **Interface** (Интерфейс).

   Отобразится статистика интерфейса.

Просмотр статистики удаленного мониторинга с помощью команд консоли

В следующей таблице приведены команды консоли для просмотра статистики удаленного мониторинга.

Таблица 8-5. Команды консоли для просмотра статистики удаленного мониторинга

Команда консоли	Описание
show rmon statistics {**ethernet** *interface (интерфейс)* | **port-channel** *port-channel-number (номер_канала_порта)*}	Отображает статистику удаленного мониторинга по Ethernet.

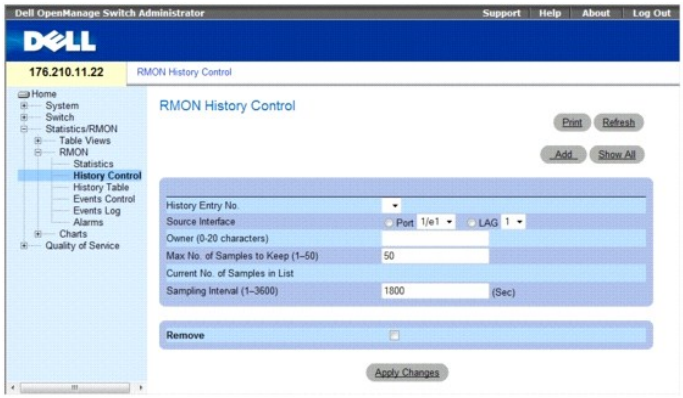
Далее приведен пример команд консоли.

```
console# show rmon statistics ethernet 1/e1

Port 1/e1

Dropped: 8

Octets: 878128 Packets: 978

Broadcast: 7 Multicast: 1

CRC Align Errors: 0 Collisions: 0

Undersize Pkts: 0 Oversize Pkts: 0

Fragments: 0 Jabbers: 0

64 Octets: 98 65 to 127 Octets: 0

128 to 255 Octets: 0 256 to 511 Octets: 0

512 to 1023 Octets: 491 1024 to 1632 Octets: 389
```

Просмотр статистики управления журналом удаленного мониторинга

Страница RMON History Control (Управление журналом удаленного мониторинга) содержит информацию по выборкам данных удаленного мониторинга, полученных с портов. Например, в выборки могут входить определения интерфейса или интервалы опроса. Чтобы открыть страницу RMON History Control (Управление журналом удаленного мониторинга), выберите **Statistics/RMON** (Статистика/RMON)→ **RMON**→ **History Control** (Управление журналом) на панели дерева.

Рис. 8-8. RMON History Control (Управление журналом удаленного мониторинга)



Страница RMON History Control (Управление журналом удаленного мониторинга) содержит следующие поля:

- **History Entry No. (Номер записи журнала)**. Номер записи для страницы **History Control** (Управление журналом удаленного мониторинга).
- **Source Interface (Интерфейс-источник)**. Порт или LAG, из которых были получены выборки журнала.
- **Owner (0-20 characters)(Владелец (0-20 символов))**. Станция удаленного мониторинга или пользователя, запросившего информацию по удаленному доступу.
- **Max No. of Samples to Keep (1-50) (Максимальное число выборок для хранения) (1-50)**. Число сохраняемых выборок. Значение по умолчанию. 50.
- **Current No. of Samples in List (Текущее число выборок)**. Текущее количество полученных выборок.
- **Sampling Interval (Интервал дискретизации) (1-3600)**.Время в секундах, за которое происходит выборка с портов. Возможные значения: 1-3600 сек. Значение по умолчанию: 1800 секунд (30 минут).
- **Remove (Удалить)**. Когда этот флажок установлен, запись удаляется из **History Control Table** (таблицы управления журналом).

Добавление записи управления журналом

1. Откройте страницу RMON History Control (Управление журналом удаленного мониторинга).
2. Нажмите кнопку **Add** (Добавить).

   Откроется страница **Add History Entry** (Добавление записи журнала).
3. Введите значения в полях диалогового окна.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Запись добавится в **History Control Table** (Таблицу управления журналом).

Изменение записи таблицы управления журналом

1. Откройте страницу RMON History Control (Управление журналом удаленного мониторинга).
2. Выберите запись в поле **History Entry No.** (Номер записи журнала).
3. Выполните необходимые изменения в полях.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Запись таблицы изменяется, а устройство обновляется.

Удаление записи таблицы управления журналом

1. Откройте страницу RMON History Control (Управление журналом удаленного мониторинга).
2. Выберите запись в поле **History Entry No.** (Номер записи журнала).
3. Нажмите кнопку **Apply Changes** (Применить изменения).

   Запись таблицы будет удалена, а устройство обновлено.

Просмотр управления журналом удаленного мониторинга с помощью команд консоли

В следующей таблице приведены команды консоли для просмотра управления журнала удаленного мониторинга.

Таблица 8-6. Команды консоли журнала удаленного мониторинга

Команда консоли	**Описание**
rmon collection history индекс [**owner** *bucket-number (имя владельца)* | **buckets** *seconds (номер_блока)ownername*] [**interval секунды**]	Включает и настраивает удаленный мониторинг на интерфейсе.
show rmon collection history [**ethernet** *interface (интерфейс)* | **port-channel** *port-channel-number(номер_канала_порта)*]	Отображает статистику журнал совокупности удаленного мониторинга.

Далее приведен пример команд консоли.

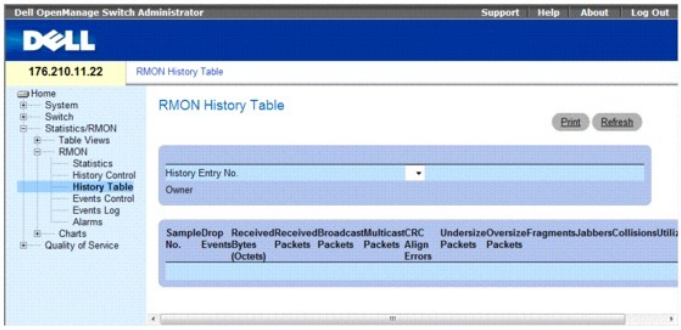
```
console(config)# interface ethernet 1/e8

console(config-if)# rmon collection history 1 interval 2400
```

Просмотр журнала удаленного мониторинга

Страница RMON History Table (Журнал удаленного мониторинга) содержит статистические сетевые выборки для конкретного интерфейса. Каждая запись таблицы представляет собой все значения счетчиков, скомпилированные в течение однократной выборки. Чтобы открыть страницу RMON History Table (Журнал удаленного мониторинга), щелкните **Statistics / RMON** (Статистика/RMON)→ **RMON**→ **History Table** (Управление журналом) на

панели дерева.

Рис. 8-9. RMON History Table (Таблица журнала удаленного мониторинга)



Страница RMON History Table (Таблица управления журналом удаленного мониторинга) содержит следующие поля:

Не все поля показаны в таблице управления журналом удаленного мониторинга на рисунке RMON History Table (Таблица управления журналом удаленного мониторинга).

- **History Entry No. (Номер записи журнала)**. Указывает номер записи страницы **History Control** (Управление журналом).
- **Owner (Владелец)**. Станция удаленного мониторинга или пользователя, запросившего информацию по удаленному доступу.
- **Sample No. (Номер выборки)**. Указывает номер конкретной выборки, которую отражает информация в таблице.
- **Drop Events (Потерянные события)**. Число пакетов, потерянных из-за нехватки сетевых ресурсов в течение интервала выборки. Так как указать точное количество потерянных пакетов невозможно, то указывается, сколько раз были обнаружены потерянные пакеты.
- **Received Bytes (Octets) (Полученные байты (Октеты))**. Число октетов данных, включая поврежденные пакеты, полученные по сети.
- **Received Packets (Полученные пакеты)**. Число пакетов, полученных во время интервала выборки.
- **Broadcast Packets (Широковещательные пакеты)**. Число корректных широковещательных пакетов, полученных во время интервала выборки.
- **Multicast Packets (Многоадресные пакеты)**. Число корректных многоадресных пакетов, полученных во время интервала выборки.
- **CRC Align Errors (Ошибки выравнивания CRC)**. Число пакетов, полученных во время сеанса выборки с длинной в 64-1632 октетов. Однако пакеты имеют неверную последовательность проверки кадра (FCS) с целым числом октетов или неверную FCS с нецелым числом.
- **Undersize Packets (Пакеты с размером меньше допустимого)**. Число пакетов, полученных во время сеанса выборки, с длиной меньше 64 октетов.
- **Oversize Packets (Пакеты с размером меньше допустимого)**. Число пакетов, полученных во время сеанса выборки, с длиной больше 1632 октетов.
- **Fragments (Фрагменты)**. Число пакетов, полученных во время сеанса выборки, с длиной меньше 64 октетов и содержащих контрольную последовательность кадра.
- **Jabbers (Сбойные пакеты)**. Число пакетов, полученных во время сеанса выборки, с длиной больше 1632 октетов и содержащих контрольную последовательность кадра.
- **Collisions(Коллизии)**. Оценка общего количества коллизий пакетов, имевших место во время сеанса выборки. Коллизии обнаруживаются, когда порты повторителя засекают одновременную передачу с двух или более станций.
- **Utilization (Использование)**. Оценка степени использования главного физического уровня сети на интерфейсе во время сеанса выборки. Это значение отображается сотыми долями процента.

Просмотр статистики для определенной записи журнала

1. Откройте страницу RMON History Table (Журнал удаленного мониторинга).
2. Выберите запись в поле **History Entry No.** (Номер записи журнала).

   Статистика для записи будет отображена в таблице RMON History (Журнал удаленного мониторинга).

Просмотр управления журналом удаленного мониторинга с помощью команд консоли

В следующей таблице приведены команды консоли для просмотра журнала удаленного мониторинга.

Таблица 8-7. Команды консоли для управления журналом удаленного мониторинга

Команда консоли	Описание
show rmon history *индекс* {**throughput	errors	other**} [**period** *сек*]	Отображает журнал статистики удаленного мониторинга Ethernet.

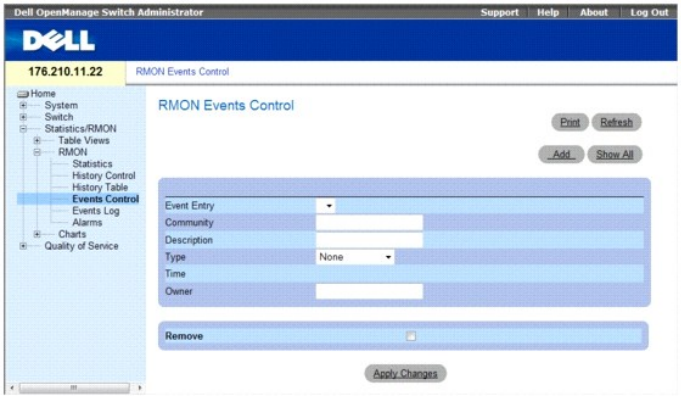
Далее приведен пример команд консоли для отображения статистики удаленного мониторинга Ethernet для пропускной способности по индексу 1:

```
console> консоль включить

console# show rmon history 1 throughput

Sample Set: 5 Owner: cli

Interface: 24 interval: 10

Requested samples: 50 Granted samples: 50

Maximum table size: 270

Time Octets Packets Broadcast Multicast %

------------------. -. ---. -. ------. ------. -. --------. --

09-Mar-2003 18:29:32 0 0 0 0 0

09-Mar-2003 18:29:42 0 0 0 0 0

09-Mar-2003 18:29:52 0 0 0 0 0

09-Mar-2003 18:30:02 0 0 0 0 0

09-Mar-2003 18:30:12 0 0 0 0 0

09-Mar-2003 18:30:22 0 0 0 0 0
```

Определение событий удаленного мониторинга устройства

Используйте страницу RMON Events Control (Управление событиями удаленного мониторинга) для определения событий удаленного мониторинга. Чтобы открыть страницу RMON Events Control (Управление событиями удаленного мониторинга) щелкните **Statistics / RMON** (Статистика/RMON)→ **RMON**→ **Events Control** (Управление событиями) на панели дерева.

Рис. 8-10. RMON Events Control (Управление событиями удаленного мониторинга)



Страница RMON Events Control (Управление событиями удаленного мониторинга) содержит следующие поля:

- **Event Entry (Запись события)**. Указывает событие.
- **Community (Сообщество)**. Сообщество SNMP, к которому принадлежит событие.
- **Description (Описание)**. Описание события, определяемое пользователем.
- **Type (Тип)**. Тип события. Возможные значения:
  - **Log (Журнал)**. Тип события. запись в журнале.
  - **Trap (Прерывание)**. Тип события. прерывание.
  - **Log and Trap (Журнал и прерывание)**. Тип события. запись в журнале и прерывание.
  - **None (Нет)**. Событие отсутствует.

- **Time (Время)**. Время, когда произошло событие.
- **Owner (Владелец)**. Устройство или пользователь, который определил событие.
- **Remove (Удалить)**. Когда этот флажок установлен, событие удаляется из таблицы журнала удаленного мониторинга **(RMON Events Table)**.

Добавление события удаленного мониторинга

1. Откройте страницу RMON Events Control (Управление событиями удаленного мониторинга).
2. Нажмите кнопку **Add** (Добавить).

   Откроется страница **Add an Event Entry** (Добавление записи журнала).
3. Введите данные в диалоговом окне и нажмите кнопку **Apply Changes** (Применить изменения).

   Запись таблицы **Event Table** (Таблица событий) будет добавлена, а устройство обновлено.

Изменение события удаленного мониторинга

1. Откройте страницу RMON Events Control (Управление событиями удаленного мониторинга)
2. Выберите запись в таблице **Event Table** (Таблица событий).
3. Измените значения в полях диалогового окна и нажмите кнопку **Apply Changes** (Применить изменения).

   Запись таблицы **Event Table** (Таблица событий) будет изменена, а устройство обновлено.

Удаление записей о событиях удаленного мониторинга

Можно удалить запись одного события со страницы **RMON Events Control** (Управление событиями удаленного мониторинга) с помощью флажка **Remove** (Удалить) на этой странице.

1. Откройте страницу RMON Events Control (Управление событиями удаленного мониторинга).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **RMON Events Table** (События удаленного мониторинга).
3. Установите флажок в поле **Remove** (Удалить) для каждого события, которое необходимо удалить, а затем нажмите кнопку **Apply Changes** (Применить изменения).

   Запись таблицы будет удалена, а устройство обновлено.

Определение событий устройств с помощью команд консоли

В следующей таблице приведены команды консоли для определения событий устройств.

Таблица 8-8. Команды консоли для определения событий устройств

Команда консоли	**Описание**
rmon event ***тип индекса*** [**community** ***text (текст сообщества)***] [**description** ***text (текст описания)*** ***index type***] [**owner** ***имя владельца***]	Настраивает события удаленного мониторинга.
show rmon events	Отображает таблицу событий удаленного мониторинга.

Далее приведен пример команд консоли.

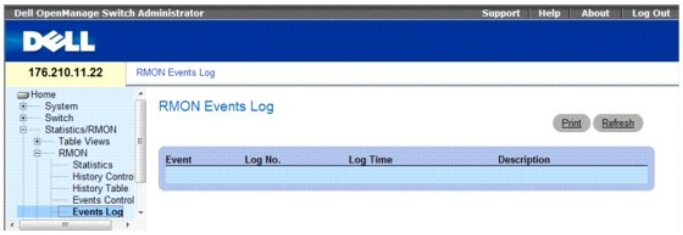
```
console (config)# rmon event 1 log
Console(config)# exit
console# show rmon events
```

Index	Description	Type	Community	Owner	Last time sent
-----	----------	--------	---------	-------	--------------
1	Errors (Ошибки)	Log		CLI	Jan 18 2002 23:58:17
2	High Broadcast	Log-Trap	router	Manager	Jan 18 2002 23:59:48

Просмотр журнала событий удаленного мониторинга

На странице RMON Events Log (Журнал событий удаленного мониторинга) содержится список событий удаленного мониторинга. Чтобы открыть страницу RMON Events Log (Журнал событий удаленного мониторинга), щелкните **Statistics/RMON** (Статистика/RMON)→ **RMON**→ **Events** (События) **Log** (Журнал) на панели дерева.

Рис. 8-11. RMON Events Log (Журнал событий удаленного мониторинга)



Страница RMON Events Log (Журнал событий удаленного мониторинга) содержит следующие поля:

- **Event (Событие)**. Номер записи в журнале событий удаленного мониторинга.
- **Log No. (№ журнала)**. Номер журнала.
- **Log Time (Время записи)**. Время внесения записи в журнал.
- **Description (Описание)**. Описывает запись в журнале.

Определение событий устройств с помощью команд консоли

В следующей таблице приведены команды консоли для определения событий устройств.

Таблица 8-9. Команды консоли для определения событий устройств

Команда консоли	**Описание**
show rmon log [*event (событие)*]	Отображает таблицу журнала событий удаленного мониторинга.

Далее приведен пример команд консоли.

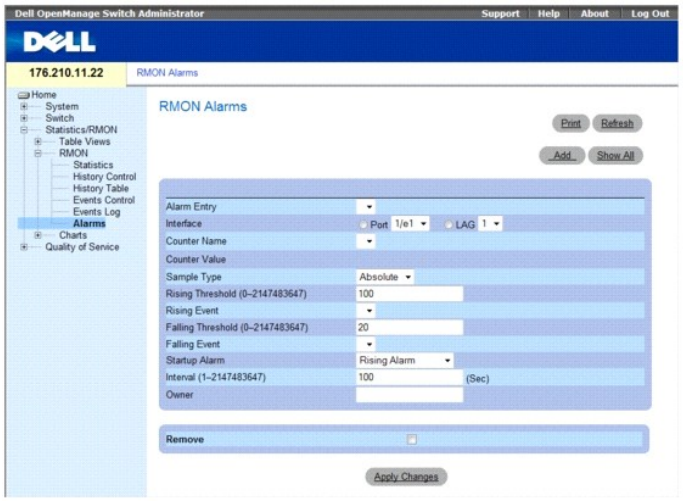
```
console (config)# rmon event 1 log

Console> show rmon log

Maximum table size: 500

Event Description Time

-----. ---------. ----. -------------

1 Errors Jan 18 2002 23:58:17

2 High Broadcast Jan 18 2002 23:59:48
```

Определение сигналов устройств удаленного мониторинга

Для настройки сетевых сигналов используйте страницу RMON Alarms (Сигналы удаленного мониторинга). Сетевая тревога происходит при обнаружении проблемы или события в сети. При повышении или понижении пороговых величин генерируются события. Для получения дополнительной информации о событиях см. раздел Просмотр журнала событий удаленного мониторинга.

Чтобы открыть страницу RMON Alarms (Сигналы удаленного мониторинга), щелкните **Statistics/RMON** (Статистика/RMON)→ **RMON**→ **Alarms** (Сигналы) на панели дерева.

Рис. 8-12. RMON Alarms (Сигналы удаленного мониторинга)



Страница RMON Alarms (Сигналы удаленного мониторинга) содержит следующие поля:

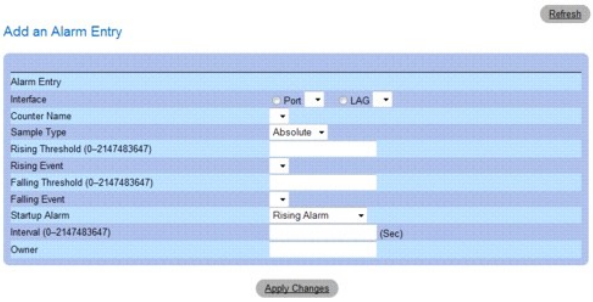
- **Alarm Entry (Запись сигнала)**. Показывает определенный сигнал.
- **Interface (Интерфейс)**. Указывает порт, для которого отображается статистика RMON.
- **Counter Name (Имя счетчика)**. Показывает выбранную переменную MIB.
- **Counter Value (Значение счетчика).** Значение выбранной переменной MIB.
- **Sample Type(Тип выборки)**. Определяет метод выборки для выбранной переменной и сравнивает значение с пороговыми величинами. Возможные значения:
  - **Delta (Разность)**. Вычитается последнее значение выборки из текущего значения. Разница значений сравнивается с пороговой величиной.
  - **Absolute (Абсолютное значение)**. Сравнивает значения с пороговыми величинами в конце интервала выборки.
- **Rising Threshold (Верхнее пороговое значение) (0–2147483647)**. Счетчик, который переключает сигналы пороговых значений. Верхнее пороговое значение отображается в верхней части столбчатых диаграмм. Каждая контролируемая переменная обозначена цветом. Значение по умолчанию: 100 секунд.
- **Rising Event (Событие увеличения)**. Механизм, который используется для выдачи сигналов LOG, TRAP или комбинация обоих. Если выбран LOG, то механизма сохранения нет ни на устройстве, ни в системе управления. Однако если не происходит перезагрузки устройства, то сигнал тревоги остается в таблице LOG устройства. Если выбран параметр TRAP, генерируется прерывание SNMP и сообщается через общий механизм прерывания. Можно сохранить TRAP с помощью этого же механизма.
- **Falling Threshold (Нижнее пороговое значение) (0–2147483647)**. Счетчик, который переключает сигналы пороговых значений. Нижнее пороговое значение графически отображается в верхней части столбчатых диаграмм. Каждая контролируемая переменная обозначена цветом. Значение поля по умолчанию: 20.
- **Startup Alarm (Запуск сигнала)**. Переключатель, активизирующий генерацию сигнала. Превышение определяется переход пороговой величины от нижнего значения порога к верхнему.
- **Interval (Интервал)(1–2147483647) (sec)**. Время между подачей сигналов. Значение по умолчанию: 100 секунд.
- **Owner (Владелец)**. Устройство или пользователь, который определил сигнал.
- **Remove (Удалить)**. Когда этот флажок установлен, сигнал удаленного мониторинга отключается.

Добавление записи в таблицу сигналов

1. Откройте страницу RMON Alarms (Сигналы удаленного мониторинга).
2. Нажмите кнопку **Add** (Добавить).

   Откроется страница **Add an Alarm Entry** (Добавление записи журнала):

   Рис. 8-13. Страница Add an Alarm Entry (Добавление записи журнала)



3. Выберите интерфейс.
4. Заполните поля.
5. Нажмите кнопку **Apply Changes** (Применить изменения).

   Сигнал удаленного мониторинга будет добавлен, а устройство обновлено.

Изменение записи в таблице сигналов

1. Откройте страницу RMON Alarms (Сигналы удаленного мониторинга).
2. Выберите запись в раскрывающемся меню **Alarm Entry** (Запись сигнала).
3. Измените поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Запись будет изменена, а устройство обновлено.

Отображение таблицы сигналов

1. Откройте страницу RMON Alarms (Сигналы удаленного мониторинга).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **Alarms Table** (Таблица сигналов).

Удаление записи в таблице сигналов

1. Откройте страницу RMON Alarms (Сигналы удаленного мониторинга).
2. Выберите запись в раскрывающемся меню **Alarm Entry** (Запись сигнала).
3. Установите флажок **Remove** (Удалить).
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Запись будет удалена, а устройство обновлено.

Определение сигналов устройств с помощью команд консоли

В следующей таблице приведены команды консоли для определения сигналов устройств.

Таблица 8-10. Команды консоли для сигналов устройств

Команда консоли	Описание

rmon alarm индекс MIB_Object_ID interval rthreshold fthreshold revent fevent [type тип] [startup направление] [owner имя владельца] *index MIB_Object_ID interval rthreshold fthreshold revent fevent* [*type*] [*direction*] [*name*]	Настраивает условия выдачи сигналов удаленного мониторинга.
show rmon alarm-table	Отображает сводную таблицу сигналов.
show rmon alarm	Отображает настройку сигналов удаленного мониторинга.

Далее приведен пример команд консоли.

```
console(config)# rmon alarm 1000 1.3.6.1.2.1.2.2.1.10.1 360000 1000000 1000000 10 20

Console# show rmon alarm-table

Index OID Owner

-----. ----------------------. -. ----

1 1.3.6.1.2.1.2.2.1.10.1 CLI

2 1.3.6.1.2.1.2.2.1.10.1 Manager

3 1.3.6.1.2.1.2.2.1.10.9 CLI
```

Просмотр диаграмм

На странице **Chart** (Диаграммы) содержатся ссылки для отображения статистики в виде диаграммы. Чтобы открыть страницу, щелкните **Statistics** (Статистика)→ **Charts** (Диаграммы) на панели дерева.

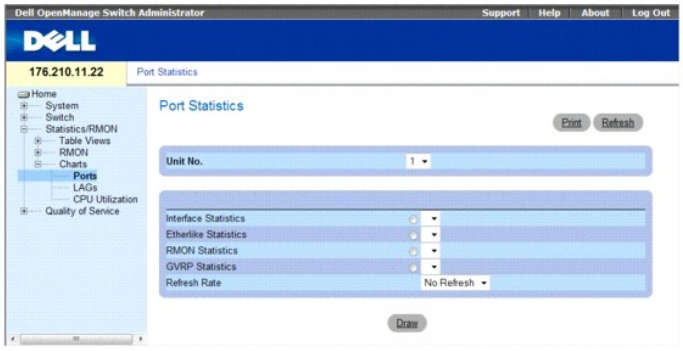
В этом разделе имеются следующие тематические подразделы:

- Просмотр статистики портов
- Просмотр статистики группы LAG
- Просмотр страницы использования ЦП
- Просмотр страницы использования ЦП с помощью команд консоли

Просмотр статистики портов

Используйте страницу Port Statistics (Статистика портов) для просмотра статистики в виде диаграмм для элементов порта. Чтобы открыть страницу Port Statistics (Статистика порта), выберите **Statistics / RMON** (Статистика/RMON)→ **Charts** (Диаграммы)→ **Port Statistics** (Статистика порта) на панели дерева.

Рис. 8-14. Port Statistics (Статистика портов)



Страница Port Statistics (Статистика порта) содержит следующие поля:

- **Unit No. (Номер устройства)**. Указывает номер устройства стека, для которого отображается статистика.
- **Interface Statistics (Статистика интерфейса)**. Выбор статистики интерфейса для отображения.
- **Etherlike Statistics (Статистика Etherlike)**. Выбор типа статистики Etherlike для отображения.

- **RMON Statistics (Статистика удаленного мониторинга)**. Выбор типа статистики удаленного мониторинга для отображения.
- **GVRP Statistics (Статистика GVRP)**. Выбор типа статистики GVRP для отображения.
- **Refresh Rate (Частота обновления)**. Период времени между обновлениями статистики интерфейса.

Отображение статистики для порта

1. Откройте страницу Port Statistics (Статистика порта).
2. Выберите тип статистики для открытия.
3. Выберите необходимую частоту обновления в раскрывающемся меню **Refresh Rate** (Частота обновления).
4. Нажмите кнопку **Draw** (Нарисовать).

   Отобразится график для выбранной статистики.

Просмотр статистики порта с помощью команд консоли

В следующей таблице приведены команды консоли для просмотра статистики портов.

Таблица 8-11. Команды консоли статистики портов

Команда консоли	Описание
show interfaces counters [**ethernet** *interface (интерфейс)* | **port-channel**- *port-channel-number (номер_канала_порта)*]	Отображает трафик, видимый физическим интерфейсом.
show rmon statistics {**ethernet** *interface (интерфейс)* | **port-channel** *port-channel-number (номер_канала_порта)*}	Отображает статистику удаленного мониторинга по Ethernet.
show gvrp statistics {**ethernet** *interface (интерфейс)* | **port-channel** *port-channel-number (номер_канала_порта)*}	Отображает статистику протокола GVRP.
show gvrp-error statistics {ethernet *интерфейс* | **port-channel** *порт-канал-номер*} { *interface* | - *port-channel-number*}	Отображает статистику ошибок протокола GVRP.

Просмотр статистики группы LAG

Для отображения статистики в виде диаграмм для групп LAG используйте страницу LAG Statistics (Статистика LAG). Чтобы открыть страницу LAG Statistics (Статистика LAG), выберите **Statistics / RMON** (Статистика/RMON)→ **Charts** (Диаграммы)→ **LAG Statistics** (Статистика LAG) на панели дерева.

Рис. 8-15. LAG Statistics (Статистика LAG)

Страница LAG Statistics (Статистика LAG) содержит следующие поля:

- **Interface Statistics (Статистика интерфейса)**. Выбор статистики интерфейса для отображения.
- **Etherlike Statistics (Статистика Etherlike)**. Выбор типа статистики Etherlike для отображения.
- **RMON Statistics (Статистика удаленного мониторинга)**. Выбор типа статистики удаленного мониторинга для отображения.
- **GVRP Statistics (Статистика GVRP)**. Выбор типа статистики GVRP для отображения.
- **Refresh Rate (Частота обновления)**. Период времени между обновлениями статистики интерфейса.

Отображение статистики LAG

1. Откройте страницу LAG Statistics (Статистика LAG).
2. Выберите тип статистики для открытия.
3. Выберите необходимую частоту обновления в раскрывающемся меню **Refresh Rate** (Частота обновления).
4. Нажмите кнопку **Draw** (Нарисовать).

   Отобразится график для выбранной статистики.

Просмотр статистики LAG с помощью команд консоли

В следующей таблице приведены команды консоли для просмотра статистики LAG.

Таблица 8-12. Команды консоли для статистики LAG

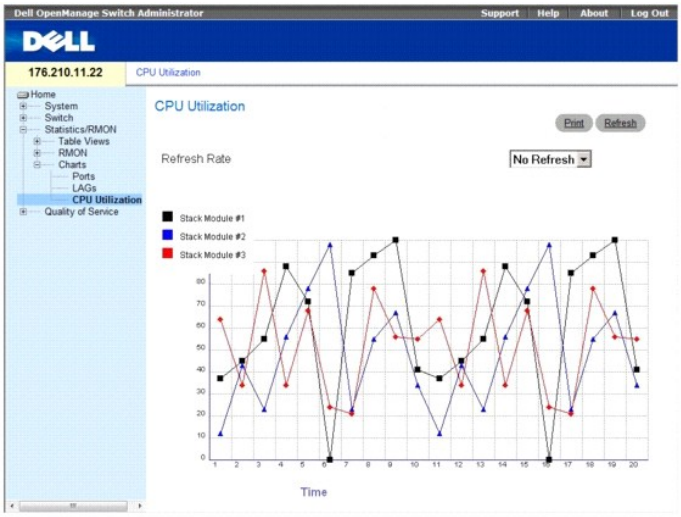
Команда консоли	Описание
show interfaces counters [**ethernet** *interface (интерфейс)* | **port-channel**- *port-channel-number (номер_канала_порта)*]	Отображает трафик, видимый физическим интерфейсом.
show rmon statistics {**ethernet** *interface (интерфейс)* | **port-channel** *port-channel-number (номер_канала_порта)*}	Отображает статистику удаленного мониторинга по Ethernet.
show gvrp statistics {**ethernet** *interface (интерфейс)* | **port-channel** *port-channel-number (номер_канала_порта)*}	Отображает статистику протокола GVRP.
show gvrp-error statistics {ethernet *интерфейс* | **port-channel** *порт-канал-номер*}	Отображает статистику ошибок протокола GVRP.

Просмотр страницы использования ЦП

На странице CPU Utilization (Использование ЦП) содержится информация об использовании ЦП системы и ресурсах ЦП в процентах, используемых каждым компонентом стека. Каждому компоненту стека на графике соответствует какой-либо цвет.

Чтобы открыть страницу CPU Utilization (Использование ЦП), щелкните **Statistics / RMON** (Статистика/RMON)→ **Charts** (Диаграммы)→ **CPU Utilization** (Использование ЦП) на панели дерева.

Рис. 8-16. CPU Utilization (Использование ЦП)



На странице CPU Utilization (Использование ЦП) содержится следующая информация.

- **Refresh Rate (Частота обновления)**. Период времени между обновлениями статистики интерфейса.

Просмотр страницы использования ЦП с помощью команд консоли

В следующей таблице приведены команды консоли для просмотра страницы использования ЦП.

Команда консоли	Описание
show cpu utilization	Отображает использование ЦП.

Далее приведен пример команд консоли.

```
Console# show cpu utilization

CPU utilization service is on.



CPU utilization

--------------------------

five seconds: 5%; one minute: 3%; five minutes: 3%
```

Назад на страницу Содержание

Назад на страницу Содержание

Настройка качества обслуживания

Руководство пользователя систем Dell™ PowerConnect™ 35xx

- Обзор качества обслуживания QoS
- Настройка общих параметров QoS

В этом разделе содержатся инструкции для определения и настройки параметров качества обслуживания (QoS). Чтобы открыть страницу **Quality of Service** (Качество обслуживания), выберите **Quality of Service** (Качество обслуживания) на панели дерева.

Обзор качества обслуживания QoS

Показатель Quality of Service (Качество обслуживания - QoS) позволяет обеспечить качество обслуживания и очередь приоритетов внутри сети.

К реализации, для которой необходима функция качества обслуживания (QoS), относятся некоторые типы трафика, например передача голоса, видеоизображения и трафик в реальном времени, для которых можно назначить очередь с высоким приоритетом, тогда как для другого трафика можно назначить очередь с низким приоритетом. Это позволяет ускорить прохождение первоочередного трафика.

Показатель QoS характеризуется следующими элементами.

- **Classification (Классификация)**. Определяет, какие поля соответствуют тем или иным значениям. Все пакеты, соответствующие пользовательским спецификациям, классифицируются вместе.
- **Action (Действие)**. Определяет управление трафиком, в котором пакеты пересылаются по информации о пакете, а также определяет значения полей пакетов, например приоритет VLAN (VPT) и DSCP (DiffServ Code Point).

Информация о классификации VPT

VLAN Priority Tags (Метки приоритета VLAN) используются для классификации пакетов путем их привязки к одной из очередей выхода. VLAN Priority Tag (Метка приоритета VLAN) для назначений очереди определяется пользователем. В таблице ниже представлена подробная информация по меткам VPT для параметров очереди по умолчанию.

Значение CoS	Значения очереди пересылки
0	q2
1	q1 (низший приоритет)
2	q1 (низший приоритет)
3	q2
4	q3
5	q3
6	q4
7	q4

Для непомеченных при поступлении пакетов по умолчанию назначается значение метки VPT, которое устанавливается отдельно для каждого порта. Назначенная метка VPT используется для привязки пакета к очереди выхода.

Значения DSCP можно поставить в соответствие очереди приоритетов. В следующей таблице представлена привязка DSCP по умолчанию к значениям очереди выхода.

Значение DSCP	Значения очереди пересылки
0-15	q1 (низший приоритет)
16-31	q2
32-47	q3
48-63	q4

Привязка DSCP активизируется индивидуально для каждой системы.

В этом разделе имеются следующие тематические подразделы:

- Обслуживание CoS

Обслуживание CoS

После постановки пакетов в определенную очередь выхода обслуживание CoS можно привязать к очереди (очередям). Настройка очередей выхода осуществляется с помощью схемы планирования одним из следующих способов.

- **Strict Priority (Строгий приоритет)**. Гарантирует, что чувствительные ко времени приложения передаются всегда. Strict Priority (Строгий приоритет) позволяет присвоить трафику, зависящему от целевого назначения и чувствительному ко времени, приоритет перед менее чувствительными ко времени приложениями.
  Например, в случае строгого приоритета, голосовой трафик по IP имеет приоритет, и IP трафик передается перед передачей трафика FTP или электронной почты (SMTP).
- **Weighted Round Robin**. Гарантирует, что одно приложение не будет использовать все ресурсы устройства по пересылке. С помощью WRR осуществляется пересылка всех очередей в цикле. Все очереди можно настроить по режимам очередей WRR или SP. Если выбран режим WRR, очередям присваиваются следующие веса: 1, 2, 4, 8.

Настройка общих параметров QoS

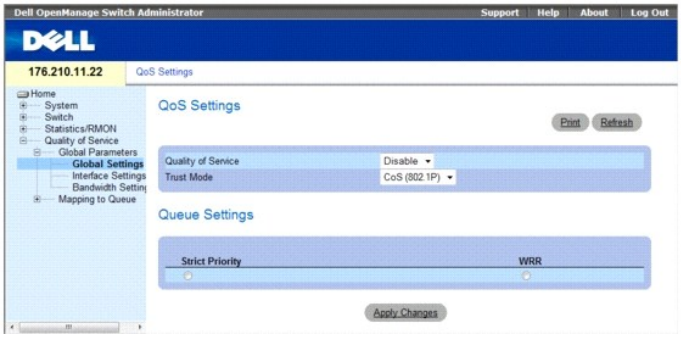
Показатель Quality of Service (Качество обслуживания - QoS) позволяет обеспечить качество обслуживания и очередь приоритетов внутри сети.

На странице **QoS Global Settings** (Общие параметры QoS) имеется поле для включения или отключения QoS. Там также имеется поле для выбора режима доверия (Trust mode). Trust mode (Режим доверия) основывается на предварительно определенных полях в пакете, чтобы определить очередь выхода.

Кроме того, страница **Global Settings** (Общие параметры) позволяет выполнять определение очередей как очереди высокого приоритета (SP) или приоритета типа (WRR).

Чтобы открыть страницу **Global Settings** (Общие параметры), выберите **Quality of Service** (Качество обслуживания)→ **QoS Parameters** (Параметры QoS)→ **Global Settings** (Общие параметры) на панели дерева.

Рис. 9-1. Общие параметры



Страница **Global Settings** (Общие параметры) содержит следующие разделы:

- Параметры QoS
- Параметры очереди

Параметры QoS

- **Quality of Service (Качество обслуживания)**. включает или отключает управление сетевым трафиком с помощью функции Quality of Service (Качество обслуживания).
- **Trust Mode (Режим доверия)**. определяет, какие поля пакета используются для классификации пакетов, входящих в устройство. Если ни одно правило не определено, трафик, содержащий предварительно определенные поля пакета (CoS или DSCP), будет привязан в соответствии с выбранным режимом доверия. Трафик, не содержащий предварительно определенные поля пакета, привязывается к очереди с максимально возможной скоростью доставки (q2). Ниже указаны возможные значения поля Trust Mode (Режим доверия).
  - **CoS** (802.1p). назначение очереди вывода определяется меткой приоритета IEEE802.1p VLAN (VPT) или меткой VPT по умолчанию, назначенной для порта. По умолчанию для устройства установлена метка IEEE802.1p.
  - **DSCP**. назначение очереди выхода определяется полем DSCP.

ПРИМЕЧАНИЕ. Параметры интерфейса Trust (Доверие) заменяют общие параметры Trust (Доверие).

Параметры очереди

- **Strict Priority (Строгий приоритет)**. При выборе этого параметра для очереди устанавливается строгий приоритет.
- **WRR**. При выборе этого параметра для очереди устанавливается строгий приоритет WRR.

Включение функции Class of Service (Качество обслуживания)

1. Откройте страницу **Global Settings** (Общие параметры).
2. Выберите **Enable** (Включено) в поле **Quality of Service** (Качество обслуживания).
3. Нажмите кнопку **Apply Changes** (Применить изменения).

   На устройстве будет включена функция Class of Service (Качество обслуживания).

Включение режима доверия:

1. Откройте страницу **Global Settings** (Общие параметры).
2. Укажите значение в поле **Trust Mode** (Режим доверия).
3. Нажмите кнопку **Apply Changes** (Применить изменения).

   На устройстве будет включен режим доверия.

Включение режима доверия с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для настройки полей, отображаемых на странице **Global Settings** (Общие параметры).

Команда консоли	Описание
qos trust [cos | dscp]	Настройка системы для использования режима доверия.
no qos trust	Возврат в состояние «без доверия».

Далее приведен пример команд консоли.

```
console(config)# qos trust dscp
```

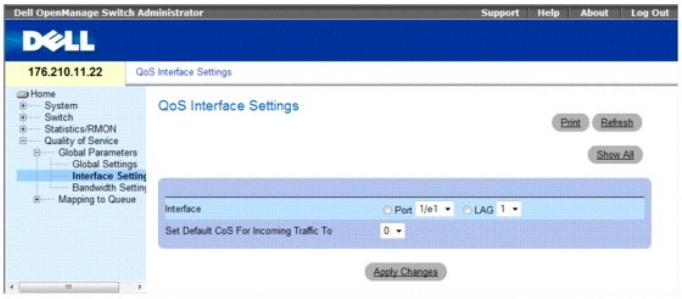
В этом разделе имеются следующие тематические подразделы:

- Определение параметров интерфейса QoS
- Определение параметров полосы пропускания
- Привязка значений CoS к очередям
- Привязка значений DSCP к очередям

Определение параметров интерфейса QoS

Страница **Interface Settings** (Параметры интерфейса) содержит поля, с помощью которых можно отключить режим доверия и настроить значение CoS по умолчанию для входящих непомеченных пакетов. Чтобы открыть страницу **Interface Settings** (Параметры интерфейса), выберите **Quality of Service** (Качество обслуживания)→ **QoS Parameters** (Параметры CoS)→ **Interface Settings** (Параметры интерфейса) на панели дерева.

Рис. 9-2. Страница Interface Settings (Параметры интерфейса)



Страница **Interface Settings** (Параметры интерфейса) содержит следующие поля:

- **Interface (Интерфейс)**. Определенный порт или группа LAG для настройки.
- **Disable «Trust» Mode on Interface (Отключить режим доверия для интерфейса)**. Отключает режим доверия для выбранного интерфейса. Этот параметр заменяет режим Trust (Доверие), настроенный на устройстве.
- **Set Default CoS For Incoming Traffic To (Задать CoS по умолчанию для входящего трафика)**. Определяет значение метки CoS по умолчанию для непомеченных пакетов. Метки CoS могут иметь значения от 0 до 7. Значение по умолчанию - 0.

Назначение параметров QoS для интерфейса

1. Откройте страницу **Interface Settings** (Параметры интерфейса).
2. Выберите интерфейс в поле **Interface** (Интерфейс).
3. Определите поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Параметры CoS будут назначены для интерфейса.

Отображение параметров QoS/CoS

1. Откройте страницу **Interface Settings** (Параметры интерфейса).
2. Нажмите кнопку **Show All** (Показать все).

   Появится таблица Interface (Интерфейс).

Назначение QoS для интерфейсов с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для настройки полей, отображаемых на странице **Interface Settings** (Параметры интерфейса).

Команда консоли	Описание
qos trust	Включает режим доверия.
no qos trust	Отключение состояния Trust (Доверие) для каждого порта.

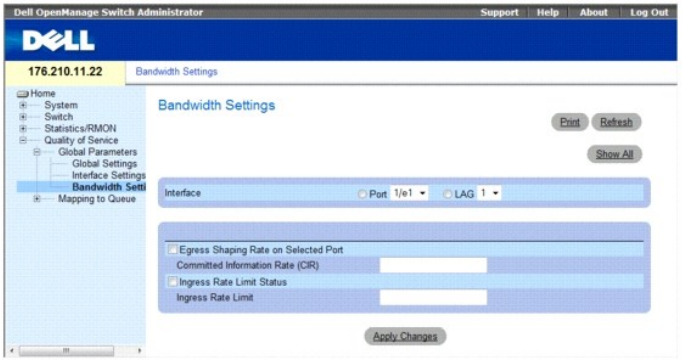
Далее приведен пример команд консоли.

```
console(config)# interface ethernet 1/e15

console(config-if)# qos trust
```

Определение параметров полосы пропускания

На странице **Bandwidth Settings** (Параметры полосы пропускания) находятся поля для определения параметров полосы пропускания для указанного выходящего интерфейса. Изменение графика очередей влияет на общие параметры очередей. Формирование очередей возможно на основе очередей и/или интерфейсов. Формирование определяется по наименьшей из указанных величин. Тип формирования очереди можно выбрать на странице Bandwidth Settings (Параметры полосы пропускания): на панели дерева выберите **Quality of Service** (Качество обслуживания)→ **CoS Global Parameters** (Общие параметры CoS)→ **Bandwidth Settings** (Параметры полосы пропускания).

Рис. 9-3. Параметры полосы пропускания



- **Interface (Интерфейс)**. указание порта или группы LAG, которые отображаются.
- **Egress Shaping Rate on Selected Port (Скорость формирования выхода для выбранного порта)**. Отображение состояния ограничения выходного трафика интерфейса.
  - *Флажок установлен*. Ограничение выходного трафика включено.
  - *Флажок снят.* Ограничение выходного трафика выключено.
- **Committed Information Rate (CIR) (Гарантированная скорость передачи данных (CIR))**. Определение ограничения выходного трафика CIR для интерфейса.
- **Ingress Rate Limit Status (Состояние ограничения скорости на входе)**. отображение состояния ограничения трафика на входе для интерфейса.
  - *Флажок установлен*. Ограничение входного трафика включено.
  - *Флажок снят.* Ограничение трафика на входе выключено.
- **Ingress Rate Limit (Ограничение скорости на входе)**. Определение ограничения трафика на входе для интерфейса.

Назначение параметров полосы пропускания для интерфейса:

1. Откройте страницу **Bandwidth Settings** (Параметры полосы пропускания).
2. Выберите интерфейс в поле **Interface** (Интерфейс).
3. Определите поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Параметры полосы пропускания будут назначены для интерфейса.

Отображение таблицы параметров полосы пропускания:

1. Откройте страницу **Bandwidth Settings** (Параметры полосы пропускания).
2. Нажмите кнопку **Show All** (Показать все).

   Отобразится таблица параметров полосы пропускания.

Рис. 9-4. Таблица параметров полосы пропускания

Присвоение параметров полосы пропускания с помощью команд консоли

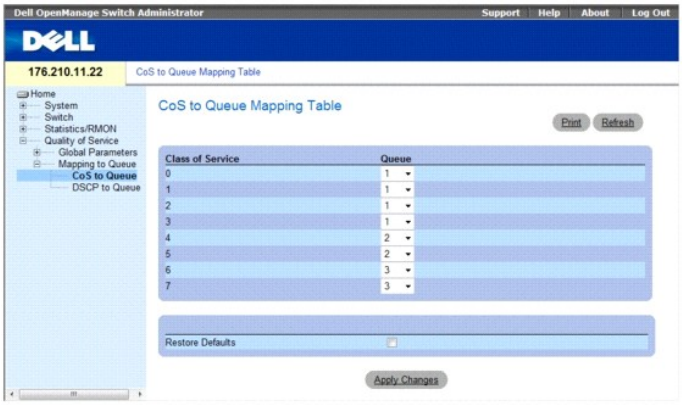
В следующей таблице приведены эквивалентные команды консоли для настройки полей, отображаемых на странице **Bandwidth Settings** (Параметры полосы пропускания).

Команда консоли	Описание
traffic-shape (форма трафика) *committed-rate* (гарантированная_скорость) [*committed-burst* (гарантированный_объем)] no traffic-shape (нет формы трафика)	Настройка формирователя для выходящего порта. Не используйте форму для отключения формирователя.
rate-limit *rate* no rate-limit	Ограничение скорости входящего трафика. Для отключения ограничения скорости используйте форму **no** (нет).

Привязка значений CoS к очередям

Страница **CoS to Queue** (Привязка CoS к очереди) содержит поля для классификации параметров CoS для очередей трафика. Чтобы открыть страницу **CoS to Queue** (Привязка CoS к очереди), выберите **Quality of Service** (Качество обслуживания)→ **QoS Mapping** (Привязка QoS)→ **CoS to Queue** (Привязка CoS к очереди) на панели дерева.

Рис. 9-5. Привязка CoS к очереди



Страница **CoS to Queue** (Привязка CoS к очереди) содержит следующие поля:

- **Class of Service (Класс обслуживания)**. определяет значения метки приоритета CoS, где 0 - это низший класс, а 7 - высший.
- **Queue (Очередь)**. очередь, к которой привязан приоритет CoS. Поддерживаются четыре очереди приоритета трафика.
- **Restore Defaults (Восстановить значения по умолчанию)**. восстанавливает заводские файлы устройства для привязки значений CoS к очереди пересылки.

Привязка значения CoS к очереди

1. Откройте страницу **CoS to Queue** (Привязка CoS к очереди).
2. Выберите запись CoS.
3. Определите номер очереди в поле **Queue** (Очередь).
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Значение CoS будет привязано к выходной очереди, а устройство обновлено.

Привязка значений CoS к очередям с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для настройки полей, отображаемых на странице **CoS to Queue** (Привязка CoS к очереди).

Команда консоли	Описание
wrr-queue cos-map *queue-id cos0.cos7*	Связь значений CoS для выделения приоритетных очередей выхода.

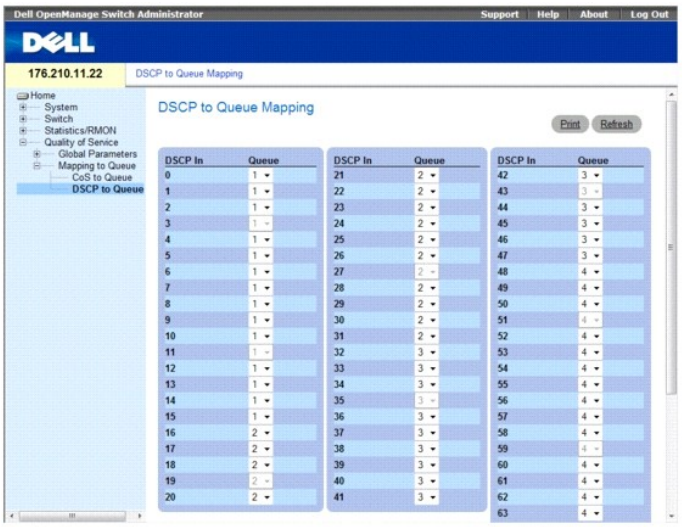
Далее приведен пример команд консоли.

```
console(config)# wrr-queue cos-map 7 4
```

Привязка значений DSCP к очередям

Страница **DSCP to Queue** (Привязка значений DSCP к очереди) содержит поля для назначения исходящих очередей конкретным полям DSCP. Чтобы открыть страницу **DSCP to Queue** (DSCP к очереди), выберите **Quality of Service** (Качество обслуживания)→ **QoS Mapping** (Привязка QoS)→ **DSCP to Queue** (DSCP к очереди) на панели дерева.

Рис. 9-6. DSCP к очереди



Страница **DSCP to Queue** (DSCP к очереди) содержит следующие поля:

- **DSCP In (DSCP входящего пакета)**. Значения в поле DSCP внутри входящего пакета.
- **Queue (Очередь)**. Очередь, для которой назначены пакеты с определенным значением DSCP. Значения: от 1 до 4, где 1 - это наименьшее значение, а 4 - наибольшее.
- **Restore Defaults (Восстановить значения по умолчанию)**. Восстанавливает заводские файлы устройства для привязки значений CoS к очереди пересылки.

Привязка значения DSCP и назначение очереди приоритета

1. Откройте страницу **DSCP to Queue** (DSCP к очереди).
2. Выберите значение в столбце **DSCP In** (DSCP входящего пакета).
3. Определите поле **Queue** (Очередь).
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   DSCP перезаписывается, а значение присваивается очереди выхода.

Привязка значений DSCP с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для настройки полей, отображаемых на странице **DSCP to Queue** (DSCP к очереди).

Команда консоли	Описание

qos map dscp-queue *dscp-list* **to** *идентификатор_очереди*	Изменение привязки DSCP к очереди.

Далее приведен пример команд консоли.

```
console(config)# qos map dscp-queue 33 40 41 to 1
```

Назад на страницу Содержание

Назад на страницу Содержание

Глоссарий

Руководство пользователя систем Dell™ PowerConnect™ 35xx

Этот глоссарий содержит основные технические термины, представляющие интерес.

А | Б | В | Д | Е | З | И | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Ц | Ш | D | F | G | I | L | N | O | R | S | U | V | W

А

Автоматическое согласование

Допускает использование портов 10/100 Мбит/с или 10/100/1000 Мбит/с Ethernet для установки следующих функций:

- Дуплексный и полудуплексный режим
- Управление потоком
- Скорость

ACL

Access Control List - список управления доступом. Позволяет сетевым администраторам определять классификационные действия и правила для определенных входных портов.

ARP

Address Resolution Protocol - протокол разрешения адресов. Этот протокол преобразует IP-адреса в физические адреса.

ASIC

Application Specific Integrated Circuit - специализированная интегральная схема. Заказная микросхема, разработанная для определенного приложения.

Б

Бод

Число сигнальных элементов, передаваемых за одну секунду.

В

Версия загрузчика

Версия загрузчика.

BootP

Bootstrap Protocol - протокол загрузки. Позволяет рабочей станции обнаружить свой IP-адрес, IP-адрес сервера BootP в сети или файл настройки, загруженный в систему загрузки модуля коммутатора.

BPDU

Bridge Protocol Data Unit - модуль данных мостового протокола. Предоставляет информацию о преобразовании данных в формате сообщения. Пакеты BPDU передаются вместе с информацией модуля коммутатора в составе настройки протокола Spanning Tree. Пакеты BPDU содержат информацию о портах, адресах, приоритетах и стоимости пересылки.

Входной порт

Порт, используемый для приема сетевого трафика.

Выходные порты

Порт, используемый для передачи сетевого трафика.

Выравнивание нагрузки

Обеспечивает равномерное распределение данных или пакетов для обработки между доступными ресурсами сети. Например, в результате выравнивания нагрузки входящие пакеты равномерно распределяются между всеми серверами или направляются на следующий доступный сервер.

Д

Дескриптор ресурса

Определяет ссылку на модуль коммутатора, задаваемую пользователем.

Домен

Совокупность компьютеров, программ и устройств в сети объединенная общими правилами и процедурами.

Динамический режим распределения VLAN (DVA)

- Обеспечивает автоматическое распределение пользователей по сетям VLANs при авторизации сервера RADIUS. После авторизации пользователя сервером RADIUS, пользователь автоматически подключается к сети VLAN, конфигурация которой произведена сервером RADIUS.

Дуплексный режим

Позволяет одновременно передавать и принимать данные. Существует два типа дуплексного режима:

- **Полный дуплексный режим**. Обеспечивает бисинхронную передачу, например по телефону. Две стороны могут одновременно передавать информацию.
- **Полудуплексный режим**. Обеспечивает асинхронную передачу, например по портативной радиостанции. Передачу информации может одновременно осуществлять только одна сторона.

Е

Ethernet

Ethernet стандартизирован по IEEE 802.3. Ethernet – это наиболее распространенный стандарт, используемый для локальной сети. Поддерживает следующие скорости передачи данных: 10, 100 или 1000 Мбит/с.

EWS

Embedded Web Server - встроенный веб-сервер. Используется для управления устройством с помощью стандартного обозревателя. Встроенные веб-серверы используются в дополнение либо вместо CLI или NMS.

З

Зеркалирование портов

Контролирует и дублирует сетевой трафик путем пересылки копий входящих и исходящих пакетов с одного порта на другой (контролирующий).

Дополнительную информацию о зеркалировании портов см. в разделе **Определение сеансов с зеркалированием портов**.

Запрос

Извлекает информацию из базы данных и предоставляет информацию для использования.

И

ИС

Интегральная схема. Интегральные схемы – это небольшие электронные устройства, состоящие из полупроводникового материала.

К

Кадр

Пакеты, содержащие информацию заголовка и заключительной части, необходимую для физической среды.

Класс обслуживания

Класс обслуживания (CoS). Класс обслуживания является схемой приоритетов стандарта 802.1p. CoS обеспечивает способ маркировки пакетов, содержащих приоритетную информацию. Значение CoS от 0 до 7 добавляется к заголовку Layer II пакетов, где ноль означает самый низкий приоритет, а семь – самый высокий.

Перекрывающаяся передача двух или нескольких конфликтующих пакетов. Переданные данные использовать невозможно, и сеанс начинается заново.

Клиент DHCP

Устройство, использующее протокол DHCP для получения параметров конфигурации, например сетевого адреса.

Коммутатор

Фильтрует и пересылает пакеты из одного сегмента локальной сети в другой. Маршрутизаторы поддерживают любые типы пакетных протоколов.

Л

«Лавина» широковещательной передачи

Результат чрезмерного количества широковещательных сообщений, одновременно переданных по сети через один порт. Ответы на пересылаемые сообщения являются причиной чрезмерной нагрузки на сеть, перегружая ее ресурсы или вызывая задержки в сети.

Дополнительную информацию о «лавинах» широковещательной передачи см. в разделе Определение параметров LAG.

ЛВС

Local Area Network - локальная (вычислительная) сеть. Сеть, развернутая в одном помещении, здании, на одной территории или в пределах другой географически ограниченной области.

M

Максимально возможная скорость доставки

Трафик назначается для очереди с низшим приоритетом, и доставка пакетов не гарантируется.

MAC-адрес

Адрес Media Access Control. MAC-адрес – это аппаратный адрес, определяющий каждый узел в сети.

Маска

Фильтр, включающий или исключающий определенные значения, например части IP-адреса.

Например, если Блок 2 вставляется на первой минуте десятиминутного цикла, а Блок 1 вставляется на пятой минуте этого же цикла, они будут рассматриваться как блоки одного периода.

Маска ввода

Указывает, какие биты IP-адреса используются, а какие игнорируются. Маска ввода модуля коммутатора 255.255.255.255 указывает, что нет важных битов. Маска ввода 0.0.0.0 указывает, что все биты важны.

Маска подсети

Используется для замены всего IP-адреса или его части, которые используются в адресе подсети.

Маршрутизатор

Устройство, устанавливающее соединение с отдельной сетью. Маршрутизаторы пересылают пакеты между двумя или несколькими сетями. Маршрутизаторы работают на уровне Layer 3.

Многоадресная передача

Передает копии одного и того же пакета на несколько портов.

Мост

Устройство, соединяющее две сети. Мосты могут быть оснащены разным аппаратным обеспечением, но при этом не зависят от протоколов. Мосты функционируют на уровнях Layer 1 и Layer 2.

MD5

Message Digest 5 - профиль сообщения 5. Алгоритм, создающий 128-разрядную хеш-строку. MD5 является разновидностью алгоритма MD4, который обеспечивает большую безопасность по сравнению с MD4. MD5 проверяет целостность передаваемых данных, а также определяет источник передаваемых данных.

MDI

Media Dependent Interface - интерфейс, зависящий от среды. Кабель, используемый для оконечных станций.

MDIX

Media Dependent Interface with Crossover - интерфейс, зависящий от среды, с перекрещиванием. Кабель, используемый для концентраторов и коммутаторов.

MIB

Management Information Base - база управляющей информации. В базах MIB содержится информация, описывающая определенные аспекты сетевых компонентов.

H

Наблюдение по протоколу DHCP

Наблюдение по протоколу DHCP усиливает безопасность сети, обеспечивая с помощью брандмауэра защиту между серверами DHCP и ненадежными интерфейсами.

Наблюдение по протоколу IGMP

Наблюдение на базе протокола IGMP проверяет содержимое кадров IGMP, когда они пересылаются коммутатором от рабочих станций на многоадресные маршрутизаторы. Кадр позволяет устройству определить рабочие станции, настроенные для многоадресных сеансов, а также, какие маршрутизаторы посылают многоадресные кадры.

Назначение полосы пропускания

Часть полосы пропускания, назначенная для определенного приложения, пользователя или интерфейса.

Настройка для запуска

Сохраняет полную настройку модуля коммутатора при его отключении или перезагрузке.

HOL

Head of Line - защита от блокировки очереди. Для пакетов устанавливается очередь. Пакеты, стоящие в начале очереди, пересылаются до пакетов, находящихся в конце очереди.

HTTP

Протокол HTTP (HyperText Transport Protocol). Используется для обмена документами формата HTML через Интернет между серверами и клиентами.

О

Одноадресная передача

Форма пересылки, при которой один пакет передается одному пользователю.

Объединенные VLAN

Группа нескольких сетей VLAN, объединенных в одну сеть VLAN. Объединение VLAN позволяет маршрутизаторам отвечать на запросы ARP для узлов, расположенных в разных подсетях VLAN, принадлежащих одной общей сети VLAN. Маршрутизаторы отвечают, используя собственные MAC-адреса.

Объединительная плата

Основная шина, которая используется для передачи информации в модуле коммутатора.

Обратное давление

Этот механизм используется в полудуплексном режиме и позволяет отключить получение сообщений на порты.

Оконечная система

Устройство конечного пользователя в сети.

OID

Организационно-уникальные идентификаторы. Идентификаторы, связанные с голосовыми сетями VLAN.

OUI

Object Identifier - идентификатор объекта. Используется в SNMP для идентификации управляемых объектов. В схеме сетевого управления «управляющее устройство/агент SNMP» каждый управляемый объект должен иметь идентифицирующий его OID.

П

Пакеты

Блоки информации, предназначенные для передачи в системах коммутирования пакетов.

Переключение

Переключение происходит, когда состояние интерфейсов постоянно меняется. Например, состояние порта STP постоянно изменяется с прослушивания на распознавание, а затем на пересылку. Это может привести к потере трафика.

Полоса пропускания

Полоса пропускания указывает объем данных, которые могут быть переданы за определенный период времени. Для цифровых модулей коммутаторов полоса пропускания указывается в битах в секунду (бит/с) или байтах в секунду.

Порт

Физические порты обеспечивает связь между компонентами, что позволяет микропроцессорам устанавливать связь с периферийным оборудованием.

Подсеть

Подсеть. Подсети – это части сети, использующие общий компонент адреса. В сетях TCP/IP устройства, использующие одинаковый префикс, являются частями одной и той же сети. Например, все устройства с префиксом 157.100.100.100 являются частями одной и той же сети.

Прерывание

Сообщение, отправленное по протоколу SNMP, означающее, что произошло системное событие.

Профили доступа

Позволяют сетевым администраторам определять профили и правила доступа к модулю коммутатора. Можно ограничить доступ к функциям управления группам пользователей, которые определены следующими критериями:

- входящими интерфейсами;
- исходными IP-адресами или маской исходной подсети.

Профили проверки подлинности

Набор правил, с помощью которых осуществляется вход и проверка подлинности пользователей и приложений.

Протокол

Набор правил, управляющий тем, как устройства обмениваются информацией по сети.

Протокол STP (Spanning Tree Protocol)

Исключает образование циклов сетевого трафика. Протокол STP (Spanning Tree Protocol) предоставляет древовидную топологию для любого расположения мостов. STP обеспечивает единственный путь между конечными станциями сети и исключает циклы.

P

Распознавание MAC-адреса

Распознавание MAC-адреса характеризует мост распознавания, в котором записывается MAC-адрес источника пакета. Пакеты, направляемые на этот адрес, пересылаются только на интерфейс моста, на котором находится этот адрес. Пакеты, направляемые на неизвестные адреса, пересылаются на интерфейсы всех мостов. Распознавание MAC-адреса минимизирует трафик в локальной сети, к которой выполнено подключение.

Режим доступа

Определяет метод, с помощью которого пользователь получает доступ к системе.

PDU

Protocol Data Unit - модуль данных протокола. Модуль данных, указанный в протоколе уровня и состоящий из управляющей информации протокола и пользовательских данных уровня.

PING

Packet Internet Groper - отправитель Интернет-пакетов. Проверяет доступность конкретного IP-адреса. Пакет отправляется на другой IP-адрес и ожидает ответа.

PVE

*Протокол VLAN Edge.*Порт может быть задан как порт PVE (Private VLAN Edge) порта соединения с магистралью, таким образом, что он будет изолирован от других портов той же сети VLAN.

C

CLI

Command Line Interface - интерфейс командной строки. Набор команд, указываемых в строке, которые используются для настройки системы. Дополнительную информацию по использованию консоли CLI см. в разделе **Использование режима командной строки**.

Сообщества

Указывает группу пользователей, для которой сохраняются одинаковые права для доступа к системе.

Сервер

Центральный компьютер, предоставляющий службы другим компьютерам в сети. Службы могут включать хранение файлов и доступ к приложениям.

Сегментация

Делит локальные сети на отдельные сегменты локальной сети для установки связи. Сегментация позволяет преодолеть ограничения полосы пропускания в локальной сети.

Скорость порта

Означает скорость порта. Существуют следующие скорости портов:

- Ethernet 10 Мбит/с
- Fast Ethernet 100 Мбит/с
- Gigabit Ethernet 1000 Мбит/с

Создание транков

Объединение каналов. Оптимизирует использование портов, связывая между собой группу портов и формируя один транк (объединенные группы).

CDB

Configuration Data Base - база данных конфигурации. Файл, содержащий информацию о конфигурации устройства.

Т

Telnet

Протокол Telnet (Terminal Emulation Protocol). Обеспечивает пользователям системы возможность входа в удаленные сети и использования имеющихся в них ресурсов.

TCP/IP

Протокол TCP (Transmission Control Protocol). Обеспечивает двум хостам возможность установки связи и обмена потоками данных. TCP гарантирует доставку пакета, а также передачу и прием пакетов в порядке их отправки.

TFTP

Протокол TFTP (Trivial File Transfer Protocol). Использует протокол UDP (User Data Protocol) без функций защиты для передачи файлов.

У

Узел

Конечная точка сетевого соединения или обычная точка пересечения нескольких сетевых линий. К узлам относятся:

- процессоры;
- контроллеры;
- рабочие станции.

Управление потоком

Позволяет низкоскоростным устройствам осуществлять связь с высокоскоростными устройствами. При этом высокоскоростные устройства делают паузы между отправкой пакетов.

Уровень MAC

Подуровень уровня *DTL* (Data Link Control).

Ф

Файл образа

Системные образы сохраняются в двух секторах Flash, называемых образами (Image 1 и Image 2). Активный образ хранит активную копию, другой образ - вторую копию.

Файл рабочей настройки

Содержит все команды файла настройки для запуска, а также все команды, введенные во время последнего сеанса. После выключения питания или перезагрузки модуля коммутатора все команды, сохраненные в файле рабочей настройки, теряются.

Файл резервной настройки

Содержит резервную копию настройки модуля коммутатора. Резервный файл настройки изменяется, когда в него копируется файл рабочей настройки или файл настройки для запуска.

Фрагмент

Пакеты Ethernet размером менее 576 бит.

Х

Хост

Компьютер, являющийся источником информации или служб для других компьютеров.

Ц

ЦП

Центральный процессор. Часть компьютера, в которой обрабатывается информация. ЦП состоят из управляющего устройства и арифметико-логического устройства.

Ш

Широковещательная передача

Метод передачи пакетов на все порты в сети.

Широковещательный домен

Группы устройств, получающие широковещательные кадры, которые передаются любым устройством, входящим в назначенную группу. Маршрутизаторы связывают широковещательные домены, так как маршрутизаторы не пересылают широковещательных кадров.

D

DRAC/MC

DRAC/MC. Является единой точкой управления для компонентов системы модульного сервера Dell.

DSCP

DiffServe Code Point - точка кодов DiffServe. DSCP обеспечивает способ маркировки IP-пакетов с помощью информации о приоритетах QoS.

F

FIFO

First In First Out - метод «первым пришел - первым обслужен». Процедура установки очередности, когда первым пакетом в очереди является первый из поступивших пакетов.

FFT

Fast Forward Table - таблица быстрой пересылки. Предоставляет информацию о маршрутах пересылки. Если на устройство поступает пакет с известным маршрутом, то он пересылается по маршруту, указанному в FFT. Если маршрут не известен, ЦП пересылает пакет и обновляет FFT.

G

GARP

Протокол GARP (General Attributes Registration Protocol). Регистрирует клиентские компьютеры в многоадресном домене.

Gigabit Ethernet

Gigabit Ethernet позволяет передавать данные со скоростью 1000 Мбит/с и совместим со стандартами Ethernet 10/100 Мбит/с.

GVRP

Протокол регистрации GARP VLAN (GVRP). Регистрирует клиентские компьютеры в группах VLAN.

I

IEEE

Institute of Electrical and Electronics Engineers - Институт инженеров по электротехнике и электронике. Организация, занимающаяся разработкой стандартов связи и использования сетей.

IEEE 802.1d

Мост стандарта IEEE 802.1d, используемый в протоколе STP, поддерживает MAC-преобразование, позволяющее исключить образование сетевых контуров.

IEEE 802.1p

Устанавливает приоритет для сетевого трафика на уровне канала передачи данных или подуровне MAC.

IEEE 802.1Q

Определяет работу мостов VLAN, при которой возможно определение, работа и администрирование групп VLAN внутри инфраструктур локальных сетей с мостами.

ICMP

Протокол ICMP (Internet Control Message Protocol). Позволяет шлюзу или хосту назначения устанавливать связь с хостом, являющимся источником данных, например для передачи отчета об ошибке обработки.

IP

Internet Protocol - протокол Интернета. Определяет формат пакетов и способ назначения адресов для них. IP назначает пакетам адреса и пересылает пакеты на нужный порт.

IP-адрес

Адрес по протоколу Интернета. Уникальный адрес, назначаемый сетевому устройству, подключенному к двум или нескольким локальным или глобальным сетям.

IP, версия 6 (IPv6)

Версия систем обработки IP-адресов, позволяющая работать с более длинными адресами, чем традиционная IPv4. Адреса системы IPv6 имеют длину 128 бит, в то время как в версии IPv4 адреса имеют длину 32 бита; предоставляя больше свободного пространства для адресов.

ISATAP

Протокол автоматической туннельной внутриобъектной адресации.
ISATAP представляет собой автоматический механизм туннелирования, который использует сеть IPv4 в качестве слоя звена циркулярного доступа для IPv6. Протокол ISATAP предназначен для передачи пакетов IPv6 в пределах объекта в случаях, когда его собственная инфраструктура IPv6 еще не организована.

L

LAG

Link Aggregated Group - объединенная группа каналов. Объединяет порты или группы VLAN в единый виртуальный порт или единую группу VLAN.

Дополнительную информацию о группах LAG см. в разделе **Определение членства в группе LAG**.

Layer 2

Уровень канала передачи данных или уровень MAC. Содержит физический адрес клиентского компьютера или сервера. Обработка на уровне Layer 2 выполняется быстрее обработки на уровне Layer 3 из-за меньшего объема обрабатываемой информации.

Layer 4

Устанавливает соединение и обеспечивает доставку всех данных в место их назначения. Пакеты, проверяемые на уровне Layer 4, анализируются, и решения о пересылке принимаются на основе того, как они используются.

LLDP-MED

Link Layer Discovery Protocol - Media Endpoint Discovery (Выявление конечной медиа-точки по протоколу обнаружения каналов передачи данных). Протокол LLDP позволяет сетевым администраторам выполнять поиск и устранение неисправностей и совершенствовать управление сетью путем выявления и сохранения топологии сети в средах, включающих оборудование самых разных поставщиков. Расширение протокола MED повышает гибкость сети, давая возможность различным системам IP использовать один сетевой протокол LLDP.

N

NA

Neighbor Advertisement - сообщение «соседнего» узла.

ND - Neighbor Discovery - обнаружение «соседнего» узла

Протокол обнаружения соседнего узла.

NMS

Network Management System - система сетевого управления. Интерфейс, обеспечивающий управление системой.

NS

Neighbor Solicitation - запрос обнаружения «соседнего» узла.

Q

QoS

Quality of Service - качество обслуживания. QoS позволяет сетевым администраторам решить, каким образом и какая часть сетевого трафика пересылается в зависимости от приоритетов, типов приложений, а также адресов источников и мест назначения.

R

RA

Сообщение сервера RADIUS.

RADIUS

Служба Remote Authentication Dial-In User Service. Способ проверки пользователей системы и отслеживания времени соединения.

RMON

Remote Monitoring - удаленный мониторинг. Предоставляет возможность сбора сетевой информации с одной рабочей станции.

RD

RADIUS Discovery - обнаружение сервера RADIUS.

RS

Router Solicitation - запрос маршрутизатора.

RSTP

Протокол RSTP (Rapid Spanning Tree Protocol). Выявляет и использует топологию сети, обеспечивая лучшую сходимость для протокола STP без образования циклов пересылки.

S

SNMP

Протокол SNMP (Simple Network Management Protocol). Управляет локальными сетями. Программное обеспечение, использующее SNMP, осуществляет связь с сетевыми устройствами со встроенными агентами SNMP. Агенты SNMP собирают информацию о работе в сети и состоянии устройства и отправляют эту информацию назад на рабочую станцию.

SNTP

Протокол SNTP (Simple Network Time Protocol). Протокол SNTP гарантирует точность синхронизации времени такта сетевого коммутатора до миллисекунды.

SoC

System on a Chip - система в микросхеме. Специализированная интегральная схема (ASIC), в которой содержится вся система. Например, телекоммуникационная SoC может содержать микропроцессор, процессор цифровых сигналов, оперативную (RAM) и постоянную (ROM) память.

SSH

Протокол SSH (Secure Shell). Обеспечивает вход на другой компьютер сети, а также позволяет выполнять команды на удаленном компьютере и передавать файлы с одного компьютера на другой. Secure Shell обеспечивает строгую проверку подлинности и методы безопасного соединения по незащищенным каналам.

U

UDP

Протокол UDP (User Data Protocol). Передает пакеты, но не гарантирует их доставку.

V

VLAN

Virtual Local Area Network - виртуальная локальная (вычислительная) сеть. Логические подгруппы локальной сети (ЛВС), созданные программным, а не аппаратным путем.

VoIP

Voice over IP. Протокол VoIP, голос через IP

W

WAN

Wide Area Network - глобальная (вычислительная) сеть. Сеть, действующая в пределах большой географической зоны.

Назад на страницу Содержание