Системы Dell™ PowerConnect™ 34XX Руководство пользователя

Примечания, предупреждения и предостережения

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

ЗАМЕЧАНИЕ. ПРЕДУПРЕЖДЕНИЕ указывает на возможность повреждения оборудования или потери данных и объясняет, как этого избежать.

ПРЕДУПРЕЖДЕНИЕ. ПРЕДОСТЕРЕЖЕНИЕ указывает на потенциальную опасность повреждения, получения легких травм или угрозу для жизни.

Март 2005

Назад на страницу Содержание

Введение

Системы Dell™ PowerConnect™ 34XX Руководство пользователя

Устройства PowerConnect 3424/3448 и PowerConnect 3424P/3448P представляют собой наращиваемые усовершенствованные коммутаторы многоуровневой структуры. Устройства PowerConnect могут работать либо как автономные коммутаторы -многоуровневой структуры, либо как наращиваемые коммутаторы с возможностью использования до шести компонентов стека.

В этом *Руководстве пользователя* содержится необходимая информация по установке, настройке и техническому уходу за устройством.

Описание системы

Коммутаторы PowerConnect 3424/3448 и PowerConnect 3424P/3448P универсальны и просты в управлении. PowerConnect серий 3424 и 3448 включают в себя следующие виды устройств:

- Коммутатор PowerConnect 3424
- PowerConnect 3424P
- Коммутатор PowerConnect 3448
- Коммутатор PowerConnect 3448P

Коммутатор PowerConnect 3424

PowerConnect 3424 предоставляет 24 порта со скоростью передачи 10/100Мбит/с, два порта SFP и два порта Copper, которые могут использоваться для пересылки трафика в автономном блоке или в качестве стековых портов в стековом блоке. В устройстве также имеется один консольный порт типа RS-232. PowerConnect 3424 является стековым устройством, но оно может работать и в автономном режиме.

PowerConnect 3424P

PowerConnect 3424P предоставляет 24 порта со скоростью передачи 10/100Мбит/с, два порта SFP и два порта Copper, которые могут использоваться для пересылки трафика в автономном блоке или в качестве стековых портов в стековом блоке. В устройстве также имеется один консольный порт типа RS-232. PowerConnect 3424P является стековым устройством, но оно может работать и в автономном режиме. В коммутаторе PowerConnect 3424P также есть блок питания с поддержкой технологии питания через сеть Ethernet (PoE).

Рисунок 1-1. Коммутаторы PowerConnect 3424 и PowerConnect 3424P

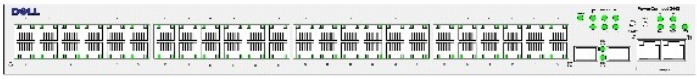
Коммутатор PowerConnect 3448

PowerConnect 3448 предоставляет 48 портов со скоростью передачи 10/100Мбит/с, два порта SFP и два порта Copper, которые могут использоваться для пересылки трафика в автономном блоке или в качестве стековых портов в стековом блоке. В устройстве также имеется один консольный порт типа RS-232. PowerConnect 3448 является стековым устройством, но оно может работать и в автономном режиме.

Коммутатор PowerConnect 3448P

PowerConnect 3448P предоставляет 48 портов со скоростью передачи 10/100Мбит/с, два порта SFP и два порта Copper, которые могут использоваться для пересылки трафика в автономном блоке или в качестве стековых портов в стековом блоке. В устройстве также имеется один консольный порт типа RS-232. Кроме того, коммутатор PowerConnect 3448P предоставляет поддержку технологии питания через сеть Ethernet (PoE).

Рисунок 1-2. Коммутаторы PowerConnect 3448 и PowerConnect 3448P



Обзор стекирования

Стекирование в коммутаторах PowerConnect 3424/P и PowerConnect 3448/P обеспечивает управление несколькими устройствами из одной точки, как если бы все компоненты стека были одним устройством. Доступ ко всем компонентам стека осуществляется через единый IP-адрес, который служит для управления стеком. Управление стеком происходит через:

- Веб-интерфейс
- Станцию управления SNMP
- Режим командной строки (CLI)

Коммутаторы PowerConnect 3424/P и PowerConnect 3448/P позволяют стекировать до шести компонентов в одном стеке или могут работать в качестве автономного устройства.

Во время настройки стекирования один коммутатор выбирается к качестве главного стекового устройства, а другой компонент может использоваться какрезервное устройство. Все остальные устройства назначаются обычными компонентами стека, и им присваивается уникальный идентификатор устройства.

Программное обеспечение коммутатора загружается отдельно для каждого компонента стека. Тем не менее, для всех компонентов стека должна использоваться одна и та же версия программного обеспечения.

Стекирование коммутаторов и их конфигурация поддерживается с помощью главного стекового устройства. Главное стековое устройство распознает и корректирует конфигурацию портов с минимальным воздействием на работу в следующих случаях:

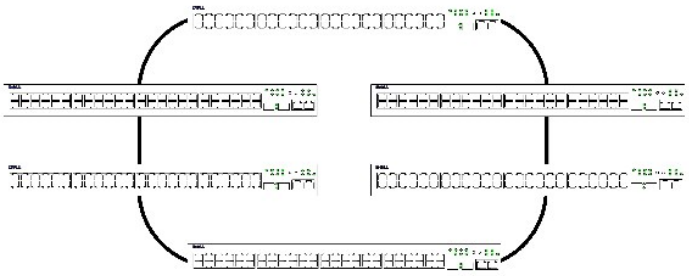
- Сбой устройства
- Сбой связи между устройствами в стеке
- Добавление устройства
- Удаление устройства из стека

Понятие топологии стека

Коммутаторы PowerConnect серии 3400 работают по кольцевой топологии. Стековая кольцевая топология подразумевает подсоединение всех устройств в стеке по кругу. Каждое устройство в стеке получает данные и передает их на следующее устройство. Пакет передается по стеку до тех пор, пока он не достигнет цели. Система разрабатывает оптимальный путь передачи трафика.

Рисунок 1-3. Стековая кольцевая топология

Кольцевая топология



Большинство проблем при работе по кольцевой топологии возникает из-за неисправности одного из компонентов в цепи или повреждения связи. При наличии стеков PowerConnect 3424/P и PowerConnect 3448/P происходит автоматическое переключение системы на топологию, используемую в случае сбоя работы в стеке, без замедления в работе системы. Автоматически выдается сообщение протокола SNMP, при этом не требуется выполнение какого-либо дополнительного действия по управлению стеком. Тем не менее, необходимо отремонтировать поврежденное соединение или компонент, чтобы восстановить целостность стека.

После того, как неисправность устранена, можно снова подключить устройство к стеку, и кольцевая топология будет восстановлена.

Топология для переключения в случае сбоя в стеке

В случае сбоя в топологии стека он переключается на топологию, используемую в случае сбоя работы. При такой топологии устройства расположены в цепи последовательно. Главное стековое устройство определяет, куда передаются пакеты. Каждый из компонентов (кроме верхнего и нижнего) подключен к двум соседним устройствам.

Компоненты стека и идентификатор устройства

Идентификаторы устройства - это важные элементы конфигурации стека. Режим стековых операций определяется во время загрузки. Операционный режим задается в зависимости от идентификатора устройства, выбранного во время процесса инициализации. Например, если пользователь выбрал автономный режим работы, устройство загружается как автономный коммутатор.

Компоненты устройства поставляются с идентификатором устройства, заданным по умолчанию для автономного блока. Если устройство работает автономно, все стековые индикаторы выключены.

В случае, если пользователь выбирает другой идентификатор устройства, его значение не удаляется и остается действительным даже после перезагрузки устройства.

Идентификаторы 1 и 2 зарезервированы для устройств, работающих от главного стекового устройства. Идентификаторы 3 - 6 могут быть назначены для компонентов стека.

Когда загружается главное устройство или вставляется либо удаляется компонент стека, главное устройство инициирует процесс распознования устройств в стеке.

ПРИМЕЧАНИЕ. При обнаружении в стеке двух компонентов с одинаковым идентификатором стек продолжает работать, при этом в составе стека функционирует тот компонент, который был подключен раньше. Пользователь получает сообщение, что устройство не удалось подключить к стеку.

Удаление и замена компонентов стека

Устройства 1 и 2 работают от главного стекового устройства. Устройства 1 и 2 обозначены либо как главное устройство, либо как главное резервное устройство. Назначение главного стекового устройства выполняется во время процесса настройки. Один компонент, работающий от главного устройства, назначается главным стековым устройством, а другой - главным резервным в соответствии со следующей процедурой принятия решений:

- При наличии только одного устройства, работающего от главного, оно назначается главным.
- Если имеются два устройства, работающих от главного, одно из которых пользователь вручную настроил как главное стековое устройство,

главным стековым устройством считается то, которое было настроено вручную.

- При наличии двух устройств, работающих от главного, ни одно из которых не было настроено вручную как главное, главным стековым устройством считается то, которое было подключено раньше.
- При наличии двух устройств, работающих от главного и настроенных как главное устройство, главным стековым устройством считается то, которое было подключено раньше.
- Если оба компонента стека подключены одновременно, устройство 1 выбирается в качестве главного стекового устройства.

ПРИМЕЧАНИЕ. Считается, что стеки подключены одновременно, если разница во времени подключения не превышает десяти минут.

Например, если устройство 2 подключено на первой минуте десятиминутного цикла, а устройство 1 - на пятой того же самого цикла, считается, что они подключены одновременно. При наличии двух компонентов стека, работающих от главного устройства и подключенных одновременно, устройсво 1 выбирается в качестве главного стекового устройства.

Главное стековое и главное резервное устройства обеспечивают работу в "теплом" резервном режиме. "Теплый" резервный режим гарантирует, что в случае сбоя главное резервное устройство начнет выполнять функции главного стекового устройства. Таким образом гарантируется бесперебойная работа стека.

Во время работы в "теплом" резервном режиме главное стековое и главное резервное устройства синхронизированы только со статическими параметрами настройки. Если главное стековое устройство настроено, оно должно синхронизировать параметры главного резервного устройства. Динамические параметры не сохраняются. Например, динамически опознанные MAC-адреса не сохраняются.

Каждый порт в стеке имеет свою собственную комбинацию идентификатора устройства Unit ID/тип порта и номера порта, которая используются как в командах конфигурирования, так и в файлах конфигурации. Файлами конфигурации можно управлять только из главного стекового устройства, включая:

- Сохранение во флэш-память
- Выгрузка файлов конфигурации на внешний TFTP-сервер
- Загрузка файлов конфигурации из внешнего TFTP-сервера

ПРИМЕЧАНИЕ. Конфигурация стека для всех настроенных портов сохраняется даже в том случае, когда стек перегружается и/или портов больше не существует.

При каждой перезагрузке выполняется процедура диагностики топологии, и в главное устройство поступает информация о всех компонентах стека. Идентификаторы устройства сохраняются в коммутаторе и распознаются в процессе диагностики топологии. При попытке загрузить коммутатор, который работает не в автономном режиме, не выбрав предварительно главное устройство, коммутатор не загрузится.

Файлы конфигурации можно изменить только по явной пользовательской конфигурации. Файлы конфигурации не изменяются автоматически в следующих случаях:

- Добавление устройства
- Удаление устройства
- Переназначение идентификаторов устройств
- Переход утройства из режима стекирования в автономный режим и обратно

Каждый раз при перезагрузке системы файл конфигурации для запуска, находящийся в главном устройстве, используется для настройки стека.

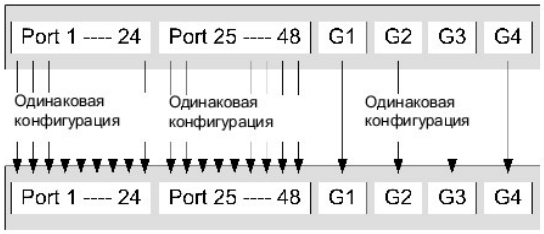
Если компонент удаляется из стека, а затем заменяется на другой с таким же идентификатором устройства, компонент стека настраивается по параметрам первоначального устройства. На странице OpenManage Switch Administrator отображаются только порты, которые физически присутствуют в системе и могут быть настроены через веб-интерфейс. Отсутствующие порты настраиваются через режим командной строки или протокол SNMP.

Замена компонентов стека

Если компонент стека заменяется на другой с таким же идентификатором устройства, новый компонент стека настраивается по параметрам первоначального устройства. Если количество портов в новом устройстве не совпадает с предыдущим (т.е. их больше или меньше), то к новому компоненту стека применяется конфигурация соответствующих портов. Например,

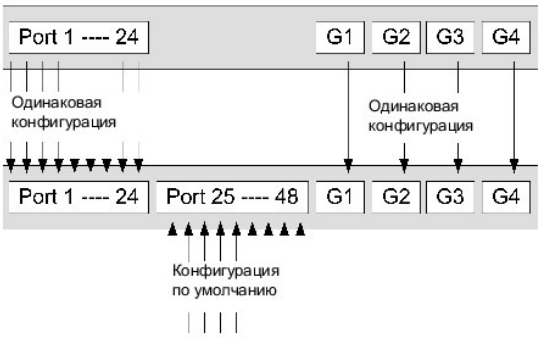
- Если PowerConnect 3424/P устанавливается вместо PowerConnect 3424/P, все параметры настройки порта остаются неизменными.
- Если PowerConnect 3448/P устанавливается вместо PowerConnect 3448/P, все параметры настройки порта остаются неизменными.

Рисунок 1-4. PowerConnect 3448/P устанавливается вместо PowerConnect 3448/P



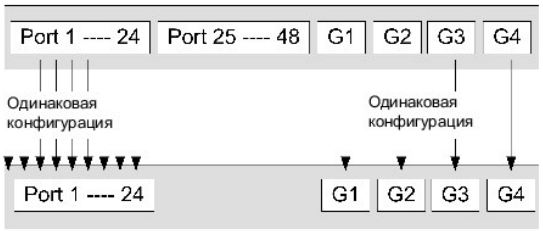
- Если PowerConnect 3448/P устанавливается вместо PowerConnect 3424/P, на первые 24 FE-порта коммутатора 3448/P передается конфигурация 24 FE-портов коммутатора 3424/P. Конфигурация GE-порта остается неизменной. Остальные порты получают конфигурацию по умолчанию.

Рисунок 1-5. Порт PowerConect 3424/P устанавливается вместо порта PowerConnect 3448/P



- Если PowerConnect 3424/P устанавливается вместо PowerConnect 3448/P, на первые 24 FE-порта коммутатора 3424/P передается конфигурация 24 FE-портов коммутатора 3448/P. Конфигурация GE-порта остается неизменной.

Рисунок 1-6. Порт PowerConect 3448/P устанавливается вместо порта PowerConnect 3424/P



Переключение с главного стекового устройства на резервное

Резервное стековое устройство заменяет главное в следующих случаях:

- Сбой главного стекового устройства или удаление его из стека.
- Повреждение связи между главным стековым устройством и компонентами стека.
- Включение теплого резерва через веб-интерфейс или через командную строку.

Переключение с главного стекового устройства на резервное приводит к потере полной функциональности. Все таблицы с динамическими параметрами переустанавливаются в случае сбоя. Файл рабочей конфигурации синхронизирован для главного стекового и главного резервного устройств, поэтому он продолжает работать в главном резервном устройстве.

Общие сведения

В данном разделе описаны возможности устройства. Для получения полного списка всех обновленных возможностей коммутатора см. примечания к новой версии программного обеспечения.

Блок питания с поддержкой технологии питания через сеть Ethernet

Блок питания с поддержкой технологии питания через сеть Ethernet (PoE) поставляет питание в устройства через проводку локальной сети, не изменяя при этом инфраструктуру сети. Блок питания PoE исключает необходимость размещать устройства в сети рядом с источником питания. Блок питания PoE можно использовать в следующих случаях:

- IP-телефон
- Точки доступа беспроводной сети
- IP-шлюзы
- PDA
- Аудио- и видео- удаленный мониторинг

Дополнительную информацию о блоке питания с поддержкой технологии питания через сеть Ethernet см. в разделе Управление питанием через сеть Ethernet.

Защита от блокировки очереди

Блокировка очереди (Head of Line - HOL) приводит к задержкам трафика и потере кадров вследствие возникновения конфликтов трафика, претендующего на одни и те же ресурсы выходных портов. При блокировке очереди блокируются пакеты очередей, и пакеты из начала очереди пересылаются перед пакетами из конца очереди.

Поддержка управления потоком (IEEE 802.3X)

Механизм управления потоком позволяет устройствам с низкой скоростью передачи данных взаимодействовать с высокоскоростными устройствами, удерживая устройства с высокой скоростью передачи данных от отправки пакетов. Передача временно приостанавливается для предотвращения переполнения буфера.

Дополнительную информацию по настройке управления потоком для портов или групп LAG см. в разделе Определение конфигурации порта или Определение параметров LAG.

Поддержка обратного давления

В полудуплексных соединениях принимающий порт не допускает переполнения буфера, занимая соединение и делая его недоступным для дополнительного трафика.

Дополнительную информацию по настройке управления потоком для портов или групп LAG см. в разделе Определение конфигурации порта или Определение параметров LAG.

Виртуальное тестирование кабелей (VCT)

При виртуальном тестировании кабелей обнаруживаются такие повреждения кабелей с медными контактами, как открытый кабель и замыкание . Более подробную информацию о тестировании кабелей см. в разделе Запуск диагностики кабелей.

Поддержка интерфейсов MDI/MDIX

Устройство автоматически обнаруживает перекрещивание или перегибание кабеля, подключенного к порту RJ-45.

В качестве стандартной проводки для конечных станций используется **Media-Dependent Interface** (MDI) (Интерфейс, зависящий от среды передачи), а для концентраторов и коммутаторов - **Media-Dependent Interface with Crossover** (MDIX) (Интерфейс, зависящий от среды передачи, с перекрещиванием).

Дополнительную информацию по настройке интерфейсов MDI/MDIX для портов или групп LAG см. в разделе Определение конфигурации порта или Определение параметров LAG.

Автоматическое согласование

Автоматическое согласование позволяет коммутатору посылать оповещение о режиме работы. Функция автоматического согласования обеспечивает способ обмена информацией между двумя коммутаторами, совместно использующими сегмент двухточечного соединениями, и автоматической настройки обоих коммутаторов для наиболее выгодного применения возможностей передачи данных.

В коммутаторах PowerConnect серии 3400 функция автоматического согласования улучшена за счет оповещения порта. Благодаря оповещению порта системный администратор может настраивать объявленные скорости портов.

Дополнительную информацию по автоматическому согласованию см. в разделе Определение конфигурации порта или Определение параметров LAG.

Поддерживаемые функции MAC-адреса

Поддержка возможности использования MAC-адреса

Устройство поддерживает до 8K MAC-адресов. В устройстве зарезервированы определенные MAC-адреса для использования в системе.

Статические MAC-записи

В качестве альтернативного решения MAC-записи можно добавить в таблицу мостов вручную, а не путем распознавания их из входящих кадров. Такие записи, заданные пользователем, не изменяются по истечении определенного времени и сохраняются при переустановке или перезагрузке системы.

Более подробную информацию см. в Определение статических адресов.

Авторасознавание MAC-адресов

На коммутаторе активируется автоматическое распознавание MAC-адресов из входящих пакетов. MAC-адреса сохраняются в таблице мостов.

Срок хранения MAC-адресов

MAC-адреса, из которых в течение заданного периода нет трафика, убираются. Таким образом удается избежать переполнения таблицы мостов.

Более подробную информацию по настройке срока хранения MAC-адресов см. в Просмотр динамических адресов.

Коммутация на основании MAC-адресов, распознаваемых в сети VLAN

Устройство всегда выполняет соединение с помощью мостов, способных работать с сетью VLAN. Классическое соединение посредством моста (IEEE802.1D) не выполняется, когда кадры пересылаются только на основании соответствующих MAC-адресов приемников. Однако подобную функциональность можно настроить для непомеченных кадров. Кадры, адресованные на MAC-адрес приемника, который не связан ни с каким портом, рассылаются "лавиной" на все порты соответствующей VLAN.

Поддержка многоадресного трафика MAC

Служба многоадресной передачи представляет собой широковещательную службу, которая обеспечивает соединение одного входа и нескольких выходов, а также нескольких входов и нескольких выходов, при распределения информации. При использовании службы многоадресной передачи уровня 2 (Layer 2) каждый кадр обращается к определенному адресу многоадресной передачи, таким образом копии кадра передаются на соответствующие порты.

Более подробную информацию см. в Назначение параметров многоадресной передачи всем.

Функции уровня Layer 2

Отслеживание протокола IGMP

Функция отслеживания протокола IGMP анализирует содержимое кадра IGMP, которое передается устройством с рабочих постов на восходящий многоадресный маршрутизатор. На основнии данных кадра устройство идентифицирует рабочие посты, настроенные на сеанс многоадресной передачи, и определяет с каких многоадресных маршрутизаторов были отправлены кадры.

Более подробную информацию см. в Отслеживание протокола IGMP.

Зеркалирование портов

Зеркалирование портов контролирует и дублирует сетевой трафик путем пересылки копий входящих и исходящих пакетов с контролируемого порта на дублирующий. Пользователи указывают целевой порт, который должен получать копии все данных, проходящих через определенный исходный порт.

Более подробную информацию см. в Определение сеансов с зеркалированием портов.

Контроль транслируемой "лавины"

Контроль "лавины" позволяет ограничить количество многоадресных и широковещательных кадров, принимаемых и пересылаемых коммутатором.

При пересылке кадров уровня Layer 2 широковещательные и многоадресные кадры рассылаются "лавиной" на все порты соответствующей сети VLAN. Это приводит к снижению пропускной способности и загрузке всех узлов, соединенных со всеми портами.

Более подробную информацию см. в Включение контроля "лавины".

Функции, поддерживаемые сетью VLAN

Поддержка VLAN

Сети VLAN - это группы коммутационных портов, составляющие единый широковещательный домен. Пакеты классифицируются в соответствии с

принадлежностью к определенной сети VLAN на основании либо метки VLAN, либо сочетания входного порта и содержимого пакетов. Пакеты, совместно использующие общие атрибуты, можно сгруппировать в одну сеть VLAN.

Более подробную информацию см. в Настройка сетей VLAN.

Виртуальные локальные сети на основе портов (VLAN)

В виртуальных локальных сетях на основе портов (Port-based Virtual LAN - VLAN) входящие пакеты классифицируются на основании их входящего порта.

Более подробную информацию см. в Определение параметров порта сети VLAN.

Полная совместимость маркировки 802.1Q для сетей VLAN

IEEE 802.1Q определяет архитектуру виртуальных локальных сетей, службы, предоставляемые в сетях VLAN, а также протокоты и алгоритмы, необходимые для работы этих служб.

Поддержка протокола GVRP

Регистрационный протокол GARP в сетях VLAN (GVRP) обеспечивает отсечение IEEE 802.1Q-совместимых сетей VLAN и динамическое создание сетей VLAN в портах, работающих в режиме транков и помеченных как 802.1Q. При включении протокола GVRP устройство регистрирует и передает члены сети на все порты, которые входят в состав действующей Функции протокола STP топологии.

Более подробную информацию см. в Настройка параметров GVRP.

Частные сети VLAN

Порты частных сетей VLAN (функция защиты уровня 2) обеспечивают изоляцию между портами одного широковещательного домена.

Более подробную информацию о частных сетях VLAN см. в разделе Настраивает частные сети VLAN.

Функции протокола STP

Функции протокола STP (STP)

802.1d Протокол STP является стандартным элементом коммутатора уровня 2, который позволяет мостам автоматически препятствовать возникновению циклов пересылки L2 и устанавливать причины их появления. Коммутаторы обмениваются конфигурационными сообщениями с помощью специально настроенных кадров и выборочно включают и выключают передачу данных на порты.

Более подробную информацию см. в Настройка протокола STP.

Быстрая связь

Протоколу STP может потребоваться от 30 до 60 секунд на сходимость. В течение этого времени протокол STP определяет возможные замкнутые цепи, а также передает информацию об изменении состояния системы и дает время на получение ответа с соответствующих устройств. Для многих приложений временной промежуток 30-60 секунд считается слишком долгим для времени отклика. Применение функции Fast Link (Быстрая связь) снижает время задержки, поэтому ее можно использовать в тех сетевых топологиях, где исключено возникновение замкнутых цепей.

Более подробную информацию о включении быстрой связи для портов и групп LAG см. в разделе Определение параметров STP для порта или Определение статических адресов.

IEEE 802.1w Протокол RSTP

Протоколу RSTP может потребоваться от 30 до 60 секунд для каждого хост-протокола, чтобы проверить, передается ли трафик через его порты. Протокол RSTP выявляет и использует топологию сети, таким образом обеспечивая лучшую сходимость без образования циклов пересылки.

Более подробную информацию см. в Настройка протокола RSTP.

IEEE 802.1s Протокол MSTP

Протокол MSTP отображает виртуальные сети VLAN на реализации протокола STP. MSTP предлагает другой сценарий распределения нагрузки. Пакеты, назначенные для различных сетей VLAN, передаются по различным каналам в области протокола MSTP (Области MST). Области представляют собой один или несколько мостов MSTP, по которым передаются кадры. Наличие стандартов позволяет администраторам сетей назначать конкретные каналы для трафика в сетях VLAN.

Дополнительную информацию см. в разделе Настройка протокола STP.

Объединение канала

Объединение канала

Имеется возможность задать до восьми объединенных каналов, для каждого из которых можно определить до восьми участвующих портов, образующих единую объединенную группу каналов (LAG). Это обеспечивает:

- Отказоустойчивость (защита от физического разрушения канала).
- Соединения с более высокой пропускной способностью.
- Повышенную степень структурирования полосы пропускания.
- Высокую пропускную способность соединения с сервером.

Объединенная группа каналов состоит из портов с одинаковой скоростью, работающих в дуплексном режиме.

Более подробную информацию см. в Определение параметров LAG.

Объединение канала и LACP

Протокол LACP использует проходящие через каналы одноранговые данные, чтобы определить возможность объединения различных каналов, и предоставляет наиболее оптимальный вариант комбинации каналов для заданной пары устройств. LACP автоматически определяет, настраивает, связывает и управляет комбинацией портов в системе.

Более подробную информацию см. в Объединение портов.

Клиенты BootP и DHCP

Протокол динамического конфигурирования хостов DHCP предоставляет дополнительные параметры настройки, получаемые с сетевого сервера при запуске системы. Служба DHCP представляет собой активный процесс. DHCP дополнением к BootP.

Более подробную информацию о протоколе DHCP см. в Определение параметров интерфейса DHCP .

Качество обслуживания

Поддержка класса обслуживания 802.1p

Способ подачи сигналов IEEE 802.1p представляет собой стандарт OSI Layer 2 для создания и определения приоритетов сетевого трафика в канале передачи данных или на уровне MAC-адресов. Трафик 802.1p классифицируется и передается в приемник. Не устанавливается ни резервирования полосы пропускания, ни ограничений. 802.1p - вариант стандарта 802.1Q (VLAN). 802.1p определяет восемь уровней приоритета, аналогично битовой карте IP Precedence IP Header.

Более подробную информацию см. в Настройка качества обслуживания.

Функции управления устройством

Тревоги и системные прерывания протокола SNMP

В системе ведется журнал событий с указанием степени их важности и отметкой времени. Событиях передаются как прерывания SNMP в список получателей системных прерываний.

Более подробную информацию о тревогах и системных прерываниях протокола SNMP см. в разделе Определение параметров SNMP.

Версии 1, 2 и 3 протокола SNMP

Простой протокол сетевого управления (SNMP) протоколом UDP/IP управляет доступом к системе. Определяется запись сообществ, каждая из которых состоит из строки сообщества и прав доступа. Существует 3 уровня защиты протокола SNMP: только для чтения, чтение и запись и исключительная. Только пользователь с исключительными правами имеет доступ к таблице сообществ.

Более подробную информацию см. в Определение параметров SNMP.

Управление через веб-интерфейс

С помощью веб-интерфейса управления системой коммутатора можно управлять через веб-обозреватель. Система содержит встроенный веб-сервер (Embedded Web Server - EWS), обслуживающий HTML-страницы, посредством которых могут осуществляться контроль и настройка системы. Система преобразует полученные веб-данные в команды конфигурации, настройки переменных MIB и другие параметры управления.

Загрузка файла конфигурации с сервера и на сервер

Параметры конфигурации устройства находятся в файле конфигурации. Файл конфигурации содержит параметры конфигурации как для системы в целом, так и для конкретного порта. Файлы конфигурации можно вызвать с помощью командной строки, они находятся в текстовом формате.

Более подробную информацию см. в Управление файлами.

Тривиальный протокол передачи файлов TFTP

Устройство поддерживает загрузку образа, программного обеспечения и конфигурации с протокола TFTP.

Удаленный мониторинг

Удаленный мониторинг (RMON) является дополнением к протоколу SNMP, которое предоставляет возможность управления трафиком в системе (в отличие от протокола SNMP, который позволяет системному устройству выполнять функции управления и контроля). Функция удаленного мониторинга является стандартом MIB, который определяет текущую и предыдущую статистики уровня MAC-адресов и объектов управления, что позволяет осуществлять сбор достоверной информации по всей сети.

Более подробную информацию см. в Просмотр статистики.

Режим командной строки

Синтаксис и семантика режима командной строки (CLI) отвечает, насколько это возможно, общепринятым стандартам. Командная строка включает обязательные и дополнительные элементы. Интерпретатор командной строки предоставляет пользователю команды и сочетания клавиш.

Syslog

Syslog - это протокол, который позволяет отправсить уведомления о событиях на несколько удаленных серверов, где их можно сохранить и проанализировать. Система отправляет уведомления о важных событиях в условиях реального времени и сохраняет запись о них для использования позже.

Более подробную информацию о протоколе Syslog см. в Управление журналами.

SNTP

Простой протокол сетевого управления(SNTP) гарантирует синхронизацию времени на таймере сети Ethernet с точностью до миллисекунд. Синхронизация выполняется сетевым сервером SNTP. Уровень декомпозиции устанавливает файлы источника времени. Он иакже устанавливает расстояние от источника отправного значения времени. Чем выше уровень декомпозиции (0 является максимальным значением), тем точнее время.

Более подробную информацию см. в Настройка параметров протокола SNTP.

Служба имен доменов

Служба имен доменов(DNS) преобразует заданные пользователем домены в IP-адреса. Всякий раз, когда имя домена задается в DNS, служба преобразует имя в IP-адрес. Например, www.ipexample.com преобразуется в 192.87.56.2. На сервере DNS сохраняются базы данных с именами домена и соответствующие им IP-адреса.

Дополнительную информацию см. в разделе Конфигурация систем именования доменов.

Отслеживание маршрута

Функция отслеживания маршрута отслеживает IP-маршруты, чьи пакеты были перенаправлены в процессе пересылки. Функцию отслеживания маршрута в командной строке можно вызвать либо в режиме user-exec или privileged.

Средства защиты

SSL

Протокол SSL - это протокол на уровне приложений, который обеспечивает надежную передачу данных с сохранением их неприкосновенности, идентификации и целостности. Он основан на использовании сертификатов, а также открытых и закрытых ключей шифрования.

Идентификация на основе портов (802.1x)

Идентификация на основе портов позволяет определять системных пользователей индивидуально для каждого порта через внешний сервер. Только известные и утвержденные системой пользователи могут передавать и получать данные. Порты идентифицируются через сервер RADIUS с помощью наращиваемого протокола идентификации (EAP).

Более подробную информацию см. в Конфигурация идентификации на основе портов.

Поддержка заблокированных портов

Заблокированные порты позволяют улучшить безопасность в сети за счет разрешения доступа к определенному порту только пользователям, имеющим MAC-адреса. Эти адреса определяются либо вручную, либо автоматически через порт. В случае отображения кадра на заблокированном порте и отсутствия привязки MAC-адреса исходного кадра к этому порту срабатывает механизм защиты.

Более подробную информацию см. в Настройка безопасности портов.

Клиент сервера RADIUS

RADIUS представляет собой протокол типа клиент/сервер. На сервере RADIUS хранится пользовательская база данных, содержащая идентификацию каждого пользователя (имя пользователя, пароль с учет использования ресурсов).

Более подробную информацию см. в Настройка параметров RADIUS.

SSH

Протокол Secure Shell (SSH) - это протокол, который предоставляет для устройства надежное удаленное соединение. В настоящее время поддерживается версия 2 протокола SSH. Он позволяет клиентам SSH установить с устройством безопасное кодируемое соединение. Это подключение обеспечивает функциональность, подобную входящему подключению Telnet. Протокол SSH использует криптографию с открытым ключом RSA и DSA для подсоединения и идентификации устройств.

TACACS+

TACACS+ предоставляет централизованную защиту при проверке пользователя, пытающегося получить доступ к устройству. TACACS+ предоставляет централизованную систему управления, обеспечивая согласованность с сервером RADIUS и другими процедурами идентификации.

Более подробную информацию см. в Определение параметров TACACS+.

Управление с помощью паролей

Управление с помощью паролей гарантирует повышенный уровень защиты в сети. Пароли для доступа к SSH, Telnet, HTTP, HTTPS и SNMP являются назначенными функциями защиты. Более подробную информацию об управлении с помощью паролей см. в разделе Управление паролями.

Дополнительная документация по режиму командной строки

Справочное руководство по режиму CLI, имеющееся на компакт-диске с документацией, содержит сведения о командах, которые используются для настройки конфигурации устройства. В этом документе содержится информация по описанию команды, ее синтаксису, параметрам по умолчанию,

инструкциям и примерам.

Назад на страницу Содержание

Назад на страницу Содержание

Описание аппаратного обеспечения

Системы Dell™ PowerConnect™ 34XX Руководство пользователя

Описание портов

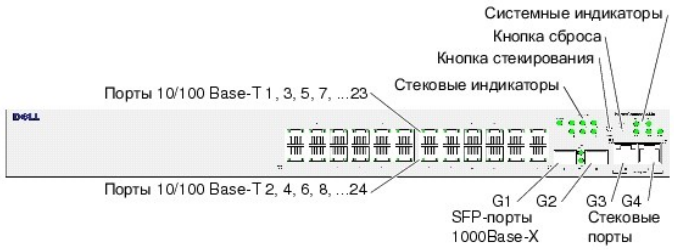
Описание портов коммутатора PowerConnect 3424

В коммутаторе PowerConnect 3424 имеются следующие порты:

- **24 порта Fast Ethernet** - это порты RJ-45, обозначенные как 10/100Base-T
- **2 оптоволоконных порта** - Они обозначены как SFP-порты 1000Base-X
- **2 порта Gigabit** - Они обозначены как порты 1000Base-T
- **Консольный порт** - порт на основе RS-232

На приведенном ниже рисунке показана передняя панель устройства PowerConnect 3424.

Рисунок 2-1. Передняя панель устройства PowerConnect 3424



На передней панели расположены 24 порта RJ-45 с порядковыми номерами от 1 до 25. Порты, расположенные в верхнем ряду, обозначены нечетными номерами 1-23, находящиеся в нижнем - четными 2-24. Кроме того, на передней панели находятся оптоволоконные порты G1 - G2 и порты с медными разъемами G3- G4. Порты G3 - G4 можно использовать либо в качестве стековых портов, либо для передачи трафика , если устройство работает в автономном режиме.

На передней панели имеются две кнопки. Кнопка Stack ID (идентификатор стека) используется для выбора номера блока. Вторая кнопка - кнопка Reset (сброс), которая предназначена для перезагрузки устройства вручную. Кнопка сброса находится в небольшом углублении, что предотвращает ее случайное нажатие. На передней панели расположены все индикаторы устройства.

На следующем рисунке показана задняя панель коммутатора PowerConnect 3424.

Рисунок 2-2. Задняя панель устройства PowerConnect 3424

На задней панели расположен разъем RPS, консольный порт и разъем питания.

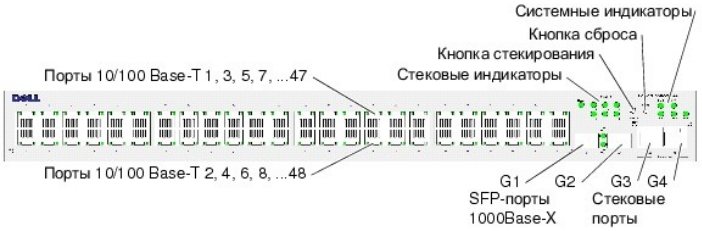
Описание портов коммутатора PowerConnect 3448

В коммутаторе PowerConnect 3448 имеются следующие порты:

- **48 порта Fast Ethernet** - это порты RJ-45, обозначенные как 10/100Base-T
- **2 оптоволоконных порта** - Они обозначены как SFP-порты 1000Base-X
- **2 порта Gigabit** - Они обозначены как порты 1000Base-T
- **Консольный порт** - порт на основе RS-232

На приведенном ниже рисунке показана передняя панель устройства PowerConnect 3448.

Рисунок 2-3. Передняя панель устройства PowerConnect 3448



На передней панели расположены 48 портов RJ-45 с порядковыми номерами от 1 до 48. Порты, расположенные в верхнем ряду, обозначены нечетными номерами 1-47, находящиеся в нижнем - четными 2-48. Кроме того, на передней панели находятся оптоволоконные порты G1 - G2 и порты с медными разъемами G3- G4. Порты G3 - G4 можно использовать либо в качестве стековых портов, либо для передачи трафика , если устройство работает в автономном режиме.

На передней панели имеются две кнопки. Кнопка Stack ID (идентификатор стека) используется для выбора номера блока. Вторая кнопка - кнопка Reset (сброс), которая предназначена для перезагрузки устройства вручную. Кнопка сброса находится в небольшом углублении, что предотвращает ее случайное нажатие. На передней панели расположены все индикаторы устройства.

На следующем рисунке показана задняя панель коммутатора PowerConnect 3448:

Рисунок 2-4. Задняя панель устройства PowerConnect 3448

На задней панели расположен разъем RPS, консольный порт и разъем питания.

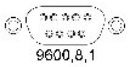
Порты SFP

Порты небольшого размера с возможностью "горячей" замены (SFP) - это двухпроводный последовательный интерфейс (TWSI) для связи через комплексное программируемое логическое устройство (CPLD), обозначенный как 1000Base-SX или LX.

Консольный порт RS-232

Один разъем DB-9 для соединения с терминалом используется для отладки, загрузки программного обеспечения и т.д. Скорость передачи данных по умолчанию составляет 9600 бит/с. Значение скорости передачи можно задать в диапазоне от 2400 до 115200 бит/с.

Рисунок 2-5. Консольный порт



Габариты

Коммутаторы PowerConnect 3424/P и PowerConnect 3448/P имеют следующие габариты:

Модель с блоком питания PoE:

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

Модель без блока питания PoE:

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

Описание индикаторов

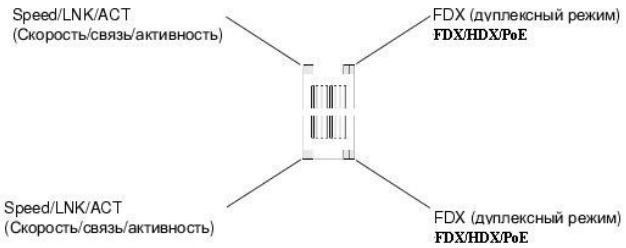
На передней панели расположены светодиоды (индикаторы), которые показывают состояние связи, источников питания, вентиляторов и системы диагностики.

Индикаторы портов

Каждому из портов 10/100/1000 Base-T и 10/100 Base-T соответствуют два индикатора. Индикатор скорости находится слева от порта, а индикатор соединения/дуплексного режима/активности - справа.

На следующем рисунке показаны индикаторы портов 10/100 Base-T на коммутаторах PowerConnect 3424 /P и PowerConnect 3448/P:

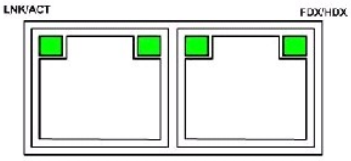
Рисунок 2-6. Индикаторы RJ-45 10/100 BaseT



Порт RJ-45 100 Base-T на коммутаторах PowerConnect 3424 /P и PowerConnect 3448/P имеет два индикатора с обозначением LNK/ACT.

На следующем рисунке показаны индикаторы 100 Base-T.

Рисунок 2-7. Индикатор RJ-45 1000 BaseT



Описание показаний индикатора RJ-45 в коммутаторах PowerConnect 3424 и PowerConnect 3448 приведено в следующей таблице:

Таблица 2-1. Показания индикатора RJ-45 100BaseT в коммутаторах PowerConnect 3424 и PowerConnect 3448

Индикатор	Цвет	Описание
Link/Activity/Speed	Зеленый, горит постоянно	Порт работает со скоростью 100 Мбит/с.
	Зеленый, мигает	Порт передает или принимает данные на скорости 100 Мбит/с.
	Желтый, горит постоянно	Порт работает со скоростью 10 Мбит/с.
	Желтый, мигает	Порт передает или принимает данные на скорости 10 Мбит/с.
	Не горит	Порт в данный момент не работает.
FDX (дуплексный режим)	Зеленый, горит постоянно	Порт в данный момент осуществляет передачу в дуплексном режиме.
	Не горит	Порт в данный момент осуществляет передачу в полудуплексном режиме.

Описание показаний индикатора RJ-45 в коммутаторах PowerConnect 3424P и PowerConnect 3448P приведено в следующей таблице:

Таблица 2-2. Показания индикатора RJ-45 100BaseT в коммутаторах PowerConnect 3424P и PowerConnect 3448P

Индикатор	Цвет	Описание
Speed/Link/Act	Зеленый, горит постоянно	Порт подключен на скорости 100 Мбит/с.
	Зеленый, мигает	Порты подключены на скорости 100 Мбит/с.
	Не горит	Порт подключен на скорости 10 Мбит/с или не подсоединен.
PoE	Зеленый, горит постоянно	Обнаружено устройство, работающее от блока питания, работа с нормальной нагрузкой. Более подробную информацию об устройствах, работающих от блока питания, см. в разделе Управление питанием через сеть Ethernet.
	Оранжевый, горит постоянно	Перегрузка или замыкание в устройстве, работающего от блока питания. Дополнительную информацию о блоке питания с поддержкой технологии питания через сеть Ethernet см. в разделе Управление питанием через сеть Ethernet.
	Оранжевый, мигает	Потребление питания в устройстве, работающего от блока питания, превышает допустимую норму. Дополнительную информацию о нормах потребления питания в сети Ethernet см. в разделе Управление питанием через сеть Ethernet.

	Не горит	Устройство, работающего от блока питания, не обнаружено.

Индикаторы порта Gigabit

В следующей таблице описаны индикаторы стекового порта Gigabit:

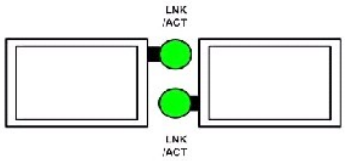
Таблица 2-3. Показания индикатора RJ-45 100BaseT в коммутаторах PowerConnect 3424 и PowerConnect 3448

Индикатор	Цвет	Описание
Link/Activity/Speed	Зеленый, горит постоянно	Порт работает со скоростью 1000 Мбит/с.
	Зеленый, мигает	Порт передает или принимает данные на скорости 1000 Мбит/с.
	Желтый, горит постоянно	Порт работает со скоростью от 10 до 100 Мбит/с.
	Желтый, мигает	Порт передает или принимает данные на скорости 10 или 100 Мбит/с.
	Не горит	Порт в данный момент не работает.
FDX (дуплексный режим)	Зеленый, горит постоянно	Порт в данный момент осуществляет передачу в дуплексном режиме.
	Не горит	Порт функционирует в полудуплексном режиме.

Индикаторы SFP

Каждый из SFP-портов имеет индикатор с обозначением LNK/ACT. В коммутаторах PowerConnect 3424/P и PowerConnect 3448/P индикаторы имеют круглую форму и находятся между портами. На следующих рисунках показаны индикаторы для каждого устройства.

Рисунок 2-8. Индикаторы порта SPF



Показания индикатора порта SFP описаны в следующей таблице:

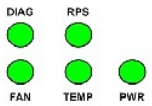
Таблица 2-4. Показания индикатора порта SFP

Индикатор	Цвет	Описание
Link/Activity	Зеленый, горит постоянно	Соединение установлено.
	Зеленый, мигает	Порт передает или получает данные.
	Не горит	Порт в данный момент не подключен.

Системные индикаторы

Системные индикаторы коммутаторов PowerConnect 3424 /P и PowerConnect 3448/P предоставляют информацию о состоянии источников питания, вентиляторов, теплового режима и системы диагностики. На следующем рисунке показаны системные индикаторы.

Рисунок 2-9. Системные индикаторы



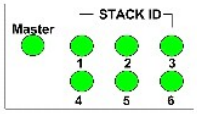
В следующей таблице приведены описания показаний системного индикатора.

Таблица 2-5. Показания системного индикатора

Индикатор	Цвет	Описание
Источник питания (PWR)	Зеленый, горит постоянно	Коммутатор включен.
	Не горит	Коммутатор выключен.
Резервный блок питания (RPS) (модели: 3424 и 3448)	Зеленый, горит постоянно	Резервный блок питания включен.
	Красный, горит постоянно	Сбой резервного блока питания.
	Не горит	Резервный блок питания не подключен.
Резервный блок питания (RPS) (модели: 3424P и 3448P)	Зеленый, горит постоянно	Резервный блок питания включен.
	Не горит	Резервный блок питания не подключен, или произошел сбой в его работе.
Диагностика (DIAG)	Зеленый, мигает	Выполняется тест диагностики системы.
	Зеленый, горит постоянно	Тест диагностики системы выполнен успешно.
	Красный, горит постоянно	Произошел сбой при тесте диагностики системы.
	Не горит	Система нормально работает.
Температура (TEMP)	Красный, горит постоянно	Температура в устройстве вне допустимого диапазона.
	Не горит	Устройство работает в допустимом температурном диапазоне.
Вентилятор (FAN)	Зеленый, горит постоянно	Все вентиляторы устройства работают в нормальном режиме.
	Красный, горит постоянно	Один или несколько вентиляторов устройства не работает.

Стековые индикаторы определяют положение устройства в стеке. На приведенном ниже рисунке показаны индикаторы на передней панели.

Рисунок 2-10. Стековые индикаторы



Стековые индикаторы пронумерованы от 1 до 6. Каждому компоненту в стеке соответствует свой индикатор, на котором высвечивается его идентификационный номер. Если стековый индикатор показывает цифру 1 или 2, это обозначает что устройство является главным стековым или главным резервным устройством.

Таблица 2-6. Показания стековых индикаторов

Индикатор	Цвет	Описание
Все стековые индикаторы	Не горит	Коммутатор работает в автономном режиме.
Стековый индикатор 1-6 (S1-S6)	Зеленый, горит постоянно	Устройство является компонентом стека с порядковым номером N.
	Не горит	Устройство не является компонентом стека с порядковым номером N.
Индикатор Stacking Master	Зеленый, горит постоянно	Устройство является главным стековым устройством
	Не горит	Устройство не является главным стековым устройством.

Источники питания

В устройстве имеется встроенный блок питания (от источника переменного тока) и разъем для подключения коммутаторов PowerConnect 3424/P и

PowerConnect 3448/P к блоку PowerConnect EPS-470, или для подключения коммутаторов PowerConnect 3424 и PowerConnect 3448 к блоку PowerConnect RPS-600. В коммутаторах PowerConnect 3424/P и PowerConnect 3448/P есть встроенный блок питания (12 Вольт).

Работа от обоих источников питания регулируется за счет распределения нагрузки. Индикаторы Power supply отображают состояние источника питания.

В коммутаторах PowerConnect 3424/P и PowerConnect 3448/P имеется встроенный источник питания 470W (12V/-48V), с предоставлением 370W для 24 портов блока питания PoE.

Блок источника питания переменного тока

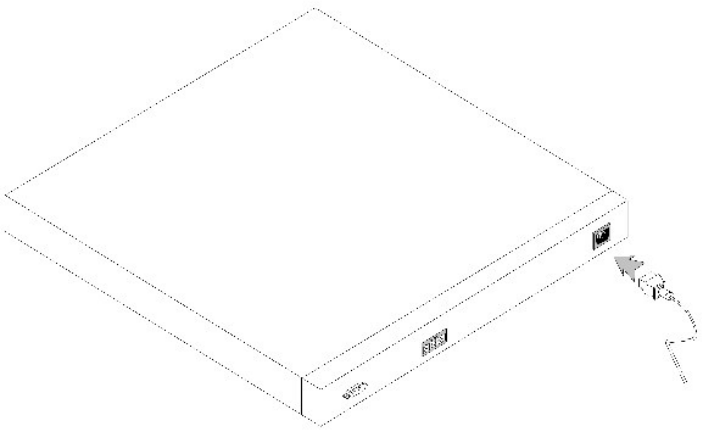
Блок источника питания переменного тока расчитан на 90 - 264 В переменного тока, 47 - 63 Гц. Для этого блока используется стандартный разъем. Индикатор находится на передней панели и обозначает подключен ли блок источника питания переменного тока.

Блок источника питания постоянного тока

Коммутаторы PowerConnect 3424 и PowerConnect 3448 подключаются к внешнему блоку RPS-600, чтобы предоставить дополнительный резервный источник питания. Настройка не требуется. Индикатор "RPS" на передней панели указывает, подключен ли внешний блок RPS-600. Определение индикатора RPS см. в таблице 2-5.

Коммутаторы PowerConnect 3424/P и PowerConnect 3448/P подключаются к внешнему блоку EPS-470, чтобы предоставить дополнительный резервный источник питания. Настройка не требуется. Индикатор "RPS" на передней панели указывает, подключен ли внешний блок EPS-470. Определение индикатора RPS см. в таблице 2-5.

Рисунок 2-11. Подключение питания



Подключение устройства к разным источникам питания снижает вероятность сбоя в случае прекращения подачи электроэнергии.

Кнопка Stack ID

На передней панели коммутатора есть кнопка Stack ID (Идентификатор стека), которая позволяет вручную выбирать идентификатор для главного стекового устройства и компонентов стека.

Главное стековое устройство и компоненты стека должны быть заданы в течение 15 секунд после загрузки устройства. Если главное стековое устройство не задано по истечении 15 секунд, коммутатор загружается для работы в автономном режиме. Чтобы задать идентификатор устройства, перезагрузите коммутатор.

Главному стековому устройству соответствует идентификатор 1 или 2. При наличии двух устройств (1 и 2) коммутатор, чей идентификатор не задан,

выполняет роль главного резервного устройства. Компонентам стека достаются идентификаторы 3-6. Например, при наличии четырех устройств в стеке главному стековому устройству соответствует идентификатор 1 или 2, главному резервному устройству - 1 или 2 в зависимости от идентификатора главного устройства, третьему компоненту присваивается номер 3, а четвертому - 4.

ПРИМЕЧАНИЕ. Устройство не определяет автоматически коммутатор, работающий в автономном режиме. Если идентификатор устройства уже выбран, нажмите кнопку Stack ID несколько раз, пока не погаснут все стековые индикаторы.

Кнопка Reset (сброс)

На передней панели коммутаторов PowerConnect 3424/P и PowerConnect 3448/P имеется кнопка сбоса, которая позволяет перезапускать устройство вручную. При перезагрузке главного стекового устройства перезагружается весь стек. При перезагрузке только одного компонента стека остальные компоненты не перезагружаются.

Симплексная цепь перезагрузки коммутатора активируется при включении питания или в условиях низкого напряжения.

Система вентиляции

Коммутаторы PowerConnect 3424/P и PowerConnect 3448/P с блоком питания PoE снабжены пятью встроенными вентиляторами. В устройствах PowerConnect 3424 и PowerConnect 3448 без блока питания PoE имеются два встроенных вентилятора. Проверить работу вентиляторов можно с помощью сигнала индикатора, сообщающего о наисправности одного или нескольких вентиляторов.

Назад на страницу Содержание

Назад на страницу Содержание

Установка коммутаторов PowerConnect 3424/P и PowerConnect 3448/P

Системы Dell™ PowerConnect™ 34XX Руководство пользователя

Подготовка места

Устройства PowerConnect 3424 /P и PowerConnect 3448/P можно монтировать в стандартную аппаратурную 48.26-см (19-дюймовую) стойку, размещать на столе или закреплять на стене. Перед установкой устройства необходимо убедиться в том, что выбранное место установки удовлетворяет следующим требованиям:

- **Питание** - Устройство устанавливается поблизости от легко доступной розетки напряжением 100-240 В переменного тока и частотой 50-60 Гц.
- **Общее** - Убедитесь в том, что резервный блок питания (RPS) смонтирован правильно, о чем свидетельствуют светящиеся индикаторы на передней панели.
- **Модели с блоком питания PoE** - Убедитесь в том, что резервный блок питания (RPS) установлен, о чем свидетельствуют светящиеся индикаторы PoE на передней панели.
- **Свободный доступ** - Оператор должен иметь свободный доступ к передней панели. Необходимо также обеспечить свободный доступ к кабелям, электрическим соединениям и вентиляционным устройствам.
- **Укладка кабеля** - Кабели прокладываются так, чтобы избежать наводок от электрических полей таких источников, как радиопередатчики, усилители радиосигнала, линии электропередач и источники флуоресцентного освещения.
- **Окружающая среда** - Температура окружающей среды должна быть от 0 до 50 °C (от 32 до 122 °F) при относительной влажности до 95 %, влага не должна конденсироваться.

Распаковка

Комплект поставки

При распаковке устройства проверьте наличие следующих компонентов:

- Устройство/коммутатор
- Кабель питания пер. т.
- Перекрестный кабель RS-232
- Самоклеящиеся резиновые ножки
- Крепежный набор для монтажа в стойке или на стене
- Компакт-диск с документацией
- Информационное руководство по продуктам

Распаковка устройства

ПРИМЕЧАНИЕ. Перед распаковкой устройства проверьте целостность упаковки и немедленно сообщите о любом обнаруженном повреждении.

1. Положите упаковочную коробку на чистую плоскую поверхность.
2. Откройте коробку или снимите с нее верхнюю крышку.
3. Аккуратно достаньте устройство из упаковочной коробки и поставьте его в безопасное и чистое место.
4. Отложите в сторону весь упаковочный материал.

5. Проверьте устройство и принадлежности на наличие повреждений. О любых обнаруженных повреждениях следует немедленно сообщить.

Монтаж устройства

Следующие инструкции по монтажу относятся к устройствам PowerConnect 3424/P и PowerConnect 3448/P. Консольный порт находится на задней панели. Разъемы питания расположены на задней панели. Присоединение источника резервного питания (RPS) не является обязательным, но рекомендуется. Разъем RPS располагается на задней панели устройства.

Монтаж в стойке

⚠ **ПРЕДУПРЕЖДЕНИЕ. Прочитайте инструкции по технике безопасности при работе с устройствами, которые подключаются к коммутатору, в документе Информационное руководство по продуктам.**

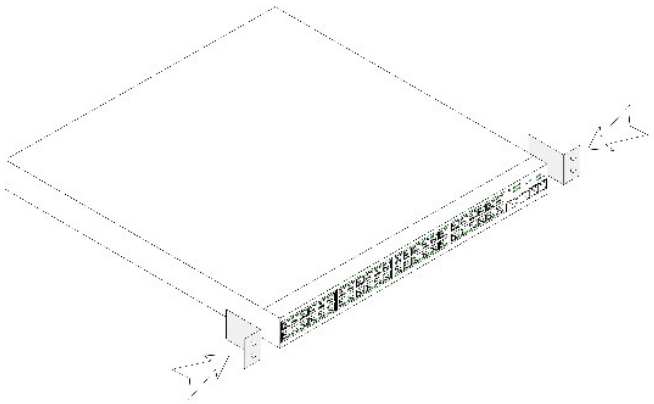
⚠ **ПРЕДУПРЕЖДЕНИЕ. Перед установкой устройства в стойку или в шкаф отсоедините от него все кабели.**

⚠ **ПРЕДУПРЕЖДЕНИЕ. При монтаже нескольких устройств в стойку начинайте устанавливать их снизу вверх.**

1. Расположите поставляемый монтажный кронштейн на одной стороне устройства так, чтобы монтажные отверстия на устройстве совпадали с монтажными отверстиями на кронштейне.

   На следующем рисунке показано, где монтировать кронштейны.

Рисунок 3-1. Установка кронштейнов при монтаже в стойку



2. Вставьте прилагаемые винты в монтажные отверстия в стойке и закрепите их отверткой.
3. Повторите действия для кронштейна с другой стороны устройства.
4. Установите устройство в 48.26-см (19-дюймовую) стойку, при этом следите за тем, чтобы монтажные отверстия на устройстве совпадали с монтажными отверстиями на стойке.
5. Закрепите устройство на стойке с помощью винтов стойки (не поставляются). Затяните нижнюю пару винтов до того, как затягивать верхнюю пару винтов. Убедитесь, что вентиляционные отверстия не закрыты.

Установка на плоской поверхности

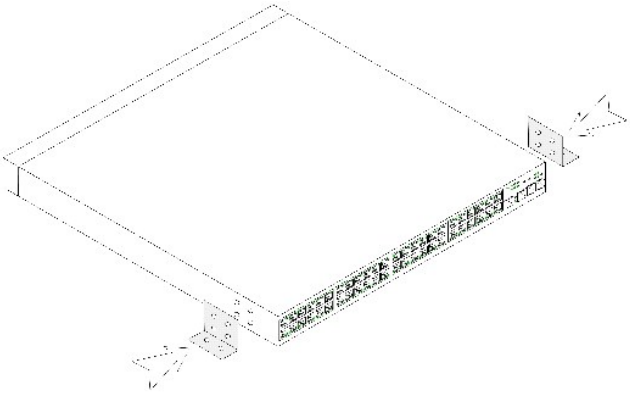
Необходимо установить устройство на плоскую поверхность, если оно не будет монтироваться в стойку. Поверхность должна выдерживать вес устройства и отходящих от него кабелей.

1. Прикрепите самоклеющиеся резиновые ножки на каждом отмеченном участке на нижней стороне блока.
2. Установите устройство на плоскую поверхность, предусмотрев зазоры по 5,08 см (2 дюйма) с каждой стороны и 12,7 см (5 дюймов) с задней стороны.
3. Убедитесь, что в месте установки устройства обеспечена достаточная вентиляция.

Установка устройства на стене

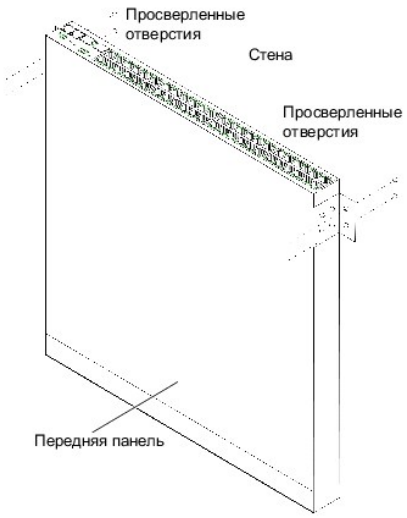
1. Расположите поставляемый настенный монтажный кронштейн на одной стороне устройства так, чтобы монтажные отверстия на устройстве совпадали с монтажными отверстиями на кронштейне. На следующем рисунке показано, где монтировать кронштейны.

Рисунок 3-2. Установка кронштейнов при монтаже не стене



2. Вставьте прилагаемые винты в монтажные отверстия в стойке и закрепите их отверткой.
3. Повторите действия для настенного кронштейна с другой стороны устройства.
4. Приложите устройство к тому месту на стене, где это устройство будет установлено.
5. Отметьте на стене расположение крепежных винтов.
6. Просверлите отверстия в отмеченных местах и вставьте в них стопорные втулки (не поставляются).
7. Закрепите устройство на стене с помощью винтов (не поставляются). Убедитесь, что вентиляционные отверстия не закрыты.

Рисунок 3-3. Монтаж устройства на стене



Подключение к терминалу

1. Подсоедините перекрестный кабель RS-232 к терминалу ASCII или разъему последовательного порта программного обеспечения эмуляции терминала на настольной системе.
2. Присоедините розетку DB-9 на другом конце кабеля к разъему последовательного порта устройства.

Подключение устройства к питанию

Присоедините кабель питания к разъему переменного тока на блоке питания.

ПРИМЕЧАНИЕ. Пока не подсоединяйте кабель питания к заземленной электророзетке. Подключите устройство к источнику питания как подробно описанно в разделе Запуск и конфигурация устройства.

Рисунок 3-4. Разъем питания на задней панели

Вид сзади устройства PowerConnect 3424/3448

Вид сзади устройства PowerConnect 3424P/3448P

После подключения устройства к источнику питания, необходимо проверить, правильно ли подключено и работает устройство, для чего следует проверить состояние индикаторов на передней панели.

Установка стека

Обзор

Каждое устройство может работать в качестве автономного устройства или может быть включено в стек. Стек поддерживает наличие до шести устройств и до 192 портов.

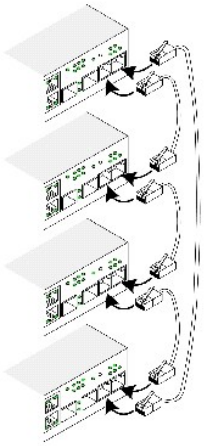
Все стеки должны иметь главное устройство, могут иметь главное резервное устройство, а все прочие устройства должны быть подключены к стеку в качестве компонентов.

Стековые коммутаторы PowerConnect серии 3400

В составе всех стеков PowerConnect серии 3400 имеется главное устройство, может присутствовать главное резервное устройство, а все прочие устройства считаются компонентами стека.

В стековых коммутаторах PowerConnect серии 3400 для осуществления стекирования используются порты RJ-45 Gigabit Ethernet (G3 и G4). Это обеспечивает возможность стекирования без дополнительных стыковочных принадлежностей. Чтобы объединить устройства в единый стек, подключите стандартный кабель категории 5 в порт G3 верхнего устройства и в порт G4 находящегося ниже устройства (того, которое находится непосредственно под верхним устройством стека). Повторите эту процедуру, пока все компоненты не будут соединены друг с другом. Соедините порт G3 самого нижнего устройства с портом G4 самого верхнего устройства в стеке.

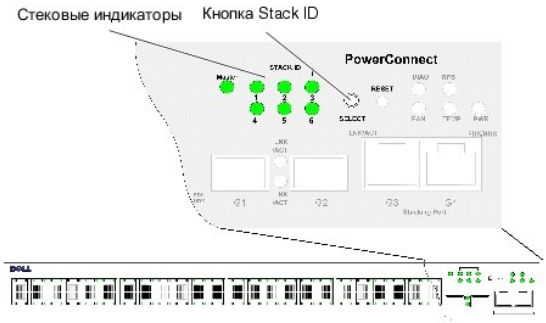
Рисунок 3-5. Схема стекового кабеля



ПРИМЕЧАНИЕ. В стековом режиме порты, обозначенные как G3 и G4, не отображаются на встроенном веб-сервере (EWS). Это результат того, что они не присутствуют в устройстве. Это объясняется тем, что в стеке портам присваивается другой индекс.

Идентификация стекового блока выполняется на передней панели устройства с помощью кнопки Stack ID (Идентификатор стека).

Рисунок 3-6. Панель конфигурации и идентификации стекирования



Каждое стековое устройство обладает уникальным идентификатором, характеризующим устройство, который определяет позицию устройства и его функцию в стеке. Если устройство представляет собой автономный блок, индикатор стека не горит. По умолчанию устройство является автономным.

Идентификатор устройства конфигурируется вручную с помощью кнопки Stack ID (Идентификатор стека). Идентификатор устройства отображается светодиодами идентификатора стека. Идентификаторы устройства 1 и 2 резервируется для главного и главного резервного устройств, а идентификаторы устройства с 3 по 6 - для устройств-компонентов.

Процесс выбора идентификатора устройства

Процесс выбора идентификатора устройства состоит в следующем:

1. Убедитесь в том, что консольный порт автономного/главного устройства подключен к устройству терминала VT100 или эмулятору терминала VT100 через перекрестный кабель RS-232.
2. Определите местоположение разъема питания переменного тока.
3. Отключите разъем питания переменного тока.
4. Подсоедините устройство к разъему переменного тока.
5. Подключите разъем питания переменного тока.

После подключения индакатор с настроенным номером (соответствующим предварительно сохраненному идентификатору) начинает мигать. Индикатор мигает в течение 15 секунд. В течение этого времени выбирите определенный идентификатор стека, нажимая на кнопку «Stack ID» (Идентификатор стека) до тех пор, пока не загорится соответствующий индикатор идентификатора стека.

6. Процесс выбора - Чтобы увеличить номер индикатора идентификатора стека, продолжайте нажимать на кнопку «Stack ID» (Идентификатор стека). Если нажать кнопку Stack ID при мигающем индикаторе 6, произойдет настройка устройства на работу в автономном режиме. При повторном нажатии кнопки Stack ID идентификатор принимает значение 1. Устройства 1 и 2 являются главными. См. процесс выбора главного устройства в Обзор стекирования.
7. **Закончить процесс выбора** - Процесс выбора идентификатора устройства завершается, когда заканчивается 15-секундный период мигания. Кнопка «Stack ID» (Идентификатор стека) перестает реагировать, и идентификатор устройства устанавливается на идентификатор индикатора, мигающего в конце этого периода.

ПРИМЕЧАНИЕ. Эти шаги должны выполняться отдельно для каждого устройства до тех пор, пока все компоненты стека не будут подключены к питанию, и не будут выбраны их стековые идентификаторы. Выполнение этих шагов отдельно для каждого устройства обеспечит достаточное время для выбора идентификатора стека для каждого устройства. Тем не менее, перед тем, как подключать устройство к источнику питания, весь стек в целом должен быть оснащен кабельной проводкой согласно Схема стекового кабеля.

Запуск и конфигурация устройства

После выполнения всех внешних соединений подключите терминал к устройству, чтобы сконфигурировать устройство. Дополнительные функции описаны в разделе Расширенная конфигурация.

ПРИМЕЧАНИЕ. Прежде чем приступать к выполнению, прочтите информацию о версии для данного продукта. Это программное обеспечение можно загрузить с веб- сайта технической поддержки Dell | Support (**support.dell.com**).

ПРИМЕЧАНИЕ. Рекомендуется загружать самую новую версию документации для пользователей с веб-сайта технической поддержки Dell по адресу **support.dell.com**.

Как подсоединить устройство

Чтобы настроить устройство, оно должно быть подключено к консоли. Тем не менее, если устройство является компонентом стека, то необходимо подключить к терминалу только главное стековое устройство. Поскольку стек работает как единое устройство, конфигурируется только главное устройство.

Подключение терминала к устройству

Устройство предусматривает консольный порт, который задействует подключение к программному обеспечению эмуляции терминала на настольной системе терминала для мониторинга и конфигурирования устройства. Разъем консольного порта представляет собой штепсельный разъем DB-9, выполненный как разъем для оборудования терминала данных (DTE).

Для использования консольного порта требуется выполнить следующие действия:

- VT100-совместимый терминал или настольная или мобильная система с последовательным портом и программное обеспечение эмуляции терминала VT100
- Перекрестный кабель RS-232 с розеткой DB-9 для консольного порта и соответствующий разъем для терминала

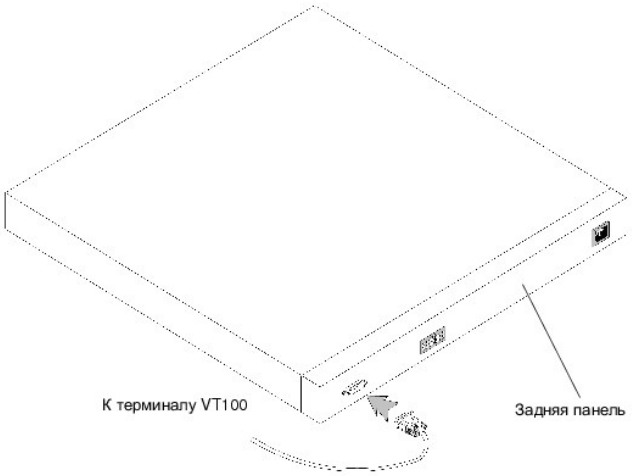
Чтобы подключить терминал к консольному порту устройства, выполните следующие действия:

1. Подсоедините поставляемый перекрестный кабель RS-232 к терминалу, использующему программное обеспечение эмуляции терминала VT100.
2. Выберите соответствующий последовательный порт (последовательный порт 1 или 2) для подключения к консоли.
3. Установите скорость передачи 9600 бод.
4. Установите формат данных 8 битов данных, 1 стоповый бит, отсутствие контроля по четности.
5. Установите значение управления потоком равным нет.
6. В меню Свойства выберите режим VT100 для эмуляции.
7. Выберите Клавиши терминала для следующих клавишей: Функциональные, со стрелками и Ctrl. Убедитесь в том, что настройка выполнена для Клавиш терминала (*а не для* Клавиш Windows).

ЗАМЕЧАНИЕ. При использовании «HyperTerminal» под Microsoft® Windows® 2000 убедитесь в том, что у вас установлена версия Windows 2000 Service Pack 2 или более поздняя. При использовании Windows 2000 Service Pack 2 клавиши со стрелками работают должным образом в эмуляции «HyperTerminal» VT100. Обратитесь на веб-сайт по адресу www.microsoft.com для информации о служебных пакетах Windows 2000.

8. Присоедините розетку перекрестного кабеля RS-232 непосредственно к консольному порту устройства на главном устройстве/автономном устройстве и затяните невыпадающие стопорные винты. Консольный порт PowerConnect серии 3400 находится на задней панели.

Рисунок 3-7. Подключение к консольному порту PowerConnect серии 3400



ПРИМЕЧАНИЕ. Консоль может быть подключена к консольному порту на любом устройстве в стеке, но управление стеком выполняется только с главного устройства в стеке (идентификатор устройства 1 или 2).

Назад на страницу Содержание

Назад на страницу Содержание

Настройка коммутаторов PowerConnect 3424/P и 3448/P

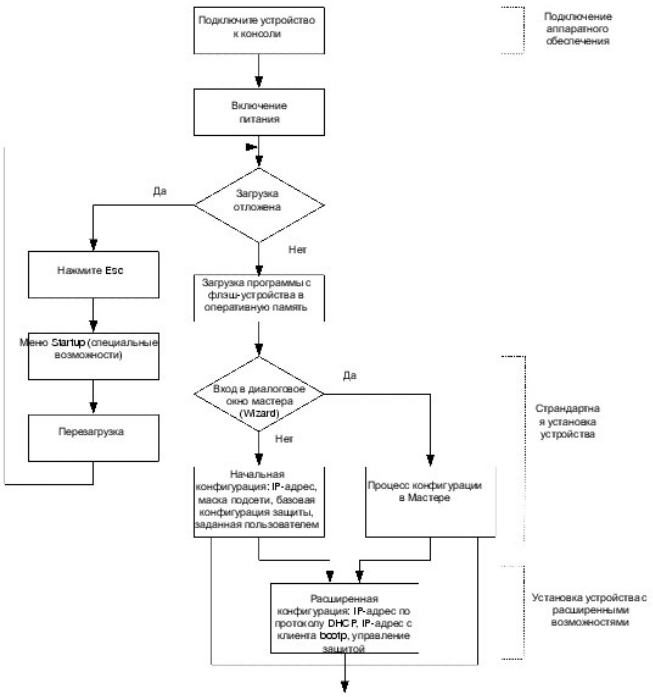
Системы Dell™ PowerConnect™ 34XX Руководство пользователя

Процедуры конфигурации

После выполнения всех внешних соединений терминал подключается к устройству, чтобы управлять загрузкой и другими процессами. Порядок установки и процесс конфигурации показаны на следующей схеме:

ПРИМЕЧАНИЕ. Прежде чем приступать к выполнению, прочтите информацию о версии для данного продукта. Загрузите информацию о верии с веб-сайта **support.dell.com**.

Рисунок 4-1. Процесс установки и конфигурации



Загрузка коммутатора

При включении питания с уже подключенным локальным терминалом коммутатор подвергается процедуре POST (Power On Self Test - самотестирование при включении питания). POST запускается каждый раз, когда устройство инициализируется, и проверяет компоненты аппаратного обеспечения, выясняя, является ли устройство полностью работоспособным перед тем, как будет полностью выполнена загрузка. Если обнаружен критический сбой, то загрузка программы останавливается. Если процедура POST проходит успешно, то действительный исполняемый образ загружается в ОЗУ. Сообщения POST выводятся на терминал и указывают на успешное завершение теста или на сбой.

Процесс загрузки занимает приблизительно 30 секунд.

Начальная конфигурация

ПРИМЕЧАНИЕ. Прежде чем приступать к выполнению, прочтите информацию о версии для данного продукта. Это программное обеспечение можно загрузить с веб- сайта технической поддержки Dell | Support (**support.dell.com**).

ПРИМЕЧАНИЕ. Начальная конфигурация предполагает следующее:

- Устройство PowerConnect никогда не конфигурировалось прежде и находится в том же состоянии, как тогда, когда вы его получили.
- Устройство PowerConnect загружается успешно.
- Подключение консоли выполнено, и на экране устройства терминала VT100 отображается запрос консоли.

Первоначальная конфигурация устройства выполняется через консольный порт. После первоначальной конфигурации устройство может управляться либо с уже подключенного консольного порта, либо дистанционно через интерфейс, определенный в процессе первоначальной конфигурации.

Если устройство загружается в первый раз, или файл конфигурации пуст по той причине, что конфигурация устройства не была выполнена, пользователю предлагается воспользоваться мастером настройки (Setup Wizard). Мастер настройки помогает выполнить начальную конфигурацию устройства и позволяет начать работу с устройством без промедлений.

ПРИМЕЧАНИЕ. Перед тем, как начать конфигурацию устройства, получите следующие данные у администратора сети:

- IP-адрес, который будет назначен интерфейсу VLAN 1, через который будет осуществляться управление устройством (по умолчанию каждый порт является компонентом VLAN 1).
- Маска подсети IP для сети
- IP-адрес шлюза по умолчанию (следующий ближайший маршрутизатор) для настройки маршрута по умолчанию.
- Строка сообщества протокола SNMP и IP-адрес системы управления протоколом SNMP (необязательно)
- Имя пользователя и пароль

Мастер настройки помогает выполнить исходную конфигурацию устройства и позволяет начать работу с устройством без промедлений. Вы можете не прибегать к услугам мастера установки и выполнить конфигурацию устройства вручную с помощью командной строки.

В мастере установки выполняется конфигурация следующих полей:

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

Появится следующее сообщение:

```
Welcome to Dell Easy Setup Wizard


The Setup Wizard guides you through the initial switch configuration, and gets you up and running as quickly as possible. You can skip
the setup wizard, and enter CLI mode to manually configure the switch.
The system will prompt you with a default answer; by pressing enter, you accept the default.
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.


Would you like to enter the Setup Wizard (you must answer this question within 60 seconds? (Y/N)[Y]Y
You can exit the Setup Wizard at any time by entering [ctrl+Z].
```

При вводе [N] мастер настройки закрывается. При отсутствии ответа в течение 60 секунд диалоговое окно мастера автоматически закрывается, и появляется сообщение консоли командной строки.

Если ввести [Y], мастер настройки поможет настроить исходную конфигурацию устройства.

ПРИМЕЧАНИЕ. При отсутствии ответа в течение 60 секунд и при условии наличия в сети сервера BootP, адрес получается с сервера BootP.

ПРИМЕЧАНИЕ. Вы можете выйти из мастера в любое время нажатием [ctrl+z].

Мастер, шаг 1

Появится следующее сообщение:

```
The system is not setup for SNMP management by default.
To manage the switch using SNMP (required for Dell Network Manager) you can

   l  Setup the initial SNMP version 2 account now.

   l  Return later and setup additional SNMP v1/v3 accounts.


For more information on setting up SNMP accounts, please see the user documentation.


Would you like to setup the SNMP management interface now? (Y/N)[Y]Y
```

Нажмите [N], чтобы пропустить шаг 2.

Введите [Y], чтобы продолжить работу в мастере установки. Появится следующее сообщение:

```
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. The wizard automatically assigns the highest access level [Privilege Level 15] to
this account.
You can use Dell Network Manager or CLI to change this setting, and to add additional management systems. For more information on adding
management systems, see the user documentation.
To add a management station:
Please enter the SNMP community string to be used: [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: [0.0.0.0]
```

Введите следующие данные:

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

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

Нажмите клавишу **Enter**.

Мастер, шаг 2

Появится следующее сообщение:

```
Now we need to setup your initial privilege (Level 15) user account.
This account is used to login to the CLI and Web interface.
You may setup other accounts and change privilege levels later.
For more information on setting up user accounts and changing privilege levels, see the user documentation.
To setup a user account:
Enter the user name<1-20>:[admin]
Please enter the user password:*
Please reenter the user password:*
```

Введите следующие данные:

- Имя пользователя, например "admin"
- Пароль и подтверждение пароля.

ПРИМЕЧАНИЕ. Если первый и второй пароли не совпадают, выдается сообщение об ошибке до тех пор, пока они не станут одинаковыми.

Нажмите клавишу **Enter**.

Мастер, шаг 3

Появится следующее сообщение:

```
Next, an IP address is setup.

The IP address is defined on the default VLAN (VLAN #1), of which all ports are members. This is the IP address you use to access the
CLI, Web interface, or SNMP interface for the switch.To setup an IP address:

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

Please enter the IP subnet mask (A.B.C.D or nn): [255.255.255.0]
```

Введите IP-адрес и IP-адрес маски подсети, например IP-адрес 1.1.1.1 и IP-адрес маски подсети 255.255.255.0.

Нажмите клавишу **Enter**.

Мастер, шаг 4

Появится следующее сообщение:

```
Finally, setup the default gateway.
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 шлюз по умолчанию.

Нажмите клавишу Enter. Появится следующее сообщение (на примере описанных параметров):

```
This is the configuration information that has been collected:

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

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

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

Мастер, шаг 5

Появится следующее сообщение:

```
If the information is correct, please select (Y) to save the configuration, and copy to the start-up configuration file. If the
information is incorrect, select (N) to discard configuration and restart the wizard: (Y/N)[Y]Y
```

Нажмите [N], чтобы запустить программу мастера установки.

Введите [Y], чтобы закрыть программу мастера установки. Появится следующее сообщение:

```
Configuring SNMP management interface
Configuring user account......
Configuring IP and subnet......

Thank you for using Dell Easy Setup Wizard. You will now enter CLI mode.
```

Мастер, шаг 6

Появляется окно командной строки.

Расширенная конфигурация

В этом разделе приведена информация по динамическому распределению IP-адресов и управлению защитой по схеме Идентификация - авторизация - учет (AAA - Authentication, Authorization, and Accounting). В раздел включены следующие темы:

- Конфигурация IP-адресов по протоколу DHCP
- Конфигурация IP-адресов по протоколу BOOTP
- Управление защитой конфигурация пароля

При конфигурации/получении IP-адресов с протоколов DHCP и BOOTP параметры настройки, получаемые с этих серверов, включают IP-адрес и могут включать маску подсети и шлюз по умолчанию.

Извлечение IP-адреса с сервера DHCP

Если для извлечения IP-адреса используется протокол DHCP, устройство ведет себя как DHCP-клиент. При перезагрузке устройства команда протокола сохраняется в файле конфигурации, а IP-адрес - нет. Чтобы извлечь IP-адрес с сервера DHCP, выполните следующие действия:

1. Чтобы извлечь IP-адрес, выберите и подключите любой порт к серверу DHCP или подсети, в которой имеется сервер DHCP.
2. Введите следующие команды, чтобы использовать выбранный порт для извлечения IP- адреса. В приведенном примере команды даны на основе порта, который был использован для конфигурации.
    - Назначение динамических IP-адресов:

```
console# configure

console(config)# interface ethernet 1/e1
```

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

console (config-if)# exit

console(config)#
```

- Назначение динамических IP-адресов (в сетях VLAN):

```
console# configure

console(config)# interface ethernet vlan 1

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

console (config-if)# exit )

console(config)#
```

Интерфейс устройства получает IP-адрес автоматически.

3. Чтобы проверить IP-адрес, введите команду **show ip interface** как показано в приведенном примере.

```
console# show ip interface

IP Address I/F Type



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

100.1.1.1/24 vlan 1 dynamic
```

ПРИМЕЧАНИЕ. Чтобы извлечь IP-адрес с сервера DHCP, не нужно удалять настройку устройства.

ПРИМЕЧАНИЕ. При копировании файлов конфигурации избегайте использовать файл конфигурации, который содержит команду вызова DHCP на интерфейс, подключенный к тому же серверу DHCP или к серверу с идентичной конфигурацией. В этом случае устройство извлекает новый файл конфигурации и загружается с его параметрами. Устройство вызывает протокол DHCP согласно команде в новом файле конфигурации, а DHCP дает команду перезагрузить тот же файл снова.

ПРИМЕЧАНИЕ. Если IP-адрес протокола DHCP уже сконфигурирован, он извлекается автоматически, а команда `ip address dhcp` сохраняется в файле конфигурации. В случае сбоя главного устройства резервное предпримет попытку извлечь адрес с DHCP. В результате возможно следующее:

- Может быть назначен тот же IP-адрес.
- Может быть назначен другой IP-адрес, что может привести к потере связи со станцией управления.
- Сервер DHCP может быть выключен, что приведет к сбою при извлечении IP-адреса и потере связи со станцией управления.

Получение IP-адреса с сервера BOOTP

Поддерживается стандартный протокол BOOTP, который позволяет устройству автоматически загружать конфигурацию хоста IP с любого

стандартного сервера BOOTP, имеющегося в сети. В этом случае устройство выполняет роль клиента BOOTP.

Как извлечь IP-адрес с сервера BOOTP:

1. Чтобы извлечь IP-адрес, выберите и подключите любой порт к серверу BOOTP или подсети, в которой имеется такой сервер.
2. В ответ на системное приглашение введите команду **delete startup configuration**, чтобы удалить файл конфигурации для запуска из флэш-памяти.

   Устройство перезагружается без учета конфигурации и через 60 секунд начинает выдавать запрсы BOOTP. Устройство получает IP-адрес автоматически.

ПРИМЕЧАНИЕ. Если ввести что-либо с клавиатуры или терминала символов ASCII во время начала перезагрузки устройства, происходит автоматическая отмена процесса BOOTP, и система не получает IP-адрес с сервера BOOTP.

Ниже приведен пример процесса:

```
console> enable

console# delete startup-config

Startup file was deleted

console# reload

You haven't saved your changes. Are you sure you want to continue (y/n) [n]?

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

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

/* the device reboots */
```

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

Теперь IP-адрес задан в конфигурации устройства.

Управление защитой конфигурация пароля

Защита системы осуществляется по схеме Идентификация - авторизация - учет (AAA - Authentication, Authorization, and Accounting), которая отвечает за права доступа для пользователей, уровень привилегированности и методы управления. Метод AAA использует как локальные, так и удаленные базы данных пользователей. Шифрование данных выполняется по технологии SSH.

Система поставляется без настроенного по умолчанию пароля. Все пароли задаются пользователем. В случае утери пароля, заданного пользователем, в меню **Startup (запуск)** можно вызвать процедуру восстановления пароля. Эта процедура применяется только для локального терминала и позволяет выполнить однократный доступ к устройству с локального терминала без введения пароля.

Настройка паролей защиты

Пароли защиты можно настроить для следующих служб:

- для терминала;
- для Telnet;
- Для SSH;
- для HTTP;
- для HTTPS

ПРИМЕЧАНИЕ. Пароли определяются пользователем.

ПРИМЕЧАНИЕ. При создании имени пользователя приоритет по умолчанию равен 1, что обеспечивает доступ к устройству, но не дает прав конфигурации. Для разрешения доступа к устройству и конфигурации необходимо установить приоритет равный 15. Несмотря на то, что имени пользователя может соответствовать приоритет 15 без требования введения пароля, рекомендуется всегда назначать пароль. Если пароль не задан, привилегированный пользователь может получить доступ к веб-интерфейсу, не вводя пароль.

ПРИМЕЧАНИЕ. Пароли можно защитить с помощью команд управления паролями, которые задают определенный срок действия пароля. Дополнительную информацию см. в разделе Управление защитой конфигурация пароля.

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 терминала в ответ на приглашение ввести пароль введите george.
- При изменении режима работы устройства в ответ на приглашение ввести пароль введите george.

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
```

- Во время первоначальной регистрации в устройстве через сеанс Telnet в ответ на приглашение ввести пароль введите bob.
- При изменении режима работы устройства 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.
```

- Во время первоначальной регистрации в устройстве через сеанс SSH в ответ на приглашение ввести пароль введите jones.
- При изменении режима работы устройства 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 user1level 15
```

Чтобы использовать сеанс HTTPS, во время настройки сеанса терминала, Telnet или SSH введите следующие команды.

ПРИМЕЧАНИЕ. Чтобы отобразить содержимое страницы в веб-браузере, активируйте SSL 2.0 или более позднюю версию.

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

```
console(config)# ip https server
```

При первоначальном включении сеанса http или https в качестве имени пользователя введите admin, а в качестве пароля - user1.

ПРИМЕЧАНИЕ. Для служб Http и Https требуется уровень доступа 15 и непосредственный доступ к уровню файла конфигурации.

Процессы в меню запуска

Меню запуска

Из меню запуска (Startup) можно вызвать процесс загрузки программного обеспечения, обработки флэш-памяти и восстановления пароля. Процессы диагностики могут выполняться только специалистами службы технической поддержки, поэтому они не освещены в настоящем документе.

В меню Startup можно войти во время загрузки устройства. Пользователь должен ввести нужную команду сразу после выполнения теста POST.

Чтобы войти в меню Startup:

1. Включите устройство, выдается автоматическое сообщение загрузки.

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

***************** SYSTEM RESET *****************

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

Boot1 Checksum Test.............................PASS

Boot2 Checksum Test.............................PASS

Flash Image Validation Test.....................PASS

BOOT Software Version 1.0.0.05 Built 06-Jan-2005 14:46:49

Carrier board, based on PPC8247

128 MByte SDRAM. I-Cache 16 KB. I-Cache 16 KB. Cache Enabled.

Autoboot in 2 seconds - press RETURN or Esc. to abort and enter prom.
```

2. После того, как появится сообщение автозагрузки, нажмите клавишу <Enter>, чтобы вызвать меню Startup. Команды из меню Startup можно вызвать с терминала ASCII или Windows HyperTerminal.

```
[1] Download Software
```

```
[2] Erase Flash File


[3] Password Recovery Procedure


[4] Enter Diagnostic Mode


[5] Set Terminal Baud-Rate


[6] Back
```

В следующем разделе дано описание команд меню Startup.

ПРИМЕЧАНИЕ. При выборе команды из меню Startup необходимо учитывать временной фактор: Если в течение 35 секунд (по умолчанию) не будет выбран ни один из пунктов меню, устройство будет перезагружено обычным образом. Это значение по умолчанию можно изменить через командную строку.

ПРИМЕЧАНИЕ. Процессы диагностики могут выполняться только специалистами службы технической поддержки (пункт меню[4]). Поэтому в этом руководстве не приведено описание режима диагностики.

Загрузка программного обеспечения - пункт меню[1]

Процедура загрузки программного обеспечивания используется, когда необходимо загрузить новую версию программы с целью заменить поврежденные файлы, а также выполнить обновление версий программ, использующихся в системе. Как загрузить программное обеспечение с помощью меню Startup:

1. В меню Startup нажмите [1]. Появляется следующее сообщение:

```
Downloading code using XMODEM


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


*** Running SW Ver. 1.0.0.30 Date 09-Jan-2005 Time 14:30:02


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


HW version is


Base Mac address is  : 00:00:b0:45:54:00


Dram size is : 128M bytes


Dram first block size is : 36864K bytes


Dram first PTR is : 0x1C00000


Flash size is: 16M
```

```
Loading running configuration.

Number of configuration items loaded: 5

Loading startup configuration.

Number of configuration items loaded: 5

Device configuration:

Slot 1 - PowerConnect 3424 HW Rev. 0.0

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

-- Unit Number 1 Standalone --

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

BOXP_high_appl_init: dpssIpcInitStandAlone

Tapi Version: v1.3.1.6P_01_03

Core Version: v1.3.1.6P_01_02

01-Jan-2000 01:01:19 %INIT-I-InitCompleted: Initialization task is completed

01-Jan-2000 01:01:19 %Box-I-FAN-STAT-CHNG: FAN# 1 status changed - operational.

01-Jan-2000 01:01:19 %Entity-I-SEND-ENT-CONF-CHANGE-TRAP: entity configuration change trap.

01-Jan-2000 01:01:19 %Box-I-FAN-STAT-CHNG: FAN# 2 status changed - operational.

01-Jan-2000 01:01:19 %Box-I-PS-STAT-CHNG: PS# 1 status changed - operational.
```

2. При использовании HyperTerminal, щелкните на пункте Transfer в строке меню HyperTerminal.
3. В поле Filename введите путь доступа к файлу, который хотите загрузить.
4. Убедитесь, что в поле Protocol выбран протокол Xmodem.
5. Нажмите кнопку Send. Начнет загружаться программное обеспечение.

ПРИМЕЧАНИЕ. По окончании загрузки программного обеспечения выполняется автоматическая перезагрузка устройства.

Удаление файла FLASH - пункт[2]

В некоторых случаях необходимо удалить конфигурацию устройства. При удалении конфигурации все параметры, настроенные через командную

строку (CLI), веб-сервер (EWS) или протокол SNMP должны быть настроены заново.

Как удалить конфигурацию устройства:

1. В меню Startup нажнажмите в течение первых двух секунд, чтобы удалить файл флэш- памяти. Появится следующее сообщение:

```
Warning! About to erase a Flash file.

Are you sure (Y/N)? y
```

2. Нажмите клавишу Y. Появится следующее сообщение:

```
Write Flash file name (Up to 8 characters, Enter for none.):config

File config (if present) will be erased after system initialization

======== Press Enter To Continue ========
```

3. Введите config как имя файла флэш-памяти. Конфигурация удаляется, и коммутатор перезагружается.
4. Восстановите исходную конфигурацию устройства.

Восстановление пароля - пункт[3]

В случае утери пароля в меню Startup можно вызвать процедуру восстановления пароля. Эта процедура дает возможность однократного входа в систему без введения пароля.

Как восстановить утерянный пароль при входе с локального терминала:

1. В меню Startup нажмите [3] и <Enter>. Пароль удаляется.

```
Введите нужный номер или нажмите Esc для выхода.

Current password will be ignored!
```

ПРИМЕЧАНИЕ. В целях защиты устройства установите новый пароль.

Режим диагностики - пункт[4]

Только для специалистов службы технической поддержки.

Установка скорости передачи на терминале - пункт[5]

Чтобы установить скорость передачи на терминале, нажмите [5] и <Enter>.

```
Введите нужный номер или нажмите Esc для выхода.

Set new device baud-rate: 38,400
```

Загрузка программного обеспечения через сервер TFTP

В этом разделе содержатся инструкции для загрузки программного обеспечения устройства (загрузка образов и системы) через сервер TFTP. Сервер TFTP должен быть настроен перед началом загрузки программного обеспечения.

Загрузка файла образа системы

Устройство загружается и запускается, когда происходит распаковка файла образа из флэш-памяти в область, где сохраняется копия образа системы. После загрузки нового образа он сохраняется в том месте, которое отводится для другой копии образа системы.

Во время последующей перезагрузки системы будет использован текущий образ системы (при отсутствии других указаний).

Как загрузить образ системы через сервер TFTP:

1. Убедитесь, что IP-адрес настроен на одном из портов устройства и что этот адрес можно вызвать с сервера TFTP.
2. Проверьте, что файл, который хотите загрузить, сохранен на сервере TFTP (файл arc).
3. Чтобы проверить номера версий программного обеспечения, выполняющегося на устройстве, введите команду **show version**. Ниже приводится пример выводимой информации:

```
console# show version

SW version 1.0.0.30 (date 27-Jan-2005 time 13:42:41)

Boot version 1.0.0.05 (date 27-Jan-2005 time 15:12:20)

HW version
```

4. Чтобы проверить, какой образ системы действует в настоящее время, введите команду **show bootvar**. Ниже приводится пример выводимой информации:

```
console# show bootvar

Images currently available on the Flash

Image-1 active (selected for next boot)

Image-2 not active

console#
```

5. Введите команду **copy tftp:**//{tftp address}/{file name} **image**, чтобы скопировать новый образ системы на устройство. После загрузки нового образа он сохраняется в том месте, которое отводится для другой копии образа системы (image-2 в приведенном примере). Ниже приводится пример выводимой информации:

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

Accessing file `file1' on 176.215.31.3Ö

Loading file1 from 176.215.31.3:
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

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

Восклицательные знаки свидетельствуют о выполнении процесса копирования. Каждый символ (!) соответствует 512 успешно скопированным байтам. Точка обозначает, что процесс копирования временно не выполняется. Последовательность точек свидетельствует о сбое копирования.

6. Выберите образ для следующей загрузки, введя команду boot system. После этого введите команду **show bootvar** , чтобы проверить, что копия, заданная в качестве параметра в команде **boot system** , выбрана для использования при следующей загрузке.

Ниже приводится пример выводимой информации:

```
console# boot system image-2

console# show bootvar

Images currently available on the Flash

Image-1 active

Image-2 not active (selected for next boot)
```

Если образ для следующей загрузки не выбран с помощью команды boot system, система загружается с образа, активного в настоящий момент.

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]?
```

8. Введите y. Устройство будет перезагружено.

Загрузка файла образа загрузки

Загрузка нового образа с сервера TFTP и внесение его в флэш-память обновляет образ загрузки. Образ загрузки загружается при включении устройства. Пользователь не может управлять копиями образа загрузки. Как загрузить образ загрузки через сервер TFTP:

1. Убедитесь, что IP-адрес настроен на одном из портов устройства и что этот адрес можно вызвать с сервера TFTP.
2. Проверьте, что файл, который хотите загрузить, сохранен на сервере TFTP (файл rfb).
3. Чтобы проверить номера версий программного обеспечения, выполняющегося на устройстве, введите команду show version. Ниже приводится пример выводимой информации:

```
console# show version

SW version 1.0.0.30 (date 27-Jan-2005 time 13:42:41)

Boot version 1.0.0.05 (date 27-Jan-2005 time 15:12:20)
```

```
HW version
```

4. Введите команду **copy tftp:**//{tftp address}/{file name} **boot**, чтобы скопировать новый образ загрузки на устройство. Ниже приводится пример выводимой информации:

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

Erasing file..done.

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

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

5. 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]?
```

6. Введите y. Устройство будет перезагружено.

Настройки порта по умолчанию

Общая информация по настройке портов устройства включает краткое описание механизма -автосогласования и параметров по умолчанию для коммутационных портов.

Автоматическое согласование

Автоматическое согласование обеспечивает определение скорости, дуплексный режим и управление потоком на всех коммутационных портах 10/100/1000BaseT. По умолчанию автоматическое согласование включается отдельно для каждого порта.

Автоматическое согласование - это протокол между двумя партнерами по связи, который позволяет порту оповестить партнера по связи о своей скорости передачи, возможности работы в дуплексном режиме и управлении потоком (управление потоком по умолчанию выключено). После обмена информацией порты работают на основе оптимальных полученных значений.

При подсоединении сетевого адаптера NIC, который не поддерживает или не настроен на автосогласование, переключаемый порт коммутатора и NIC необходимо настроить вручную на одинаковую скорость передачи и дуплексный режим.

Если станция на противоположной стороне связи пытается соединиться по протоколу автосогласования с портом 100Base-T, а этот порт настроен для работы в дуплексном режиме, то автосогласование переведет станцию в полудуплексный режим.

MDI/MDIX

Устройство поддерживает автоматическое определение кабелей прямого подключения и перекрестных кабелей на всех коммутационных портах 10/100/1000BaseT. Эта функция является частью автоматического согласования и включается, когда-включено автоматическое согласование.

При включении MDI/MDIX (интерфейса, зависящего от среды передачи, с перекрещиванием) становится возможным автоматически исправлять ошибки в выборе кабеля, поэтому разница между кабелями прямого подключения и перекрестными кабелями становится несущественна. (Стандартная проводка для конечных станций известна как MDI (Интерфейс, зависящий от среды передачи), а проводка для концентраторов и коммутаторов - MDIX.

Управление потоком

Устройство поддерживает управление потоком 802.3x для портов, настроенных на работу в полном дуплексном режиме. По умолчанию эта функция отключена. Ее можно включить для каждого порта. Механизм управления потоком позволяет принимающей стороне подавать передающей стороне сигнал о необходимости временной остановки передачи для предотвращения переполнения буфера.

Обратное давление

Устройство поддерживает обратное давление для портов, настроенных на работу в полудуплексном режиме. По умолчанию эта функция отключена. Ее можно включить для каждого порта. Механизм обратного давления временно запрещает передающей стороне пропускать дополнительный трафик. Принимающий порт может занимать соединение, делая его недоступным для дополнительного трафика.

Настройки по умолчанию для переключаемых портов

В следующей таблице приведены описания настроек по умолчанию для портов.

Таблица 4-1. Настройки порта по умолчанию

Функция	***Настройка по умолчанию***
Скорость и режим работы порта	10/100BaseT, медный: Автоматическое согласование на скорости100 Мбит/с в полном дуплексном режиме
	10/100/1000BaseT, медный / SFP: Автоматическое согласование на скорости 1000 Мбит/с в полном дуплексном режиме
Состояние пересылки пакетов для порта	Enabled (Включено)
Маркировка портов	Без маркировки
Управление потоком	Off (Выкл.) (отключена на входе)
Обратное давление	Off (Выкл.) (отключена на входе)

Назад на страницу Содержание

Назад на страницу Содержание

Использование интерфейса Dell OpenManage Switch Administrator

Системы Dell™ PowerConnect™ 34XX Руководство пользователя

В этом разделе содержится вводная информация о пользовательском интерфейсе Dell OpenManage Switch Administrator.

Запуск приложения

ПРИМЕЧАНИЕ. Перед тем, как запустить приложение, необходимо определить IP- адрес. Дополнительную информацию см. в разделе Начальная конфигурация.

1. Откройте веб-браузер.
2. Введите IP-адрес устройства в адресной строке и нажмите клавишу <Enter>.
3. Когда откроется окно **Log In** (Вход в систему), введите имя пользователя и пароль.

ПРИМЕЧАНИЕ. Пароли чувствительны к регистру вводимых символов и могут содержать как буквы, так и цифры.

4. Щелкните кнопку **OK**.

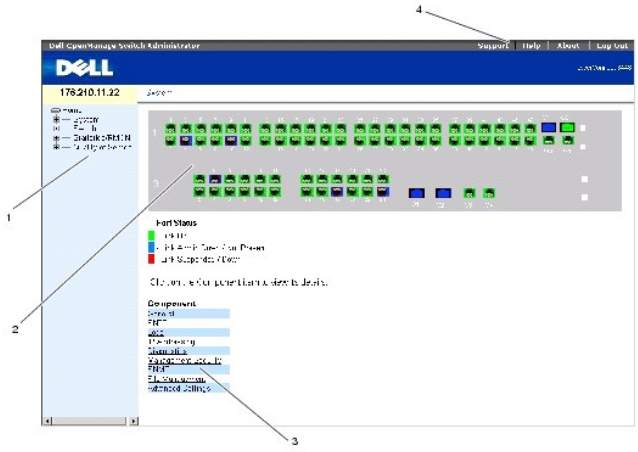
Открывается основная страница интерфейса **Dell OpenManage™ Switch Administrator**.

Элементы интерфейса

На домашней странице есть следующие поля:

- Tree view (панель дерева) - расположено слева на домашней странице; панель дерева содержит развернутое представление функций и их компонентов.
- Device view (Панель устройства) - расположено справа на домашней странице; на панели устройства имеется вид устройства, информационная или табличная область и инструкции по настройке.

Рисунок 5-1. Компоненты Switch Administrator



В Таблица 5-1 перечислены компоненты интерфейса с соответствующими номерами.

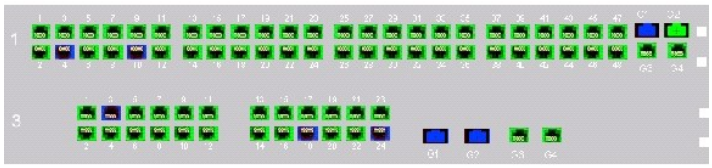
Таблица 5-1. Компоненты интерфейса

Компонент	Описание
1	Панель дерева содержит список различных парамеров устройства. Ветви дерева можно раскрывать для просмотра всех компонентов конкретного параметра или сворачивать, скрывая эти компоненты. Поле панели можно расширить, переместив ограничивающую вертикальную линию вправо, - это позволит увидеть названия компонентов полностью.
2	На панели дерева представлена информация о портах устройства, текущая конфигурация и состояние, табличная информация и компоненты функции. В зависимости от выбранного элемента, в нижней части панели дерева отображается прочая информация об устройстве или диалоговые окна для настройки параметров.
3	В поле components list (список компонентов) приводится список компонентов устройства. Компоненты также можно отобразить, раскрыв соответствующий параметр в панели tree view (панель дерева).
4	Информационные кнопки обеспечивают доступ к информации о коммутаторе и к технической поддержке Dell. Более подробную информацию см. в Информационные кнопки.

Описание устройства

На домашней странице приводится схематическое изображение передней панели коммутатора.

Рисунок 5-2. Индикаторы портов коммутатора PowerConnect



Цвет порта показывает, активен ли данный порт в настоящий момент. Порты могут быть следующих цветов:

Таблица 5-2. Индикаторы портов и стеков устройства PowerConnect

Компонент	Описание
Индикаторы портов	
Зеленый	Порт включен.
Красный	В порте произошла ошибка.
Синий	Порт выключен.

Красный	Устройство не подключено к стеку.

ПРИМЕЧАНИЕ. Индикаторы портов не показаны на передней панели PowerConnect на странице OpenManage Switch Administrator. Состояние индикаторов можно увидеть только на реально работающем устройстве. Тем не менее, стековые индикаторы отображают состояние стекового порта. Более подробную информацию об индикаторах см. в разделе **Описание индикаторов**.

Кнопки на странице Switch Administrator

В этом разделе описываются кнопки, относящиеся к интерфейсу OpenManage Switch Administrator. Кнопки интерфейса можно разбить на следующие категории:

Информационные кнопки

Информационные кнопки предоставляют доступ к странице интерактивной технической поддержки и интерактивной справке, а также к информации об интерфейсах OpenManage Switch Administrator.

Таблица 5-3. Информационные кнопки

Кнопка	Описание
Support (Поддержка)	Открывает страницу технической поддержки Dell **support.dell.com.**
Help (Справка)	Интерактивная справка, которая содержит информацию, помогающую при настройке и управлении коммутатором. Страницы интерактивной справки контекстно-зависимы. Например, если открыта страница **IP Addressing** (IP-адресация), при нажатии кнопки **Help** (Справка) открывается раздел справки для этой страницы.
About (О компьютере)	Содержит версию и номер билда, а также информацию об авторских правах компании Dell.
Log Out (Выход)	Вызывает диалоговое окно Log Out.

Кнопки управления

Кнопки управления коммутатором обеспечивают удобный способ конфигурирования информации коммутатора и включают следующие кнопки:

Таблица 5-4. Кнопки управления

Кнопка	Описание
Apply Changes (Принять изменения)	Применяет заданные изменения к устройству.
Add (Добавить)	Добавляет информацию в таблицы или диалоговые окна.
Telnet	Запускает сеанс Telnet.
Query (Запрос)	Запрашивает таблицы.
Show All (Показать все)	Отображает таблицы устройств.
Стрелка влево/Стрелка вправо	Используется для перемещения данных в списках.
Refresh (Обновить)	Обновляет информацию об устройстве.
Reset All Counters (Сбросить все счетчики).	Удаляет показания статистических счетчиков.
Print (Печать)	Распечатывает страницу **Network Management System** (Система сетевого управления) и табличную информацию.
Draw (считывание непосредственно после записи)	Оперативно создает статистические диаграммы.

Определение полей

Обычно поля задаются пользователем и могут содержать от 1 до 159 символов, в противном случае дополнительная информация предоставляется на веб-странице OpenManage Switch Administrator. Допускается использование всех символов, кроме следующих:

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

Доступ к устройству в режиме командной строки

Управлять коммутатором можно с помощью прямого подсоединения к порту терминала или связи Telnet. Если доступ осуществляется через соединение Telnet, убедитесь, что IP-адрес устройства определен, и что рабочая станция, используемая для доступа к устройству, подключена к нему до начала использования командной строки.

Информацию о настройке начального IP-адреса см. в разделе Начальная конфигурация.

ПРИМЕЧАНИЕ. Перед тем, как использовать режим командной строки для доступа к устройству, убедитесь, что программное обеспечение загружено на устройство.

Соединение с терминалом

1. Включите устройство и дождитесь конца процедуры запуска.
2. В приглашении для ввода Console> введите enable и нажмите <Enter>.
3. Настройте устройство и введите необходимые команды для выполнения нужных задач.
4. По окончании введите команду **exit** Privileged EXEC mode (Выход из режима Privileged EXEC).

   Сеанс закончен.

ПРИМЕЧАНИЕ. Если другой пользователь входит в систему в режиме Privileged EXEC, текущий пользователь вынужден выйти из системы, чтобы предоставить доступ новому пользователю.

Соединение Telnet

Telnet - это протокол TCP/IP эмуляции терминала. Терминалы RS-232 могут виртуально соединяться с локальным устройством через сеть, работающую по протоколу TCP/IP. Telnet - это альтернатива терминалу с локальной регистрацией, в котором требуется удаленная регистрация.

Устройство поддерживает до четырех одновременных сеансов Telnet для управления коммутатором. Во время сеанса Telnet можно использовать все команды консоли.

Как запустить сеанс Telnet:

1. Выберите Start>Run(Пуск-Выполнить).

   Откроется окно Run (Запуск программы).

2. В окне **Run** введите Telnet *<IP address>* в поле **Open** (Открыть).
3. Нажмите кнопку **OK**.

   Начнется сеанс Telnet.

Использование интерфейса командной строки

В этом разделе приведена информация об использовании интерфейса командной строки.

Обзор командного режима

Режим командной строки подразделяется на несколько командных режимов. Каждый из них имеет свой собственный набор команд. Если ввести знак вопроса в окне приглашения терминала, отображается список команд, имеющихся 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 для задач, не изменяющих конфигурацию терминала, и используется для доступа к подсистемам настройки, таким как режим командной строки (CLI). Для выхода на следующий уровень (Privileged EXEC) необходимо ввести пароль (при условии его наличия).

Режим Privileged EXEC обеспечивает доступ к общей настройке устройств. Для доступа к конкретным глобальным настройкам 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

При входе в устройство включается командный режим EXEC. Приглашение на пользовательском уровне состоит из имени хоста, за которым следует символ угловой скобки (>). Пример:

```
console>
```

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

Команды режима User EXEC обеспечивают соединение с удаленными устройствами, временно изменяют установки терминала, выполняют основные тесты и отображают системную информацию.

Чтобы вывести на экран команды режима User EXEC, введите знак вопроса в приглашении на ввод команды.

Режим Privileged EXEC

Привилегированный доступ можно защитить, чтобы предотвратить несанкционированный доступ и обеспечить сохранность системных параметров. Пароли отображаются на экране и чувствительны к вводу символов в разных регистрах.

Как получить доступ к командам режима Privileged EXEC:

1. По приглашению введите enable и нажмите клавишу <Enter>.
2. По запросу введите пароль и нажмите <Enter>.

Приглашение режима Privileged EXEC отображается в виде имени хоста устройства, за которым следует знак решетки #. Например:

```
console#
```

Чтобы вывести на экран команды режима Privileged EXEC, введите знак вопроса в приглашении на ввод команды.

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

Следующий пример иллюстрирует вход в режим Privileged EXEC и возврат в режим User EXEC:

```
console> enable

Enter Password: ******

console#

console# disable

console>
```

Воспользуйтесь командой **exit**(выход), чтобы вернуться в предыдущий режим. Например, из режима Interface Configuration в Global Configuration и из Global Configuration в Privileged EXEC.

Режим Global Configuration

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

Чтобы войти в режим Global Configuration, в приглашении режима Privileged EXEC введите команду **configure** (конфигурировать) и нажмите <Enter>. Режим Global Configuration отображается в виде имени хоста устройства, за которым следует (config) и знак решетки #.

```
console(config)#
```

Чтобы вывести на экран команды режима Global Configuration, введите знак вопроса в приглашении на ввод команды.

Чтобы вернуться из режима Global Configuration в Privileged EXEC, введите команду **exit** (выход) или воспользуйтесь комбинацией клавиш <Ctrl>+<Z>.

Следующий пример иллюстрирует переход в режим Global Configuration и возврат в режим Privileged EXEC:

```
console#

console# configure

console(config)# exit
```

```
console#
```

Полный список режимов интерфейса командной строки см. в руководстве **Dell™ PowerConnect™3424/P and PowerConnect 3448/P CLI Guide**.

Назад на страницу Содержание

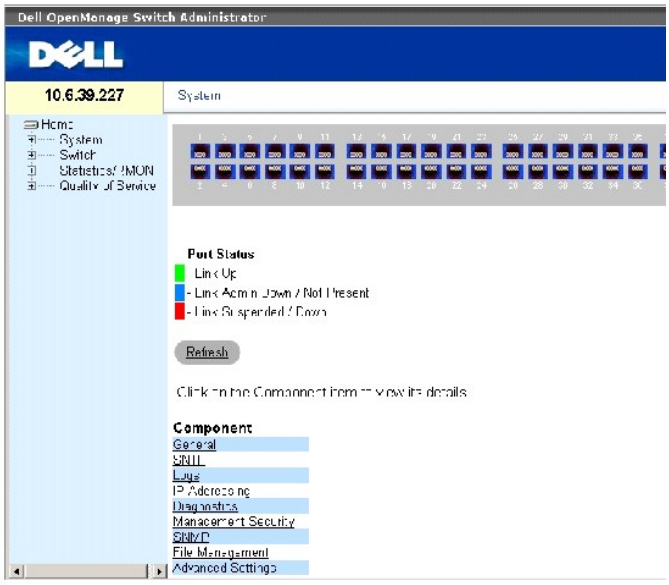
Назад на страницу Содержание

Информация о настройке системы

Системы Dell™ PowerConnect™ 34XX Руководство пользователя

В этом разделе приведена информация по определению системных параметров, включающих функции безопасности, загрузку программного обеспечения коммутатора и его перенастройку. Чтобы открыть страницу **System (Система)**, нажмите **System (Система)** на панели дерева.

Рисунок 6-1. System (Система)



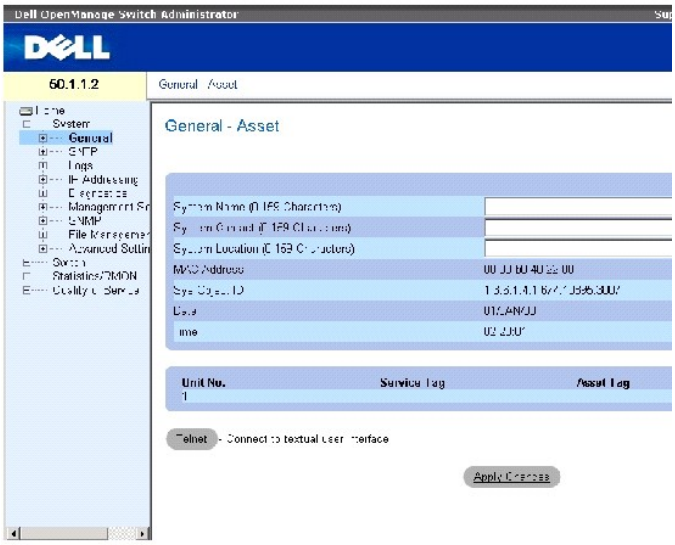
Получение общей информации о коммутаторе

Страница **General** (Общее) содержит ссылки на страницы, позволяющие системным менеджерам настраивать параметры коммутатора.

Обзор информации о коммутаторе в разделе Asset (Ресурсы)

Страница **Asset (Ресурсы)** содержит параметры для настройки и просмотра общих сведений об устройстве, включая имя системы, ее местонахождение и контактную информацию, системный MAC-адрес, системный идентификатор объекта, время, дату и время включения системы. Чтобы открыть страницу **Asset (Ресурсы)** нажмите System (Система) → General (Общее) → Asset (Ресурсы) в панели дерева.

Рисунок 6-2. Asset (Ресурсы)



На странице **Asset (Ресурсы)** есть следующие поля:

System Name (Имя системы) (от 0 до 159 символов). Определенное пользователем название коммутатора.

System Contact (Контактное лицо) (от 0 до 159 символов). Указание имени контактного лица.

System Location (Местонахождение системы) (от 0 до 159 символов). Место, где в данный момент функционирует система.

MAC Address (MAC-адрес). Указание MAC-адреса системы.

Sys Object ID (Объектный идентификатор системы). Официальная идентификация подсистемы управления сетью, которая содержится в системе и предоставляется производителем.

Date (DD/MMM//YY) (Дата (ДД/МММ//ГГ). Текущая дата. Формат даты: день, месяц, год. Например: 10/OCT/03 означает 10 октября 2003 года.

Time (HH:MM:SS) Время (ЧЧ:ММ:СС). Указание времени. Формат времени: час, минута, секунда. Например: 20:12:21 означает восемь часов двенадцать минут и двадцать одна секунда вечера.

Unit No. (Номер устройства). Номер устройства, для которого выводится информация о ресурсах.

Service Tag (Сервисная кодовая метка). Справочный сервисный номер, используемый при обслуживании устройства.

Asset Tag (Дескриптор ресурса) (от 0 до 16 символов). Определенная пользователем ссылка на коммутатор.

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.

Инициирование сеанса Telnet

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

Будет инициирован сеанс Telnet.

Настройка сведений об устройстве с помощью командной строки

В следующей таблице приведены команды консоли, соответствующие полям на странице **Asset (Ресурсы)**.

Таблица 6-1. Команды Asset

Команды 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	Задает вручную системное время и дату.
show clock [detail]	Выводит время и дату по системным часам.
show system id (системный идентификатор)	Выводит информацию метки службы
show system (система)	Выводит информацию о системе.
asset-tag текст	Устанавливает метку ресурсов устройства.
show stack <1-6>	Выводит информацию о системном стеке.
show system [unit *блок*]	Выводит информацию о системе.
show system [unit *блок*]	Выводит информацию об идентичности системы.

Далее приведен пример определения имени хоста системы, ее контактной информации и местонахождения, а также установки времени и даты на системных часах с помощью командной строки:

```
console(config)# hostname 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

Далее показан пример вывода на экран системной информации для коммутатора, работающего в автономном режиме, с помощью командной строки:

console# **show system id**	
Service tag :	
Serial number : 51	
Asset tag :	
console# **show system**	
System Description:	Ethernet Switch
System Up Time (days,hour:min:sec):	0,00:00:57
System Contact:	
System Name:	CARRIER-1
System Location:	
System MAC Address:	00:00:00:08:12:51
System Object ID:	1.3.6.1.4.1.674.10895.3006
Type:	PowerConnect 3424
Main Power Supply Status:	OK
Fan 1 Status:	NOT OPERATIONAL
Fan 2 Status:	NOT OPERATIONAL
Temperature (Celsius):	30
Temperature Sensor Status:	OK

Далее показан пример вывода на экран системной информации для коммутатора, работающего в стековом режиме, с помощью командной строки:

```
console# show system id

Unit  Serial number  Asset tag  Service tag
----  -------------  ---------  -----------
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

console# show system

Unit  Type
----  -----------------
1     PowerConnect 3424
2     PowerConnect 3424
3     PowerConnect 3428
4     PowerConnect 3424P
5     PowerConnect 3424P
6     PowerConnect 3424P

Unit  Main Power Supply  Redundant Power Supply
----  -----------------  ----------------------
1     OK
```

2	OK				
3	OK				
4	OK		OK		
5	OK		OK		
6	OK		OK		
Unit	Fan1	Fan2	Fan3	Fan4	Fan5
----	----	----	----	----	----
1	OK	OK			
2	OK	OK			
3	OK	OK			
4	OK	OK	OK	OK	OK
5	OK	OK	OK	OK	OK
6	OK	OK	OK	OK	OK
Unit	Temperature (Celsius)		Temperature Sensor Status		
----	----------		----------		
1	30		OK		
2	30		OK		
3	30		OK		
4	30		OK		
5	30		OK		
6	30		OK		

Определение настройки времени в системе

На странице **Time Synchronization (Синхронизация времени)** имеются поля для установки времени в системе как на локальных часах, так и на сервере SNTP. Если время в системе задается по показаниям часов на сервере SNTP, и на них происходит сбой, время в системе устанавливается в соответствии с показаниями локальных часов. В устройстве можно включить функцию Daylight Savings Time (летнее время). Далее следует список, указывающий начало и конец летнего времени в разных странах:

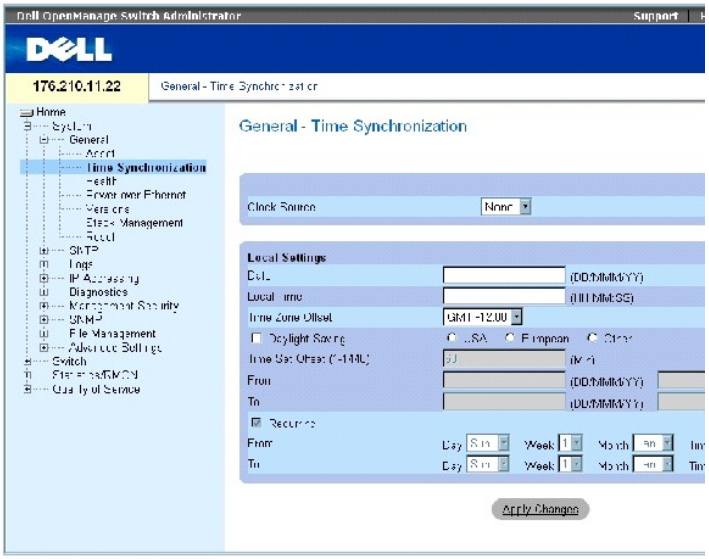
- Албания - Последние выходные марта - последние выходные октября.
- Австралия - С конца октября по конец марта.
- Австралия - Тасмания - С начала октября по конец марта.
- Армения - Последние выходные марта - последние выходные октября.
- Австрия - Последние выходные марта - последние выходные октября.
- Багамские острова - С апреля по октябрь, в соответствии с летним временем в США.
- Беларусь - Последние выходные марта - последние выходные октября.
- Бельгия - Последние выходные марта - последние выходные октября.
- Бразилия - С 3-ей субботы октября по 3-ю субботу марта. В период летнего времени часы в большинстве южно-восточных районов Бразилии переводятся на час вперед.
- Чили - остров Пасхи, с 9 марта по 12 октября. С первого воскресенья марта или после 9 марта.
- Китай - В Китае не происходит переход на летнее время.
- Канада - С первого воскресенья апреля по последнюю субботу октября. Переход на летнее время обычно регулируется местными властями. Исключение могут составлять некоторые муниципалитеты.
- Куба - С последнего воскресенья марта по последнюю субботу октября.
- Кипр - Последние выходные марта - последние выходные октября.
- Дания - Последние выходные марта - последние выходные октября.
- Египет - Последняя пятница апреля по последний четверг сентября.
- Эстония - Последние выходные марта - последние выходные октября.
- Финляндия - Последние выходные марта - последние выходные октября.
- Франция - Последние выходные марта - последние выходные октября.
- Германия - Последние выходные марта - последние выходные октября.
- Греция - Последние выходные марта - последние выходные октября.
- Венгрия - Последние выходные марта - последние выходные октября.
- Индия - В Индии не происходит переход на летнее время.
- Иран - С 1 Farvardin по 1 Mehr.
- Ирак - С 1 апреля по 1 октября.
- Ирландия - Последние выходные марта - последние выходные октября.
- Израиль - Меняется в зависимости от года.
- Италия - Последние выходные марта - последние выходные октября.
- Япония - В Японии не происходит переход на летнее время.
- Иордания - Последние выходные марта - последние выходные октября.
- Латвия - Последние выходные марта - последние выходные октября.
- Ливан - Последние выходные марта - последние выходные октября.
- Литва - Последние выходные марта - последние выходные октября.
- Люксембург - Последние выходные марта - последние выходные октября.
- Македония - Последние выходные марта - последние выходные октября.
- Мексика - С 02:00 первого воскресенья апреля до 02:00 последней субботы октября.
- Молдова - Последние выходные марта - последние выходные октября.
- Черногория - Последние выходные марта - последние выходные октября.
- Нидерланды - Последние выходные марта - последние выходные октября.
- Новая Зеландия - С первого воскресенья октября по первую субботу марта (или после 15 марта).
- Норвегия - Последние выходные марта - последние выходные октября.
- Парагвай - С 6 апреля по 7 сентября.
- Польша - Последние выходные марта - последние выходные октября.
- Португалия - Последние выходные марта - последние выходные октября.
- Румыния - Последние выходные марта - последние выходные октября.
- Россия - Последние выходные марта - последние выходные октября.
- Сербия - Последние выходные марта - последние выходные октября.

- Словацкая Республика - Последние выходные марта - последние выходные октября.
- Южно-Африканская Республика - ЮАР не переходит на летнее время.
- Испания - Последние выходные марта - последние выходные октября.
- Швеция - Последние выходные марта - последние выходные октября.
- Швейцария - Последние выходные марта - последние выходные октября.
- Сирия - С 31 марта по 30 октября.
- о-в Тайвань - На о-ве Тайвань не переходят на летнее время.
- Турция - Последние выходные марта - последние выходные октября.
- Соединенное Королевство - Последние выходные марта - последние выходные октября.
- Соединенные Штаты Америки - С 02:00 первого воскресенья апреля до 02:00 последнего воскресенья октября.

Более подробную информацию о протоколе SNTP см. в **Настройка параметров протокола SNTP**.

Чтобы открыть страницу Time Synchronization (Синхронизация времени)нажмите System (Система) → General (Общее) → Time Synchronization (Синхронизация времени) в панели дерева.

Рисунок 6-3. Time Synchronization (Синхронизация времени)



На странице **Time Synchronization (Синхронизация времени)** есть следующие поля:

Clock Source (Источник времени)

Clock Source (Источник времени) - Ресурс, по которому настраиваются системные часы. Возможные значения поля:

SNTP - Указывает на то, что системное время настроено через сервер SNTP. Дополнительную информацию см. в разделе **Настройка параметров протокола SNTP**.

None (Отсутствует) - Указывает на то, что для настройки времени в системе не использован внешний источник.

Локальные параметры

Date (Дата) - Определяет дату в системе. Дата задается в формате ДД/МММ/ГГ, напрмер 04/May/50 (04/Мая/50).

Local Time (Местное время) - Определяет время в системе. Время задается в формате ЧЧ/ММ/СС, например 21/15/03.

Time Zone Offset (Сдвиг времени в часовом поясе) - Разница во времени по Гринвичу (GMT) и местного времени. Например, сдвиг времени в часовом поясе Парижа составляет GMT +1:00, а местное время в Нью-Йорке - GMT -5:00.

Существует два вида настройки летнего времени: по конкретной дате определенного года или периодически вне зависимости от года. Чтобы выполнить настройку по конкретной дате определенного года, заполните поле **Daylight Savings (Летнее время)**, а для выполнения настройки периодически - поле**Recurring (Периодически)**.

Daylight Savings (Летнее время) - Включает функцию летнего времени (DST) в устройстве на основании его местоположения. Возможные значения поля:

USA (США) - Устройство переключается на летнее время в 02:00 первого воскресенья апреля и возвращается на зимнее в 02:00 последнего воскресенья октября.

European (Европа) - Устройство переключается на летнее время в 01:00 последнего воскресенья марта и возвращается на зимнее в 01:00 последнего воскресенья октября. Функция European (Европа) применяется для стран-членов ЕС и других стран, где используются европейские стандарты.

Other (Другое) - Летнее время устанавливается пользователем в зависимости от местонахождения. Если выбрано поле Other (Другое), требуется ввести значение времени в поля **From (С)** и **To (По)**.

Time Set Offset (1-1440) (Установка разницы во времени)- Для стран, не входящих в состав США или Европы, разницу во времени можно задать с точностью до минут. Значение по умолчанию: 60секунд.

From (С) - В этом поле задается дата начала летнего времени в странах, не входящих в состав США или Европы, в формате ДД/МММ/ГГ, а в другом поле - время. Например, если переход на летнее время происходит 25 октября 2007г. в 5:00, соответствующие поля принимают значения 25/Oct/07 и 05:00. Возможные значения поля:

Date (Дата) - Дата начала летнего времени. Возможные значения поля: от 1 до 31.

Month (Месяц) - Месяц начала летнего времени. Возможные значения поля: Jan-Dec (Янв. - Дек.).

Year (Год)- Год , в котором выполнена настройка летнего времени.

Time (Время) - Время перехода на летнее время. Формат поля: Hour (Час): Minute (Минута), например, 05:30.

From (С) - В этом поле задается дата перехода на зимнее время в странах, не входящих в состав США или Европы, в формате ДД/МММ/ГГ, а в другом поле - время. Например, летнее время заканчивается 23 марта 2008 в 12:00, соответствующие поля принимают значения 23/Mar/08 и 12:00. Возможные значения поля:

Date (Дата) - Дата окончания летнего времени. Возможные значения поля: от 1 до 31.

Month (Месяц) - Месяц окончания летнего времени. Возможные значения поля: Jan-Dec (Янв. - Дек.).

Year (Год)- Год, в котором заканчивается настройка летнего времени.

Time (Время) - Время перехода на летнее время. Формат поля: Hour:Minute (Часы:Минуты), например, 05:30.

Recurring (Периодически) - Определяет время перехода на летнее время для стран, не входящих в состав США или Европы, в которых дата начала летнего времени постоянна каждый год. Возможные значения поля:

From (С) - Определяет время перехода на летнее время. Например, в данном регионе переход на летнее время происходит в 5:00 второго воскресенье апреля. Возможные значения поля:

Day (День) - День недели, когда происходит ежегодный переход на летнее время. Возможные значения поля: Sunday-Saturday (воскресенье - суббота).

Week (Неделя) - Неделя месяца, когда происходит ежегодный переход на летнее время. Возможные значения поля: от 1 до 5.

Month (Месяц) - Месяц ежегодного перехода на летнее время. Возможные значения поля: Jan-Dec (Янв. - Дек.).

Time (Время) - Время ежегодного перехода на летнее время. Формат поля: Hour (Час): Minute (Минута), например, 02:10.

To (По) - Определяет время периодического ежегодного перехода на зимнее время. Например, в данном регионе переход на зимнее время происходит в 5:00 четвертой пятницы октября. Возможные значения поля:

Day (День) - День недели, когда происходит ежегодный переход на зимнее время. Возможные значения поля: Sunday -Saturday (воскресенье - суббота).

Week (Неделя) - Неделя месяца, когда происходит ежегодный переход на зимнее время. Возможные значения поля: от 1 до 5.

Month (Месяц) - Месяц ежегодного перехода на зимнее время. Возможные значения поля: Jan-Dec (Янв. - Дек.).

Time (Время) - Время ежегодного перехода на зимнее время. Формат поля: Hour:Minute (Часы:Минуты), например, 05:30.

Выбор источника времени

1. Откройте страницу **Time Synchronization (Синхронизация времени)**.
2. Определите поле **Clock Source** (Источник времени).
3. Нажмите кнопку Apply Changes (Применить изменения).

Источник времени выбран, а устройство обновлено.

Определение настройки локального времени

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

Локальное время настроено.

Определение настройки времени с помощью командной строки

В следующей таблице приведены команды консоли, соответствующие полям на странице **Time Synchronization (Синхронизация времени)**.

ПРИМЕЧАНИЕ. Чтобы настроить летнее время, необходимо выполнить следующие действия:

1. Настройте летнее время.
2. Выберите часовой пояс.
3. Установите время.

Пример:

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

Таблица 6-2. Команды консоли CLI по установке времени

CLI	Описание
clock source sntp	Конфигурация внешнего источника времени для системных часов.
clock time zone *hours-offset* [**minutes** *minutes-offset*][**zone** *acronym*]	Установка часового пояса.
clock summer-time	Настройка системы на автоматический переход на летнее время (Daylight Savings Time).
clock summer-time recurring {**usa** | **eu** | *week day month hh:mm week day month hh:mm*} [**offset** *offset*] [**zone** *acronym*]	Настройка системы на автоматический переход на летнее время (соответственно стандартам США и Европы).
clock summer-time date *date month year hh:mm date month year hh:mm* **[offset** *offset***] [zone** *acronym***]**	Настройка системы на автоматический переход на летнее время (Daylight Savings Time) в определенный период - формат дата/месяц/год.

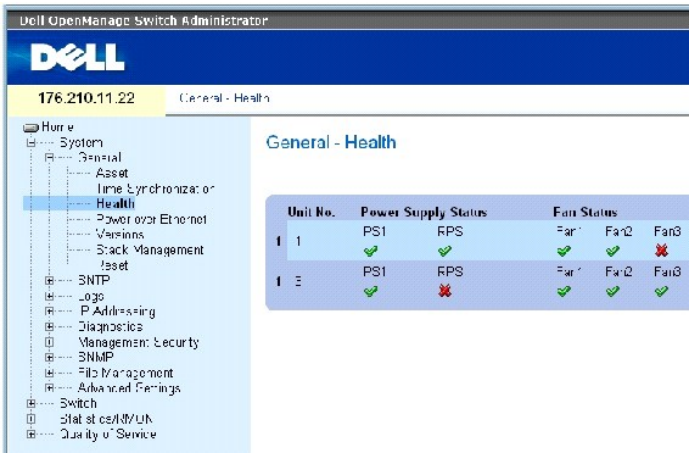
Ниже приведен пример команд консоли:

```
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

На странице Состояние системы приводитсяинформация об устройстве, включая информацию об источниках питания и вентиляции. Чтобы открыть страницу Состояние системы нажмите **System (Система)** → **General (Общее)** → **Health (Состояние)** в панели дерева.

Рисунок 6-4. Состояние системы



На странице *Состояние системы* есть следующие поля:

Unit No. (Номер устройства). - Номер устройства, для которого выводится информация о ресурсах.

Power Supply Status (Состояние источника питания) - В устройстве имеются два источника питания. Источник питания 1 обозначается в интерфейсе как PS1, а резервный источник - как RPS. Возможные значения поля:

- Источник питания работает в нормальном режиме.

- Источник питания работает неправильно.

Not Present (Отсутствует) - Источник питания отсутствует.

Fan Status (Состояние вертиляторов) - Системы без блока питания PoE снабжены двумя вентиляторами, а с ним - пятью. Каждый вентилятор обозначается в интерфейсе словом fan с последующим порядковым номером. Возможные значения поля:

- Вентилятор работает нормально.

- Вентилятор работает неправильно.

Not Present (Отсутствует) - Вентилятор отсутствует.

Temperature (Температура) - Температура, при которой устройство работает в данный момент времени. Температура дана в градусах Цельсия. Температурный диапазон устройства: 0-40 C (32-104F). В следующей таблице приведены значения температуры по Фаренгейту с приращением 5 градусов.

Таблица 6-3. Таблица 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 команды консоли, соответствующие полям на странице Состояние системы .

Таблица 6-4. Команды консоли для вызова информации о состоянии системы

Команды консоли	Описание
show system [**unit** *óñòðîéñòâî*]	Выводит информацию о системе.

Ниже приведен пример команды консоли.

```
Console> show system

System Description: Ethernet switch

System Up Time (days,hour:min:sec): 1,22:38:21

System Contact:

System Name: RS1

System Location:

System MAC Address: 00.10.B5.F4.00.01

Sys Object ID: 1.3.6.1.4.1.674.10895.3004

Type: PowerConnect 3424

Temperature Sensors:

Unit    Sensor    Temperature (Celsius)    Status
----    ------    ---------------------    ------
1       1                 41               OK
1       2                 41               OK
2       1                 42               OK
```

2	2		42	OK
Unit	Power Supply	Source	Status	
----	----------	------	------	
1	Main	AC	OK	
2	Secondary	AC	OK	
Unit	Fan	Status		
----	---	------		
1	CPU	OK		
2	CPU	OK		

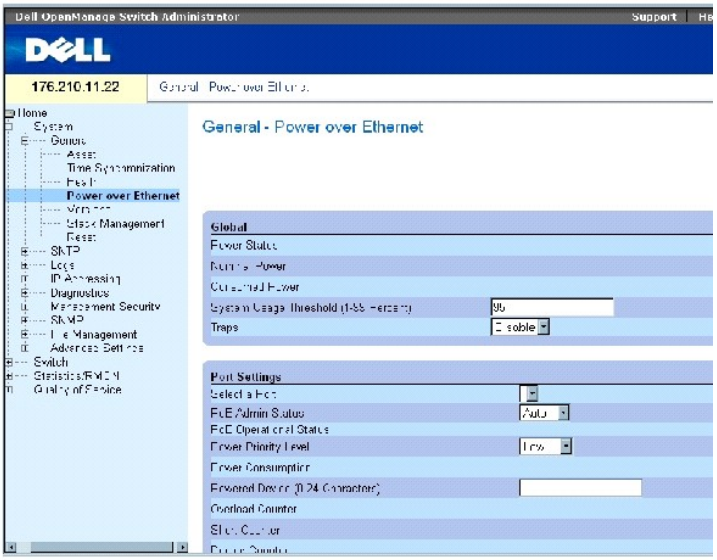
Управление питанием через сеть Ethernet

Блок питания с поддержкой технологии питания через сеть Ethernet (PoE) поставляет питание в устройства через проводку локальной сети, не изменяя при этом инфраструктуру сети. Блок питания PoE исключает необходимость размещать устройства в сети рядом с источником питания.

Подключенные устройства - это устройства, работающие от источника питания Powered Devices, например, IP-телефон. Такие устройства подключаются к коммутатору PowerConnect через порты Ethernet. Такие устройства подключаются к коммутатору либо через любой из 24 портов PowerConnect 3424P, либо из 48 портов FE PowerConnect 3448P.

Чтобы открыть страницу Блок питания с поддержкой технологии питания через сеть Ethernet, щелкните **System (Система)** → **General (Общее)** → **Power over Ethernet (Блок питания PoE)** на панели дерева.

Рисунок 6-5. Блок питания с поддержкой технологии питания через сеть Ethernet



На странице Блок питания с поддержкой технологии питания через сеть Ethernet есть следующие поля:

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

Global (Глобальные параметры)

В разделе Global (Глобальные параметры) имеются следующие поля:

Power Status (Состояние источника питания) - Показывает состояние линейного источника питания.

On (Вкл.) - Показывает, что источник питания работает.

Off (Выкл.) - Показывает, что источник питания не работает.

Faulty (Неисправность) - Показывает, что блок питания работает, но произошла ошибка. Например, перегрузка или замыкание в сети.

Nominal Power (Номинальная мощность) - Показывает действительное значение мощности, подаваемой от источника питания. Значение поля дано в Ваттах.

Consumed Power (Потребляемая мощность)- Показывает значение мощности, потребляемой коммутатором. Значение поля дано в Ваттах.

System Usage Threshold (1-99 Percent) (Порог использования - 1-99%) - Указывает значение мощности, по достижении которого подается тревога. Значение поля: 1-99 %. Значение по умолчанию - 95 %.

Traps (Системные прерывания)- Включает или выключает отправку системных прерываний с блока PoE. По умолчанию эта функцияотключениа.

Port Settings (Параметры порта)

Select a Port (Выбор порта) - Указывает, для какого интерфейса настроены параметры PoE, и определяет который из них подключен к выбранному порту.

PoE Admin Status (Состояние PoE) - Определяет режим работы блока PoE. Возможные значения поля:

Auto (Авто) - Включает протокол Device Discovery (протокол обнаружения устройства) и подает питание на устройство от модуля PoE. Протокол Device Discovery позволяет обнаружить подключенные к интерфейсу устройства, а также определить их классификацию. Это параметры по умолчанию.

Never (Никогда) - Отключает протокол Device Discovery (протокол обнаружения устройства) и прекращает подачу питания на устройство от модуля PoE.

PoE Operational Status (Состояние работы PoE) - Указывает, включен ли порт для работы с PoE. Возможные значения поля:

On (Вкл.) - Показывает, что на интерфейс поступает питание от устройства.

Off (Выкл.)- Показывает, что на интерфейс не поступает питание от устройства.

Test Fail (Тест не пройден) -Показывает, что тест подключенного устройства не пройден. Например, не удалось активировать порт, чтобы использовать его для подачи питания на устройство.

Testing (Тестирование) - Тестируется подлюченное устройство. Например, выполняется проверка того, что на устройство поступает питание.

Searching (Поиск) - Коммутатор PowerConnect осуществляет поиск подключенного устройства. Searching (Поиск) является режимом блока PoE по умолчанию.

Fault (Сбой)- Коммутатор PowerConnect обнаружил неисправность в подключенном устройстве. Напрмер, не удалось считать память подключенного устройства.

Power Priority Level (Уровень приоритета по мощности) - Определяет приоритет портов при низком значении подаваемого питания. Приоритет по мощности используется при низком значении подаваемого питания. Значение по умолчанию: low (низкое). Например, если используется 99% поступающего питания, и порт 1 имеет высокий приоритет, а порт 3 - низкий, то питание поступает на порт 1, а не на 3.

Critical (Критический) - Назначает самый высокий приоритет.

High (Высокий) - Назначает следующий по уровню высокий приоритет.

Low (Низкий) - Назначает самый низкий приоритет.

Power Consumption (Потребление мощности) - Показывает значение мощности, поступающей на подключенное устройство с выбранного интерфейса. Устройства классифицируются в зависимости от подключенного устройства, и коммутаторы PowerConnect используют эту информацию. Значение поля дано в Ваттах. Возможные значения поля:

0.44 - 12.95 - Показывает, что потребление мощности для порта составляет от 0.44 до 12.95 Ватт.

0.44 - 3.8 - Показывает, что потребление мощности для порта составляет от 0.44 до 3,8 Ватт.

3.84 - 6.49 - Показывает, что потребление мощности для порта составляет от 3,84 до 6,49 Ватт.

6.49 - 12.95 - Показывает, что потребление мощности для порта составляет от 6,49 до 12.95 Ватт.

Power Device (0-24 characters) (Подключенное устройство, 0-24 символа) - Описание подключенного устройства, заданное пользователем. В поле можно вводить до 24 символов.

Overload Counter (Счетчик перегрузки) - Указывает количество случаев перегрузки по мощности.

Short Counter (Счетчик дефицита мощности) - Указывает количество случаев дефицита мощности.

Denied Counter (Счетчик отказов) - Указывает количество случаев отказа устройству в питании.

Absent Counter (Счетчик отсутствия) - Указывает количество случаев прекращения подачи питания на подключенное устройства по причине невозможности определить его присутствие.

Invalid Signature Counter (Счетчик недействительности подписи) - Указывает количество случаев получения недействительной подписи. Подписи предназначены для идентификации подключенного устройства на PSE. Подписи создаются во время процесса обнаружения, классификации и обслуживания подключенного устройства.

Определение параметров PoE

1. Откройте страницу Блок питания с поддержкой технологии питания через сеть Ethernet.
2. Определите поля.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Параметры PoE определены, а устройство обновлено.

Упрвление блоком PoE в режиме командной строки

В следующей таблице приведены команды консоли, соответствующие полям на странице Блок питания с поддержкой технологии питания через сеть Ethernet.

Таблица 6-5. Команды консоли для вызова информации о состоянии системы

Команды консоли	Описание
`power inline {auto | never}`	Конфигурация административного режима подачи линейной мощности на интерфейс.
`power inline powered-device pd-type`	Добавление описания типа подключенного устройства.
`power inline priority {critical | high | low}`	Конфигурация приоритетности интерфейса в зависимости от распределения линейной мощности.
`power inline usage-threshold`	Конфигурация порогового значения включения тревоги
`power inline traps enable`	Включение системных прерываний в PoE
`show power inline [interface ethernet ]`	Вывод на экран сведений о конфигурации PoE

Ниже приведен пример команд консоли.

```
Console# show power inline

Power: On

Nominal Power: 150 Watts

Consumed Power: 120 Watts (80%)

Usage Threshold: 95%

Traps: Enabled
```

Port	Powered Device	State	Priority	Status	Classification [W]
----	----------	-----	--------	------	----------
1/e1	IP Phone Model A	Auto	High	On	0.44 – 12.95
2/e1	Wireless AP Model	Auto	Low	On	0.44 – 3.84
3/e1		Auto	Low	Off	N/A

```
Console# show power inline ethernet 1/e1
```

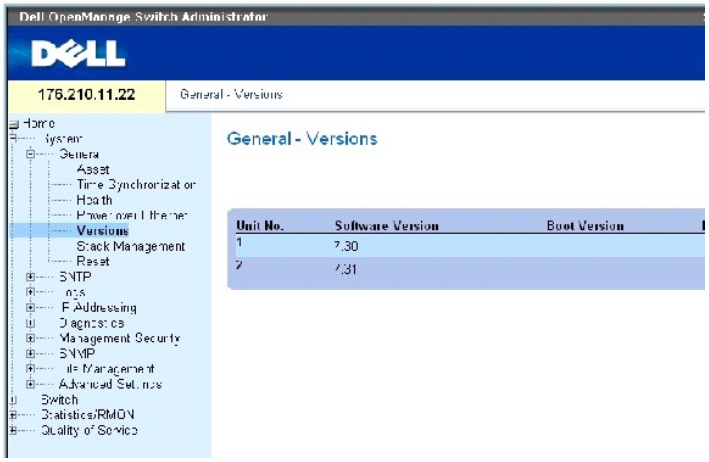
Port	Powered Device	State	Priority	Status	Classification [W]
----	----------	-----	--------	------	----------
1/1e	IP Phone Model A	Auto	High	On	0.44 – 12.95

```
Overload Counter: 1

Short Counter: 0

Denied Counter: 0

Absent Counter: 0

Invalid Signature Counter: 0
```

Вывод на экран информации о версии

Страница **Versions (Версии)** содержит сведения о версиях работающих на данный момент устройств и программного обеспечения. Чтобы открыть страницу **Versions (Версии)** нажмите System (Система) → General (Общее) → Versions (Версии) в панели дерева.

Рисунок 6-6. Versions (Версии)



На странице **Versions (Версии)** есть следующие поля:

Unit No. (Номер устройства). - Номер устройства, для которого выводится информация о его версии.

Software Version (Версия программного обеспечения) - Текущая версия программы, работающей на устройстве.

Boot Version (Версия загрузчика) - Текущая версия загрузчика, работающая на устройстве.

Hardware Version (Версия аппаратного оборудования) - Текущая версия оборудования, работающего на устройстве.

Отображение версий устройств с помощью команд консоли

В следующей таблице приведены команды консоли, соответствующие полям на странице Versions (Версии).

Таблица 6-6. Команды консоли для вызова версии

Команды консоли	Описание
show version	Выводит информацию о системе.

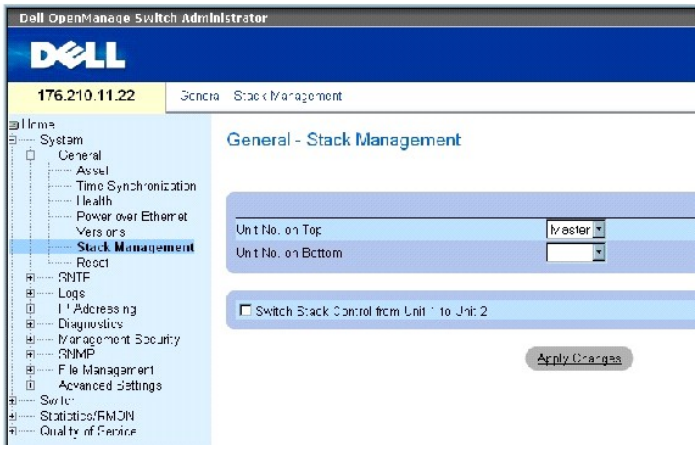
Ниже приведен пример команд консоли:

```
console> show version

SW version 1.0.0.0 (date 23-Jan-2005 time 17:34:19)

Boot version 1.0.0.0 (date 11-Jan-2005 time 11:48:21)

HW version 1.0.0
```

Управление компонентами стека

Страница **Управление стеком** дает администраторам сети возможность перезапустить либо весь стек, либо определенное устройство в стеке. Чтобы открыть страницу **Управление стеком** нажмите **System (Система)** → **General (Общее)** → **Stack Management (Управление стеком)** *в панели дерева*.

Рисунок 6-7. Управление стеком



ПРИМЕЧАНИЕ. Сохраните все изменения в файле Running Configuration (Рабочая конфигурация), прежде чем перенастроить устройство Таким образом текущая конфигурация устройства не будет утеряна. Подробности о сохранении файлов конфигурации см. в разделе Управление файлами.

Unit No. on Top - Номер первого компонента в стеке. Возможные значения: Master (Главное устройство) и 1-6.

Unit No. on Bottom - Номер второго компонента в стеке. Возможные значения: Master (Главное устройство) и 1-6.

Switch Stack Control from Unit 1 to Unit 2 - Переключение с текущего главного стекового устройства на главное резервное.

ПРИМЕЧАНИЕ. Перезапуск главного стекового устройства приводит к перезапуску всего стека.

Переключение главных устройств

1. Откройте страницу **Управление стеком** .
2. Отметьте флажком поле Switch Stack Control from Unit 1 to Unit 2.
3. Нажмите кнопку Apply Changes (Применить изменения).

   Будет выведено сообщение для подтверждения.
4. Щелкните OK.

   Произойдет сброс параметров устройства. После этого на экран будет выведен запрос имени пользователя и пароль.

Конфигурация порядка отображения компонентов в стеке

1. Откройте страницу **Управление стеком**.
2. Определите топологию стека, задав верхний и нижний компоненты. Эти компоненты должны быть соседними.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Конфигурация порядка отображения выполняется на странице System (Система).

Упрвление стеками в режиме командной строки

В следующей таблице приведены команды консоли, соответствующие полям на странице **Управление стеком**.

Таблица 6-7. Команды управления стеком

Команды консоли	Описание
reload	Перезагружает операционную систему.
stack reload	Перезагружает компоненты стека.
stack master	Назначает главное стековое устройство

Ниже приведен пример команд консоли:

```
console# reload


Are you sure you want to erase running configuration (y/n) [n]
```

Перенастройка устройства

Страница Reset (Сброс) позволяет пользователям дистанционно перенастроить устройство. Чтобы открыть страницу Reset (Сброс) , , выберите System (Система)→ General (Общее)→ Reset (Сброс) на панели дерева.

На странице Reset (Сброс) есть следующие поля:

Reset Unit No (Сброс блока №). - Перезапускает выбранный компонент стека.

ПРИМЕЧАНИЕ. Сохраните все изменения в файле Running Configuration (Рабочая конфингурация), прежде чем перенастроить устройство. Таким образом текущая конфигурация устройства не будет утеряна. Подробности о сохранении файлов конфигурации см. в разделе Управление файлами.

Перенастройка устройства

1. Откройте страницу Reset (Сброс).
2. Выберите устройство в поле **Reset Unit Number**.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

   Будет выведено сообщение для подтверждения.
4. Щелкните **OK**.

   Произойдет сброс параметров устройства. После этого на экран будет выведен запрос имени пользователя и пароль.
5. Введите имя пользователя и пароль, чтобы получить доступ к веб-интерфейсу.

Перенастройка устройства с помощью команд консоли

В следующей таблице приведены соответствующие команды консоли для перезапуска устройства в режиме командной строки:

Таблица 6-8. Команда перезапуска

Команды консоли	Описание
reload	Перезагружает операционную систему.

Ниже приведен пример команды консоли.

```
console >reload



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

Настройка параметров протокола SNTP

Коммутатор поддерживает Простой протокол сетевого управления (SNTP). Протокол SNTP гарантирует синхронизацию времени на таймере сети с точностью до миллисекунд. Синхронизация выполняется сетевым сервером SNTP. Протокол SNTP работает только как клиент и не предоставляет услуги установки времени для других систем.

Коммутатор может выполнить запрос времени на следующих видах серверов:

- Unicast (с однонаправленной передачей)
- Anycast (с альтернативной передачей)
- Broadcast (Трансляция)

Stratums (страты) устанавливает файлы источника времени. Stratums устанавливает точность отправного значения времени. Чем выше страта (0 является максимальным значением), тем точнее время. Коммутатор получает значение времени со стратой 1 и выше. Ниже приводится пример страты.

- **Stratum 0** - В качестве источника времени используется реальное время, например, глобальная система позиционирования (GPS) .
- **Stratum 1** - В качестве источника времени используется время на сервере, связанного с источником времени Stratum 0. Серверы, использующие время Stratum 1, задают исходное стандартное время в сети.
- **Stratum 2** - Источник времени удален от сервера Stratum 1 в сети. Например, на сервер Stratum 2 поступает значение времени через протокол NTP с сервера Stratum 1.

Информация, полученная с серверов SNTP, оценивается по критерию уровня времени и типу сервера. Показания времени SNTP оцениваются и определяются по следующим уровням:

- **T1** - Время отправки клиентом первоначального запроса.
- **T2** - Время получения первоначального запроса на сервере.
- **T3** - Время отправки ответа с сервера на клиент.
- **T3**- Время получения ответа с сервера клиентом.

Коммутатор может выполнить запрос времени на следующих видах серверов: Unicast (с однонаправленной передачей), Anycast (с альтернативной передачей) и Broadcast (Трансляция).

Опрос с однонаправленной передачей используется для опроса севера, IP-адрес которого известен. Запрос информации о синхронизации выполняется только с серверов SNTP, которые настроены на устройстве. Параметры T1-T4 используются для определения серверного времени. Рекомендуется использовать этот метод для синхронизации системного времени, так как он является наиболее надежным. Если выбран этот метод, информация SNTP принимается только с серверов SNTP, заданных для устройства на странице **Серверы SNTP**.

Опрос с альтернативной передачей используется для опроса севера, IP-адрес которого неизвестен. Если выбран этот метод, информация о синхронизации может быть отправлена со всех серверов SNTP в сети. Синхронизация устройства выполняется, когда оно предварительно запрашивает данные синхронизации. Самый быстрый ответ на запрос данных синхронизации (имеющий самый низкий стратум), полученный с первых трех серверов SNTP, используется для установки значения времени. Показатели T3 и T4 используются для определения серверного времени.

Использование опроса с альтернативной передачей для получения данных синхронизации является предпочтительнее, чем использование опроса с трансляцией. Тем не менее, этот метод является менее надежным, чем опрос с односторонней передачей, так как пакеты SNTP принимаются с серверов SNTP, которые не настроены в устройстве.

Опрос с трансляцией используется для опроса севера, IP-адрес которого неизвестен. Когда сообщение трансляции отправляется с сервера SNTP, клиент SNTP получает это сообщение. Если функция опроса с трансляцией включена, то принимаются все данные синхронизации, даже если запрос на них не поступал с устройства. Этот метод самый ненадежный.

Устройство получает данные синхронизации либо с помощью активного запроса информации, либо через определенный интервал времени опроса. Если включен запрос с однонаправленной, альтернативной и трансляционной передачами, получение данных происходит в следующей последовательности:

- Предпочтение отдается информации с серверов, которые определены в устройстве. Если функция опроса с однонаправленной передачей выключена или в устройстве не задан ни один сервер, то устройство принимает ответ с любого реагирующего сервера SNTP.
- Если реагируют несколько устройств с однонаправленной передачей, предпочтение отдается информации, полученной с устройства с наименьшим стратумом.
- Если серверы имеют одинаковое значение стратума, информация принимается с первого ответившего сервера SNTP.

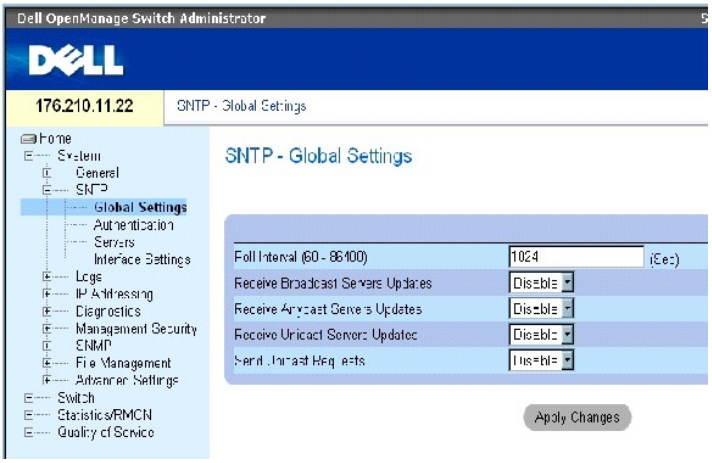
MD5 (Message Digest 5 - профиль сообщения 5) Идентификация обеспечивает защиту каналов синхронизации между устройством и серверами SNTP. MD5 - это алгоритм 128-битного шифрования. Алгоритм MD5 является вариантом MD4, который предоставляет более высокий уровень защиты. Метод MD5 проверяет целостность условий коммуникации и идентифицирует базу связи.

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

Определение общих параметров SNTP

На странице **Глобальные параметры SNTP** предоставлена информация по определению общих параметров SNTP. Чтобы открыть страницу **Глобальные параметры SNTP** нажмите **System (Система)** → **SNTP** → **Global Settings (Глобальные параметры)** в панели дерева.

Рисунок 6-8. Глобальные параметры SNTP



На странице **Глобальные параметры SNTP** есть следующие поля:

Poll Interval (60-86400) (Интервал между опросами) - Промежуток времени (в секундах), когда происходит запрос информации с односторонней передачей с сервера SNTP. Значение по умолчанию: 1024 секунды.

Receive Broadcast Servers Updates (Получение обновлений с серверов трансляции - При включении этого поля информация поступает с серверов SNTP на выбранные интерфейсы.

Receive Anycast Servers Updates (Получение обновлений с серверов альтернативной передачи) - При включении этого поля информация запрашивается с сервера SNTP с альтернативной передачей. Если включены оба поля - **Receive Anycast Servers Update** и **Receive Broadcast Servers Update**, системное время устанавливается в соответствии с данными, полученными с сервера с альтернативной передачей.

Receive Unicast Servers Updates (Получение обновлений с серверов односторонней передачи) - При включении этого поля информация запрашивается с сервера SNTP с односторонней передачей. Если включены поля **Receive Broadcast Servers Updates,**, **Receive Anycast Servers Updates** и **Receive Unicast Servers Updates**, системное время устанавливается в соответствии с данными, полученными с сервера с односторонней передачей.

Send Unicast Requests (Отправка запроса с односторонней передачей)- При включении этого поля отправляется запрос информации о времени с сервера SNTP с односторонней передачей на сервер SNTP **.**

Выбор источника времени

1. Откройте страницу **Time Synchronization (Синхронизация времени)**.
2. Определите поле **Clock Source** (Источник времени).
3. Нажмите кнопку Apply Changes (Применить изменения).

Источник времени выбран, а устройство обновлено.

Определение настройки локального времени

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

Локальное время настроено.

Определение общих параметров протокола SNTP с помощью команд консоли

В следующей таблице приведены команды консоли, соответствующие полям на странице **.**

Таблица 6-9. Команды для вывода глобальных параметров SNTP

Команды консоли	Описание
sntp broadcast client enable	Активирует клиентов трансляции сервера SNTP
sntp broadcast client enable	Активирует клиентов сервера SNTP с односторонней передачей
sntp broadcast client enable	Активирует предопределенных клиентов сервера SNTP с односторонней передачей

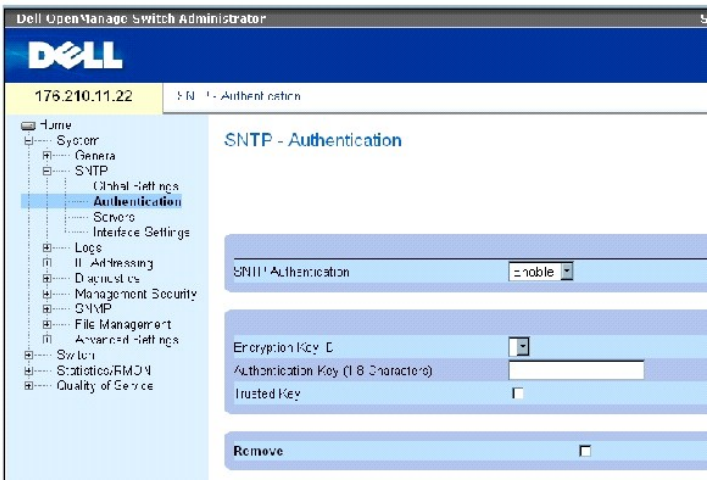
Ниже приведен пример команд консоли:

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

Определение методов идентификации SNTP

На странице Идентификация SNTP можно включить идентификацию SNTP между устройством и сервером SNTP. Другие методы ндентификации сервера SNTP приведены на странице Идентификация SNTP. Выберите **System (Система)** → **SNTP**→ **Authentication (Идентификация)** в панели дерева, чтобы открыть страницу Идентификация SNTP.

Рисунок 6-9. Идентификация SNTP



На странице Идентификация SNTP есть следующие поля:

SNTP Authentication (Идентификация SNTP)- При включении позволяет идентифицировать сеанс связи между устройством и сервером SNTP.

Encryption Key ID (Идентификатор ключа шифрования) - Определяет идентификатор ключа, использованного для аутентификации связи между устройством и сервером SNTP. Значение поля: до 4294967295.

Authentication Key (1-8 Characters) (Ключ идентификации, 1-8 символов) - Ключ, используемый для идентификации.

Trusted Key (Доверенный ключ)- Указывает ключ шифрования, использованный (с односторонней передачей) для идентификации сервера SNTP.

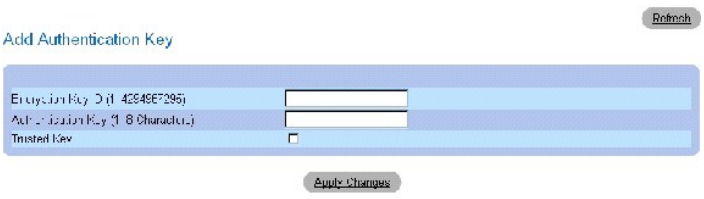
Remove (Удалить) - Если отметить это поле флажком, выбранный ключ идентификации будет удален.

Как добавить ключ идентификации сервера SNTP

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

Откроется страница .

Рисунок 6-10. Add Authentication Key (Добавление ключа идентификации)



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

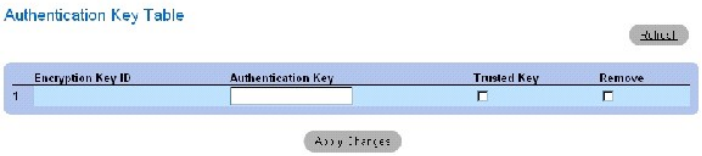
Новый ключ идентификации сервера SNMP добавлен, а устройство обновлено.

Вывод на экран таблицы ключа идентификации

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

Откроется страница **Таблица ключа идентификации**.

Рисунок 6-11. Таблица ключа идентификации



Удаление ключа идентификации

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

Откроется страница **Таблица ключа идентификации**.

3. Выберите поле **Authentication Key Table**.
4. Установите флажок Remove (Удалить).
5. Нажмите кнопку Apply Changes (Применить изменения).

Запись удалена, а устройство обновлено.

Определение параметров идентификации протокола SNTP с помощью команд консоли

В следующей таблице приведены команды консоли, соответствующие полям на странице **Идентификация SNTP**.

Таблица 6-10. Команды идентификации SNTP

Команды консоли	Описание
sntp authenticate	Определяет идентификацию полученного трафика протокола SNTP с серверов.
sntp trusted key	Идентифицирует систему, с которой будет синхронизирован сервер SNTP.
sntp authentication-key *номер* **md5** *значение*	Определяет ключ идентификации для SNTP.

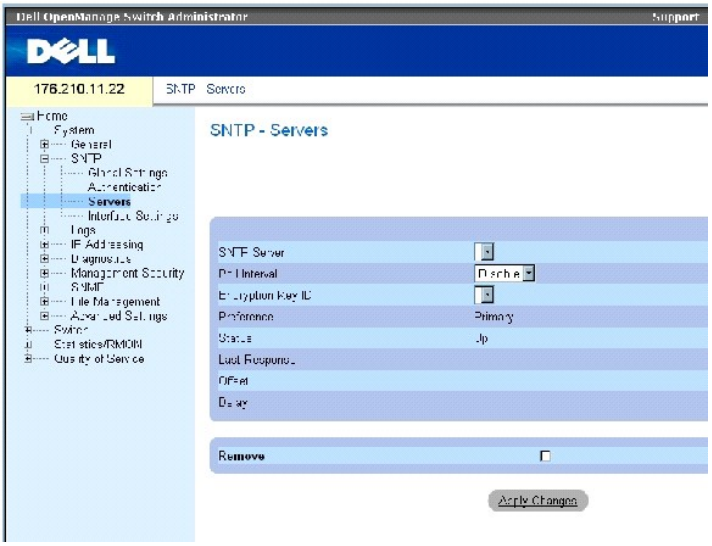
Ниже приведен пример команд консоли:

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

console(config)# sntp
trusted-key 8

Console(config)# sntp
authenticate
```

Определение серверов SNTP

Серверы SNTP можно включить или добавить со страницы **Серверы SNTP**. *Чтобы открыть страницу* **Серверы SNTP** , щелкните **System (Система)**→ **SNTP** → **Servers (Серверы)** в панели*дерева*.

Рисунок 6-12. Серверы SNTP



На странице **Серверы SNTP** есть следующие поля:

SNTP Server (Сервер SNTP)- Выбор IP-адреса сервера SNTP - задается пользователем. Можно задать до восьми серверов SNTP.

Poll Interval (Интервал между опросами)- При включении отправляет запрос информации о системном времени на выбранный сервер SNTP.

Encryption Key ID (Идентификатор ключа шифрования) - Определяет идентификатор ключа, использованного для аутентификации связи между устройством и сервером SNTP. Диапазон значений: от 1 до 4294967295.

Preference (Привилегия) - Сервер SNTP, который предоставляет информации о системном времени SNTP. Возможные значения поля:

Primary (Основной) - Информация поступает с главного сервера SNTP.

Secondary (Второстепенный) - Информация поступает с резервного сервера SNTP.

Status (Состояние) - Состояние действующего сервера SNTP. Возможные значения поля:

Up (Активен) - Сервер SNTP работает в нормальном режиме.

Down (Не активен) - Сервер SNTP временно недоступен. Например, сервер SNTP временно отключен или неактивен.

In progress (Занят)- Идет пересылка или отправление данных с сервера SNTP.

Unknown (Нет данных) - Нет данных о ходе пересылки данных SNTP. Например, в этот момент устройство выполняет поиск интерфейса.

Last Response (Последний ответ) - Время последнего ответа, поступившего с сервера SNTP.

Offset (Сдвиг) - Разница между значением локального времени устройства и полученным значением с сервера SNTP.

Delay (Задержка) - Время, необходимое для доступа к серверу SNTP.

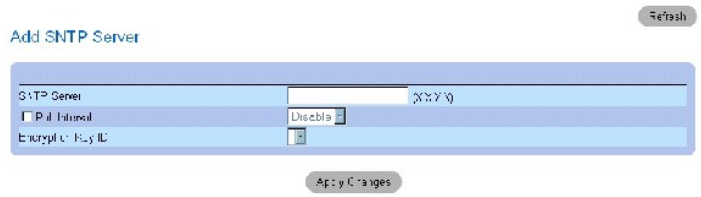
Remove (Удалить) - При включении этого поля определенный сервер SNTP удаляется из списка SNTP Servers (Серверы SNTP).

Как добавить сервер SNTP

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

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

Рисунок 6-13. Add SNTP Server (Добавление сервера SNTP)



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

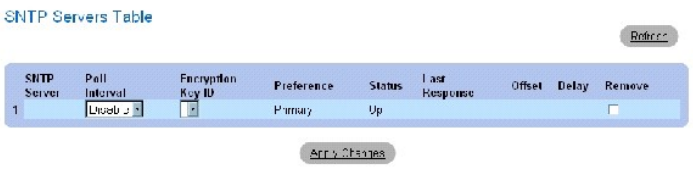
Сервер SNTP добавлен, а устройство обновлено.

Вывод таблицы серверов SNTP:

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

Откроется страница **Таблица серверов SNTP**.

Рисунок 6-14. Таблица серверов SNTP



Как модифицировать сервер SNTP

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

   Откроется страница **Таблица серверов SNTP**.
3. Выберите поле SNTP Server (Сервер SNTP).
4. Внесите изменения в соответствующие поля.
5. Нажмите кнопку Apply Changes (Применить изменения).

   Параметры сервера SNTP обновлены.

Как удалить сервер SNTP

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

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

   Запись удалена, а устройство обновлено.

Определение параметров серверов SNTP с помощью команд консоли

В следующей таблице приведены команды консоли, соответствующие полям на странице **SNTP Server (Сервер SNTP)**.

Таблица 6-11. Команды для сервера SNTP

Команды консоли	Описание
sntp server ip-адрес|hostname [poll] [key идентификатов ключа]	Конфигурация устройства на использование сервера SNTP, чтобы отправлять запросы и получать трафик SNTP.

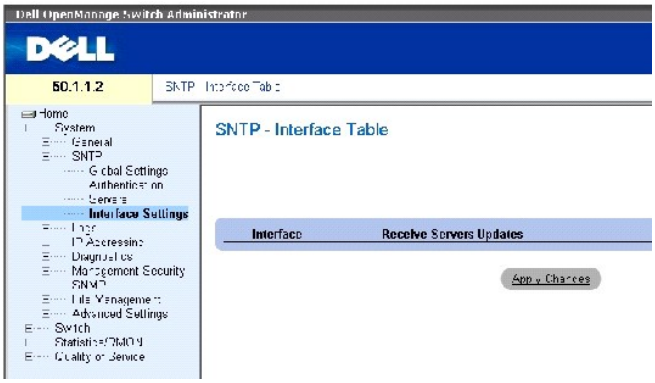
Ниже приведен пример команд консоли:

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

Определение интерфейсов SNTP

На странице **Параметры интерфейса SNTP** содержится информация об нитерфейсе SNTP. Чтобы открыть страницу **Параметры интерфейса SNTP** щелкните System (Система)→SNTP→ Interface Settings (Параметры интерфейса).

Рисунок 6-15. Параметры интерфейса SNTP



На странице Параметры интерфейса SNTP есть следующие поля:

Unit No. (Номер устройства) - Компонент стека, на котором включен интерфейс SNTP.

Interface (Интерфейс) - Список интерфейсов, на которых можно включить SNTP.

Receive Servers Updates (Получение обновлений с серверов) - Включение или отключение SNTP на определенном интерфейсе.

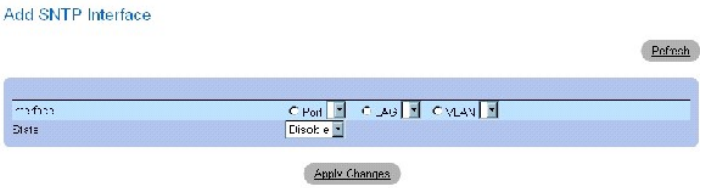
Remove (Удалить) - При включении удаляет SNTP с определенного интерфейса.

Как добавить SNTP-интерфейс:

1. Откройте страницу **Параметры интерфейса SNTP**.
2. Нажмите кнопку Add (Добавить).

   Откроется страница **Add SNTP Interface** (Добавить SNTP-интерфейс).

Рисунок 6-16. Add SNTP Server (Добавить SNTP-интерфейс)



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

   Интерфейс SNTP добавлен, а устройство обновлено.

Определение параметров интерфейса SNTP с помощью команд консоли

В следующей таблице приведены команды консоли, соответствующие полям на странице **Параметры интерфейса SNTP**.

ПРИМЕЧАНИЕ. Необходимо задать IP-адрес интерфейса, чтобы отнести его к категории альтернативных или трансляционных интерфейсов.

Таблица 6-12. Команды вызова параметров интерфейса SNTP

Команды консоли	Описание
sntp client enable	Включает клиент простого протокола сетевого управления (SNTP) на интерфейсе.
show sntp configuration	Вызов на экран конфигурации простого протокола сетевого управления (SNTP).

Далее приведен пример команды для вывода на экран интерфейсов SNTP:

```
console# show sntp configuration

Polling interval: 7200 seconds.

MD5 Authentication keys: 8, 9

Authentication is required for synchronization.

Trusted Keys: 8,9

Unicast Clients Polling: Enabled.

Server                          Polling     Encryption Key
-----------                     --------    ---------------
176.1.1.8                       Enabled     9
176.1.8.179                     Disabled    Disabled

Broadcast Clients: Enabled

Broadcast Clients Poll: Enabled

Broadcast Interfaces:1/e1, 1/e3
```

Управление журналами

На странице **Logs** (Журналы) даны ссылки на страницы разных журналов. Чтобы открыть страницу , нажмите System (Система) → Logs (Журналы) в панели дерева.

Определение общих параметров журналов

Системные журналы позволяют просматривать события устройства в условиях реального времени и сохраняют запись о них для последующего использования. Системные журнылы протоколируют и управляют событиями и создают отчет об ошибках или информационных предупреждениях.

Сообщения о событиях имеют уникальный формат, согласно рекомендуемому формату сообщений протокола System Logs для всех сообщений об ошибках. Например, отчетам об ошибках локальных устройств и серверов системных журналов назначается код важности. Они включают в себя мнемосхему сообщения, идентифицирующую исходное приложение, создавшее сообщение. Это дает возможность фильтровать сообщения по срочности и степени соответствия. Распределение сообщений журнала событий по различным пунктам назначения, например во внутренний буфер, файл журнала или сервер Syslog, управляется с помощью параметров конфигурации Syslog. Пользователи могут задать до восьми серверов системных журналов.

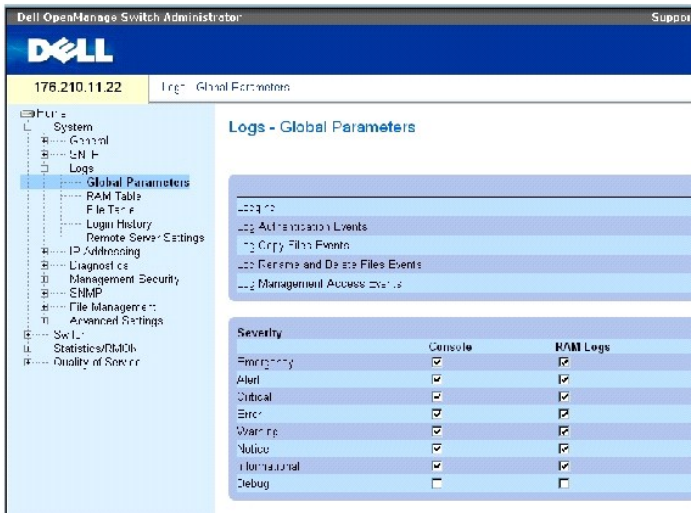
В следующей таблице приведены уровни важности ошибок журнала:

Таблица 6-13. Уровни важности журнала

Тип важности	Уровень важности	Описание
Emergency (Аварийный)	0	Система не работает.
Alert (Тревога)	1	Требуется немедленно обратить внимание на систему.
Critical (Критический)	2	Система в критическом состоянии.
Error (Ошибка)	3	Произошла системная ошибка.
Warning (Предупреждение)	4	Выдается системное предупреждение.
Notice (Замечание)	5	Система работает правильно, но выдано системное замечание.
Informational (Информационный)	6	Предоставляет сведения об устройствах.
Debug (Отладка)	7	Предоставляют подробные сведения о журнале. При ошибке Debug свяжитесь с оперативной службой технической поддержки Dell.

На странице Общие параметры журналов содержатся поля, которые позволяют определить, в каких журналах фиксируются те или иные события. Она содержит поля для включения журналов в целом и поля для определения параметров журналов. Сообщения журнала Severity перечисляются в порядке от высшей важности к низшей. Чтобы открыть страницу Общие параметры журналов нажмите System (Система) → Logs (Журналы) → Global Parameters (Глобальные параметры) в панели дерева.

Рисунок 6-17. Общие параметры журналов



На странице Общие параметры журналов есть следующие параметры:

Logging (Протоколирование) - Включает сохранение общих журналов устройства в журналах кэша, файла и сервера. Журналы консоли включены по умолчанию.

Log Authentication Events (События идентификации) - Событие заносится в журнал после того, как пользователи идентифицированы.

Log Copy Files Events (События копирования файлов) - Событие заносится в журнал после того, как файлы скопированы.

Log Rename and Delete Files Events (События переименования и удаления файлов)- Событие заносится в журнал после того, как архивный файл конфигурации был переименован или удален.

Log Management Access Events (События доступа к управлению)- Событие заносится в журнал после того, как произошел доступ к устройству с использованием метода управления. Например, каждый раз, когда выполняется доступ к устройству с использованием метода SSH, событие заносится в журнал устройства.

Severity (Важность) - Доступны следующие журналы важности:

Emergency (Аварийный) - Указывает на высший уровень предупреждений. Если устройство выключено или работает неправильно, сообщение аварийного журнала сохраняется в определенном местоположении журнала.

Alert (Тревога) - Указывает на вторую по уровню важность предупреждения. Этот журнал сохраняется при серьезных отклонениях в работе устройства , например, при попытке загрузить несуществующий файл конфигурации.

Critical (Критический) - Указывает на третью по уровню важность предупреждения. Критический журнал сохраняется, если происходят критические отклонения в работе устройства, например, если не функционируют два порта устройства, в то время как остальные остаются рабочими.

Error (Ошибка)- Произошла системная ошибка, например, не удалось выполнить операцию копирования.

Warning (Предупреждение) - Указывает на низший уровень предупреждения устройства. Например, устройство функционирует, но связь порта временно не работает.

Notice (Замечание) - Предоставляет важные сведения об устройстве.

Informational (Информационный) - Предоставляет сведения об устройствах. Например, в данный момент порт включен.

Debug (Отладка) - Предоставляет сообщения отладки.

ПРИМЕЧАНИЕ. Если выбирается уровень важности, автоматически выбираются и все уровни важности, указанные выше него.

На странице Global Log Parameters (Общие параметры журналов) также есть флажки, соответствующие разным системам протоколирования:

Console (Консоль) - Минимальный уровень важности, начиная с которого журналы отправляются на консоль.

RAM Logs (Журналы ОЗУ) - Минимальный уровень важности, начиная с которого журналы отправляются в файл журналов, хранящийся в ОЗУ (в кэше).

Log File (Файл журналов) - Минимальный уровень важности, начиная с которого журналы отправляются в файл журналов, хранящийся во FLASH-памяти.

Включение журналов:

1. Откройте страницу Global Log Parameters(Общие параметры журналов).
2. Выберите **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, соответствующие полям на странице Global Log Parameters (Общие параметры журналов).

Таблица 6-14. Команды для вызова общих параметров журнала

Команды консоли	Описание
logging on	Включает протоколирование сообщений об ошибках.
logging {ip-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.

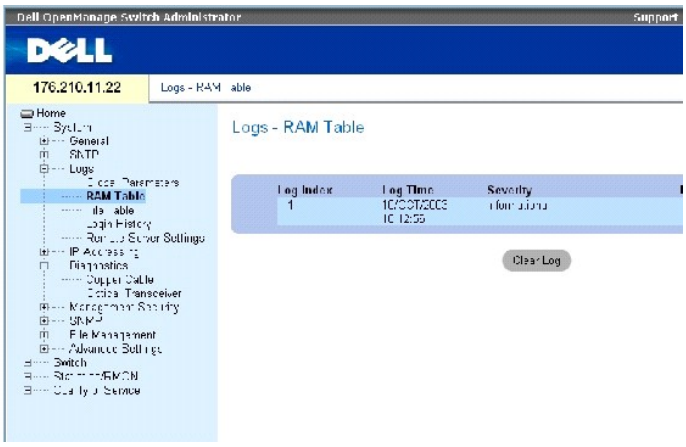
Ниже приведен пример команд консоли:

```
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
```

Просмотр 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 введен журнал, важность журнала и описание журнала. Чтобы открыть страницу **RAM Log Table (Таблица журнала ОЗУ)**нажмите System (Система) → Logs (Журналы) → RAM Table (Таблица ОЗУ) в панели дерева.

Рисунок 6-18. RAM Log Table (Таблица журнала ОЗУ)



На странице **RAM Log Table (Таблица журнала ОЗУ)** есть следующие поля:

Log Index (Индекс журнала) - 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 - Важность журнала.

Description (Описание) - Описывает запись в журнале.

Удаление информации 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** (Таблицы журнала ОЗУ), а устройство обновлено.

Просмотр и удаление RAM Log Table с помощью команд консоли

В следующей таблице приведены команды консоли, соответствующие полям на странице **RAM Log Table (Таблица журнала ОЗУ)**.

Таблица 6-15. Команды страницы RAM Log Table

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

Ниже приведен пример команд консоли:

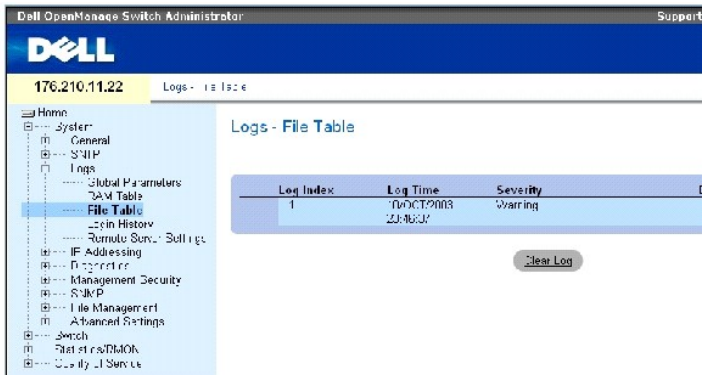
```
console# show logging

Logging is enabled.
```

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



Buffer Logging: Level
info. Buffer Messages: 26
Logged, 26 Displayed, 200
Max.



File Logging: Level error.
File Messages: 157 Logged,
26 Dropped.



1 messages were not logged



01-Jan-2000 01:03:42 :%
INIT-I-Startup: Cold
Startup



01-Jan-2000 01:01:36 :%
LINK-W-Down: 1/e14



01-Jan-2000 01:01:36 :%
LINK-W-Down: 1/e13



01-Jan-2000 01:01:36 :%
LINK-W-Down: 1/e12



01-Jan-2000 01:01:36 :%
LINK-W-Down: 1/e15



01-Jan-2000 01:01:32 :%
INIT-I-InitCompleted:
Initialization task is
completed




console# clear logging



Clear Logging Buffer
[y/n]?
```

Вывод таблицы файла журнала

Таблица Log File содержит сведения о записях журнала, сохраненных в файле журналов во FLASH-памяти, включая время, когда был введен журнал, важность журнала и описание сообщения журнала. Чтобы открыть страницу Таблица Log File нажмите System (Система) →Logs (Журналы) → File Table (Таблица файла) в панели дерева.

Рисунок 6-19. Таблица Log File



На странице Таблица Log File есть следующие поля:

Log Index (Индекс журнала) - Номер журнала в **Log File Table** (Таблица файла журнала).

Log Time (Время журнала) - Время, когда журнал был введен в **Log File Table** (Таблица файла журнала).

Severity - Важность журнала.

Description (Описание) - Текст сообщения журнала.

Вывод таблицы файла журналов с помощью команд консоли

В следующей таблице приведены команды консоли, соответствующие полям на странице Таблица Log File.

Таблица 6-16. Команды страницы Log File Table

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

Ниже 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.
```

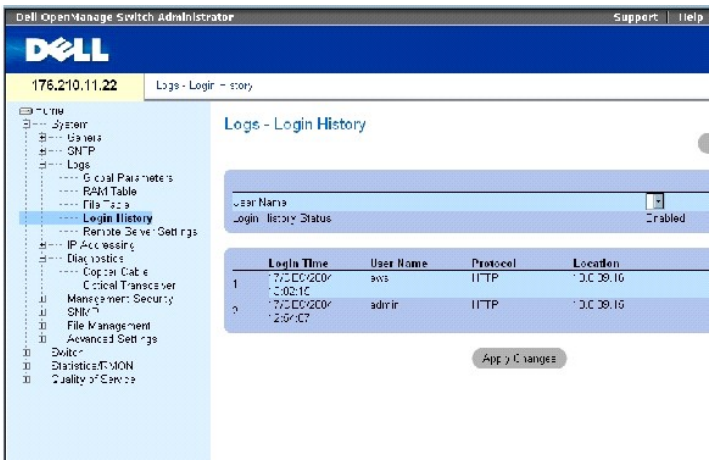
```
File Logging: Level
debug. File Messages:
11 Logged, 51
Dropped.



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
```

Обзор страницы Login History (Регистрация входа в систему)

На странице **Login History (Регистрация входа в систему)** содержится информация по просмотру и проверке использования устройства, включая время входа в систему и используемый для этого протокол.

Чтобы открыть страницу **Login History (Регистрация входа в систему)** нажмите System (Система) → Logs (Журналы) → Login History (Регистрация входа в систему) в панели дерева.

Рисунок 6-20. Login History (Регистрация входа в систему)



На странице **Login History (Регистрация входа в систему)** есть следующие поля:

User Name (Имя пользователя) - Список пользователей системы.

Login History Status (Состояние регистрации входа в систему) - Показывает, включены ли в устройстве журналы доступа по паролю.

Login Time (Время входа) - Время входа в систему определенным пользователем.

User Name (Имя пользователя) - Указывает пользователя, который выполнил вход в систему.

Protocol (Протокол) - Указывает, какой протокол был использован для входа в систему.

Location (Местоположение) - Указывает IP-адрес рабочей станции, с которой был получен доступ к устройству.

Как просмотреть регистрацию входа в систему

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

На экране появится регистрационная информация входа для выбранного пользователя.

Команды для вывода регистрации входа в систему

В следующей таблице приведены команды консоли, соответствующие полям на странице **Login History (Регистрация входа в систему)**.

Таблица 6-17. Команды страницы Log File Table

Команды консоли	Описание
show users login-history	Информация о входе по паролю

Ниже приведен пример команд консоли:

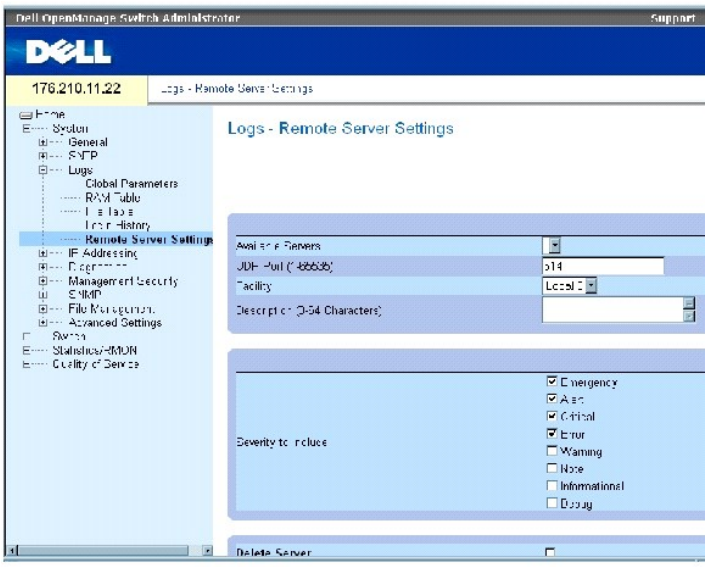
console# **show users login-history**

Login Time	Username	Protocol	Location
----------	--------	--------	----------
Jan 1. 2005 23:58:17	Anna	HTTP	172.16.1.8
Jan 1. 2005 07:59:23	Errol	HTTP	172.16.0.8
Jan 1. 2005 08:23:48	Amy	Serial	
Jan 1. 2005 08:29:29	Alan	SSH	172.16.0.8
Jan 1. 2005 08:42:31	Bob	HTTP	172.16.0.1
Jan 1. 2005 08:49:52	Cindy	Telnet	172.16.1.7

Изменение параметров отдаленного сервера протоколирования

На странице **Параметры отдаленного сервера протоколирования** есть поля для просмотра и настройки доступных серверов протоколирования. Кроме того, можно определить новые серверы журналов и важность журналов, отправляемых на каждый сервер. Чтобы открыть страницу **Параметры отдаленного сервера протоколирования** нажмите System (Система) → Logs (Журналы)→ Remote Server Settings (Параметры отдаленного сервера) в панели дерева.

Рисунок 6-21. Параметры отдаленного сервера протоколирования



На странице **Параметры отдаленного сервера протоколирования** есть следующие поля:

Available Servers (Доступные серверы) - Список серверов, которым 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 (Средство) - Показывает программу, определенную пользователем, которая используется для передачи системных журналов на отдаленный сервер. Возможно назначить только одно программное средство для каждого сервера. Если назначается вторая программа, она занимает место первой. Все программы, работающие в устройстве, используют одно программное средство на сервере. Значение по умолчанию: Local 7. Возможны следующие значения:

Local 0 - Local 7.

Description (0-64 Characters) (Описание, 0-64 символа) - Описание сервера, заданного пользователем.

Delete Server (Удалить сервер) - Удаляет выбранный сервер из списка Available Servers (Доступные серверы).

На странице Параметры отдаленного сервера протоколирования также есть список важности. Определения важности такие же, как и для страницы Общие параметры журналов.

Отправка журналов на сервер:

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

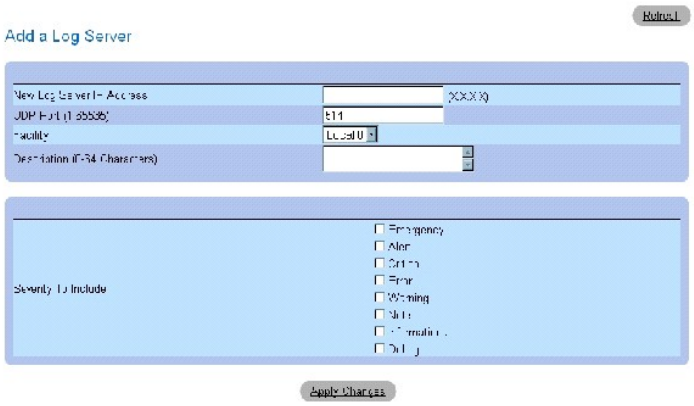
Параметры журналов будут сохранены, а устройство обновлено.

Определение нового сервера:

1. Откройте страницу Параметры отдаленного сервера протоколирования.
2. Нажмите кнопку **Add** (Добавить).

Откроется страница Add a Log Server (Добавление сервера протоколирования).

Рисунок 6-22. Add a Log Server (Добавление сервера протоколирования).



На странице Add a Log Server (Добавление сервера протоколирования) есть дополнительные поля:

New Log Server IP Address - IP-адрес для нового сервера журналов.

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

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

Отображение таблицы Log Servers Table (Таблица серверов протоколирования):

1. Откройте страницу Параметры отдаленного сервера протоколирования.
2. Нажмите кнопку **Show All** (Показать все).

Откроется страница Log Servers Table (Таблица серверов протоколирования).

Рисунок 6-23. Log Servers Table (Таблица серверов протоколирования)

Как удалить сервер протоколирования со страницы Log Servers Table (Таблица серверов протоколирования):

1. Откройте страницу **Параметры отдаленного сервера протоколирования**.
2. Нажмите кнопку **Show All** (Показать все).

Откроется страница **Log Servers Table (Таблица серверов протоколирования)**.

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

Запись **Log Servers Table (Таблица серверов протоколирования)** удалена, а устройство обновлено.

Работа с удаленными журналами с использованием команд консоли

В следующей таблице приведены команды для работы с удаленными серверами протоколирования.

Таблица 6-18. Команды страницы Remote Log Server

Команды консоли	Описание
logging *(ip-address* **|** *hostname}* **[port** *port*] [**severity** *level*] [**facility** *facility*] [**description** *text*]	Регистрирует сообщения на отдаленном сервере.
no logging	Удаляет сервер системных журналов.
show logging	Отображение состояния протоколирования и сообщений системного журнала.

Ниже 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

На странице IP Addressing (IP-адресация) даны ссылки для назначения IP-адресов интерфейса и шлюзов по умолчанию и для определения параметров ARP и DHCP для интерфейсов. Чтобы открыть страницу IP Addressing (IP-адресация) , нажмите System (Система) → IP Addressing (IP-адресация) в панели дерева.

Определение стандартных шлюзов

Страница **Default Gateway** (Шлюз по умолчанию) позволяет сетевым менеджерам назначать устройства шлюзов. При отправке кадров в удаленную сеть пакеты пересылаются на стандартный IP-адрес. Настроенный IP-адрес должен принадлежать к той же подсети IP-адресов, что и один из IP интерфейсов. Чтобы открыть страницу **Default Gateway (Шлюз по умолчанию)**, выберите System (Система) → IP Addressing (IP-адресация→ Default Gateway (Шлюз по умолчанию) на панели дерева.

На странице **Default Gateway** (Шлюз по умолчанию) есть следующие поля:

User Defined (Заданный пользователем) - IP-адрес шлюза устройства.

Active (Активен) - Шлюз активен.

Remove User Defined (Удалить заданный пользователем)- При включении шлюз устройства будет удален из раскрывающегося списка **Default Gateway (Шлюз по умолчанию)**.

Как выбрать шлюз устройства:

1. Откройте страницу **Default Gateway** (Шлюз по умолчанию).
2. Выберите IP-адрес в раскрывающемся списке **Default Gateway** (Шлюз по умолчанию).
3. Установите флажок в поле Active (Активен).
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Для устройства выбран шлюз по умолчанию, а устройство обновлено.

Удаление шлюза по умолчанию:

1. Откройте страницу **Default Gateway** (Шлюз по умолчанию).
2. Установите флажок **Remove** (Удалить), чтобы удалить шлюзы по умолчанию.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Запись шлюзов по умолчанию будет удалена, а устройство обновлено.

Определение шлюза устройства с помощью команд консоли

В следующей таблице приведены команды консоли, соответствующие полям на странице **Default Gateway** (Шлюз по умолчанию).

Таблица 6-19. Команды страницы Default Gateway

Команды консоли	Описание
ip default-gateway ip-address	Определяет шлюз по умолчанию.
no ip default-gateway	Удаляет шлюз по умолчанию.

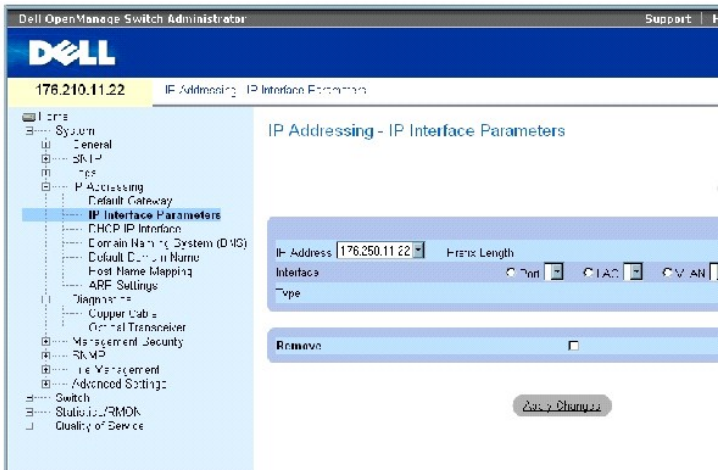
Ниже приведен пример команд консоли:

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



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

Определение IP-интерфейсов

На странице Страница IP Interfaces Parameters имеются поля для назначения IP-параметров для интерфейса. Чтобы открыть страницу Страница IP Interfaces Parameters нажмите **System (Система)** → **IP Addressing (IP-адресация)** → **IP Interface Parameters (IP-параметры интерфейса)** в панели дерева.

Рисунок 6-24. Страница IP Interfaces Parameters



На странице Страница IP Interfaces Parameters есть следующие параметры:

IP Address - IP-адрес интерфейса.

Prefix Length (Длина префикса) - Количество битов, составляющих исходный префикс IP-адреса, или маска сети исходного IP-адреса.

Source Interface (Исходный интерфейс) - Тип интерфейса, для которого определяется выбранный IP-адрес. Выберите **Port** (Порт), **LAG** или **VLAN**.

Type (Тип)- Указывает на то, был ли IP-адрес настроен статически.

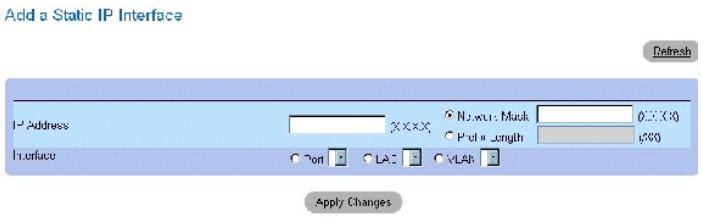
Remove (Удалить) - Удаляет выбранный интерфейс из раскрывающегося списка **IP Address** (IP-адрес).

Добавление IP-интерфейса

1. Откройте страницу Страница IP Interfaces Parameters.
2. Нажмите кнопку **Add** (Добавить).

Откроется страница Add a Static IP Interface (Добавить статический IP-интерфейс).

Рисунок 6-25. Add a Static IP Interface (Добавить статический IP-интерфейс)



Network Mask (Маска сети) - Указывает маску подсети исходного IP-адреса.

3. Заполните поля на странице.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Новый IP-адрес добавлен в интерфейс, а устройство обновлено.

Изменение параметров IP-адреса

1. Откройте страницу Страница IP Interfaces Parameters.
2. Выберите IP-адрес из раскрывающегося меню **IP Address (IP-адрес)** .
3. Измените тип интерфейса.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

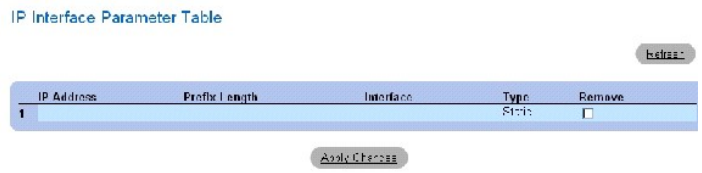
Параметры изменены, а устройство обновлено.

Удаление IP-адресов

1. Откройте страницу Страница IP Interfaces Parameters.
2. Нажмите кнопку **Show All** (Показать все).

Откроется страница **IP Interface Parameters Table** (Таблица параметров IP-интерфейсов).

Рисунок 6-26. Таблица параметров IP-интерфейсов



3. Выберите IP-адрес и отметьте флажком поле **Remove (Удалить)** .
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Выбранный IP-адрес удален, а устройство обновлено.

Определение IP-интерфейсов с помощью команд консоли

В следующей таблице приведены команды консоли, соответствующие полям на странице Страница IP Interfaces Parameters.

Таблица 6-20. Команды страницы IP Interface Parameters

Команды консоли	Описание
ip address ip-address {mask | prefix-length}	Задает IP-адрес.
no ip address [ip-address]	Удаляет IP-адрес.
show ip interface [ethernet interface-number | vlan vlan-id | port-channel number]	Выводит состояние готовности настроенных IP-интерфейсов.

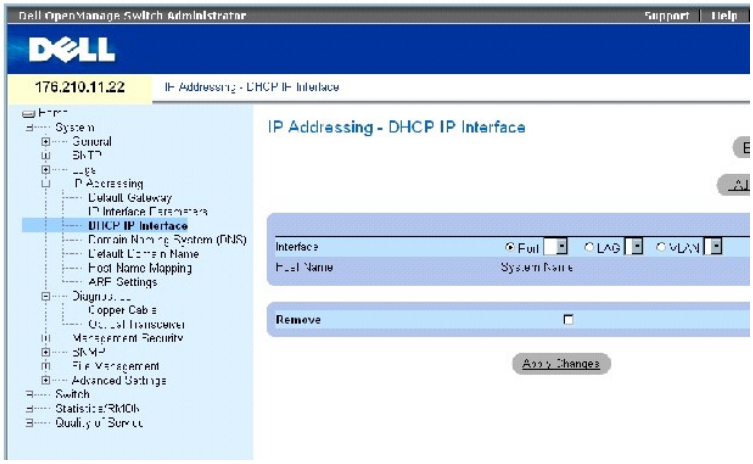
Ниже приведен пример команд консоли:

```
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 интерфейса DHCP

На странице **DHCP IP Interface (IP-интерфейс сервера DHCP)** имеются параметры для определения клиентов сервера DHCP, подключенных к устройству. Чтобы открыть страницу **DHCP IP Interface (IP-интерфейс сервера DHCP),** нажмите **System (Система)→ IP Addressing (IP-адресация) → DHCP IP Interface (IP-интерфейс сервера DHCP)** в панели дерева.

Рисунок 6-27. DHCP IP Interface (IP-интерфейс сервера DHCP)



На странице **DHCP IP Interface (IP-интерфейс сервера DHCP)** есть следующие поля:

Interface (Интерфейс) - Определенный интерфейс, подключенный к устройству. Щелкните переключатель, расположенный рядом с полями **Port**, **LAG** или **VLAN**, и выберите интерфейс, подключенный к устройству.

Host Name - Имя хоста.

Remove - Если включено, клиент DHCP удаляется.

Как добавить клиент сервера DHCP

1. Откройте страницу DHCP IP Interface (IP-интерфейс сервера DHCP).
2. Нажмите кнопку **Add** (Добавить).

   Откроется страница **Add DHCP IP Interface** .
3. Введите информацию на странице.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Интерфейс DHCP добавлен, а устройство обновлено.

Внесение изменений в IP-интерфейс сервера DHCP

1. Откройте страницу DHCP IP Interface (IP-интерфейс сервера DHCP).
2. Внесите изменения в соответствующие поля.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

   Запись будет изменена, а устройство обновлено.

Удаление IP-интерфейса сервера DHCP

1. Откройте страницу DHCP IP Interface (IP-интерфейс сервера DHCP).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **DHCP Client Table**.
3. Выберите запись клиента DHCP.
4. Установите флажок в поле **Remove** (Удалить).
5. Нажмите кнопку **Apply Changes** (Применить изменения).

   Выбранная запись удалена, а устройство обновлено.

Определение IP-интерфейсов сервера DHCP с помощью команд консоли

В следующей таблице приведены команды консоли, соответствующие полям для определения клиентов серверов DHCP.

Таблица 6-21. Команды страницы DHCP IP Interface

Команды консоли	Описание
ip address dhcp [**hostname** *host-name*]	Получает IP-адрес по интерфейсу ethernet от DHCP

Ниже приведен пример команды консоли.

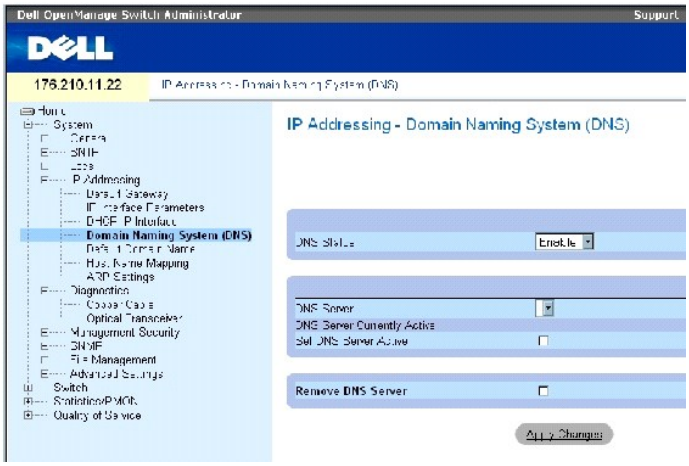
```
console(config)# interface
ethernet 1/e11

console(config-if)# ip
address dhcp
```

Конфигурация систем именования доменов

Служба имен доменов(DNS) преобразует заданные пользователем домены в IP-адреса. Всякий раз, когда имя домена задается в DNS, служба преобразует имя в IP-адрес. Например, www.ipexample.com преобразуется в 192.87.56.2. На сервере DNS сохраняются базы данных с именами домена и соответствующие им IP-адреса.

На странице **Domain Naming System (DNS) (Служба имен доменов)** имеются поля для включения и активации определенных серверов DNS . Чтобы открыть страницу **Domain Naming System (DNS) (Служба имен доменов)**нажмите **System (Система)** → **IP Addressing (IP-адресация)** → **Domain Naming System (DNS)** в панели дерева.

Рисунок 6-28. Domain Naming System (DNS) (Служба имен доменов)



На странице **Domain Naming System (DNS) (Служба имен доменов)** есть следующие поля:

DNS Status (Состояние DNS)- Включает или выключает преобразование имен доменов в IP-адреса.

DNS Server (Сервер DNS) - Список серверов DNS. Серверы DNS добавляются на странице **Add DNS Server**.

DNS Server Currently Active (Активный сервер DNS)- Сервер DNS, который является активным в данный момент.

Set DNS Server Active (Сделать сервер DNS активным) - Активирует выбранный сервер DNS.

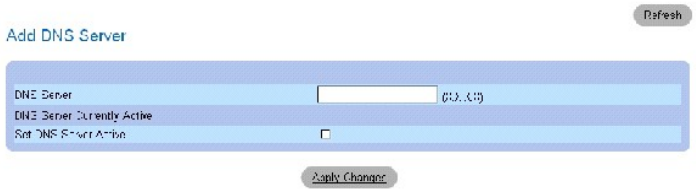
Remove DNS Server (Удалить сервер DNS) - Если поле включено, выбранный сервер DNS удаляется.

Добавление сервера DNS

1. Откройте страницу **Domain Naming System (DNS) (Служба имен доменов)**.
2. Нажмите кнопку **Add** (Добавить).

Откроется страница **Add DNS Server** (Добавить сервер DNS):

Рисунок 6-29. Add DNS Server (Добавить сервер DNS)



DNS Server (Сервер DNS) - IP-адрес сервера DNS.

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

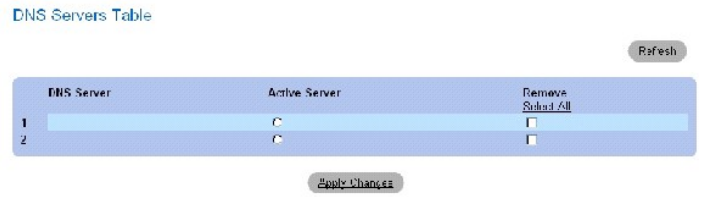
Новый сервер DNS определен, а устройство обновлено.

Вывод таблицы серверов DNS

1. Откройте страницу **Domain Naming System (DNS) (Служба имен доменов)**.
2. Нажмите кнопку **Show All** (Показать все).

Открывается страница **DNS Server Table**:

Рисунок 6-30. DNS Server Table (Таблица сервера DNS)



Удаление серверов DNS

1. Откройте страницу **Domain Naming System (DNS) (Служба имен доменов)**.
2. Нажмите кнопку **Show All** (Показать все).

Открывается страница **DNS Server Table**

3. Выберите запись **DNS Server Table** (Таблица сервера DNS).
4. Установите флажок в поле **Remove** (Удалить).
5. Нажмите кнопку **Apply Changes** (Применить изменения).

Выбранный сервер DNS удален, а устройство обновлено.

Настройка серверов DNS с помощью командной строки

В следующей таблице приведены команды консоли для конфигурации системной информации.

Таблица 6-22. Команды для сервера DNS

Команды консоли	Описание
ip name-server *server-address*	Задает доступные имена серверов. Можно задать до восьми имен серверов.
no ip name-server *server-address*	Удаляет имя сервера.
ip domain-name *name*	Определяет имя домена по умолчанию, которое используется программой для дополнения неизвестных имен хостов.
clear host {name | *}	Удаляет записи из кэша «имя хоста - адрес».
show hosts [*name*]	Отображает имя домена по умолчанию, список имен хостов сервера, статический и кэшированный списки имен хостов и адресов.
ip domain-lookup	Включает службу DNS для преобразования имен хостов в IP-адреса.

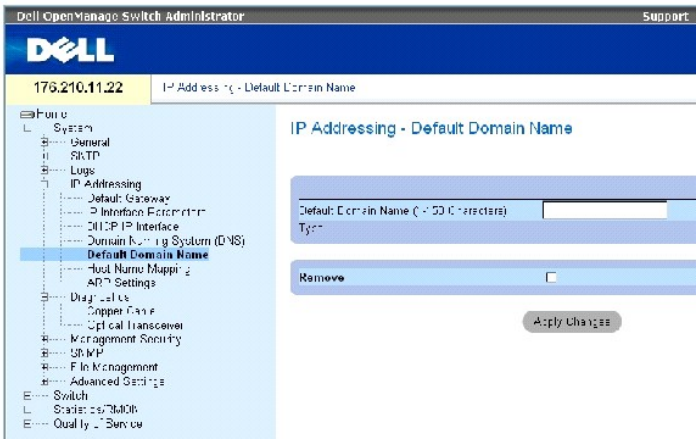
Ниже приведен пример команд консоли:

```
console(config)# ip name-server 176.16.1.18
```

Определение доменов по умолчанию

На странице **Default Domain Name (Имя домена по умолчанию)** предоставлена информация по определению имен доменов DNS по умолчанию. Чтобы открыть страницу **Default Domain Name (Имя домена по умолчанию)** щелкните **System (Система)→ IP Addressing (IP-адресация)→ Default Domain Name (Имя домена по умолчанию)**.

Рисунок 6-31. Default Domain Name (Имя домена по умолчанию)



На странице **Default Domain Name (Имя домена по умолчанию)** есть следующие поля:

Default Domain Name (1-158 characters) (Имя домена по умолчанию, 1-158 символов) - Содержит имя домена по умолчанию, заданное пользователем. При условии, что оно определено, имя домена по умолчанию применяется для всех неизвестных имен хостов.

Type (Тип)- Тип IP-адреса. Возможные значения поля:

Dynamic (Динамический)- IP-адрес создан динамически.

Static (Статический)- IP-адрес является статическим.

Remove (Удалить) - Если отмечено флажком, удаляет имя домена по умолчанию.

Команды для определения имен доменов DNS в режиме командной строки

В следующей таблице приведены команды консоли для конфигурации имен доменов DNS.

Таблица 6-23. Команды страницы DNS Domain Name

Команды консоли	Описание
ip domain-name *name*	Определяет имя домена по умолчанию, которое используется программой для дополнения неизвестных имен хостов.
no ip domain-name	Отключение службы имен доменов (DNS).
show hosts [*name***]**	Отображает имя домена по умолчанию, список имен хостов сервера, статический и кэшированный списки имен хостов и адресов.

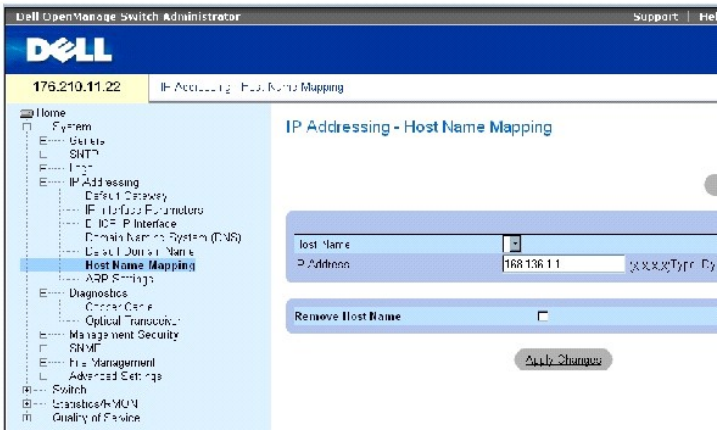
Ниже приведен пример команд консоли:

```
console(config)# ip
domain-name dell.com
```

Привязка хоста домена

На странице Host Name Mapping (Привязка хоста домена) предоставлены параметры для назначения IP-адресов статическим хостам. На этой странице каждому хосту можно присвоить один IP-адрес. Чтобы открыть страницу **Host Name Mapping (Привязка хоста домена)**, *выберите* **System (Система)→ IP Addressing (IP-адресация)→ Host Name Mapping (Привязка хоста домена)** в панели дерева.

Рисунок 6-32. Host Name Mapping (Привязка хоста домена)



На странице Host Name Mapping (Привязка хоста домена) есть следующие поля:

Host Name (Имя хоста)- Список имен хостов. Имена хостов задаются на странице **Add Host Name Mapping**. Каждый хост предоставляет один IP-адрес.

IP Address (X.X.X.X) (IP-адрес)- Предоставляет IP-адрес, назначенный для определенного имени хоста.

Type (Тип)- Тип IP-адреса. Возможные значения поля:

Dynamic (Динамический)- IP-адрес создан динамически.

Static (Статический)- IP-адрес является статическим.

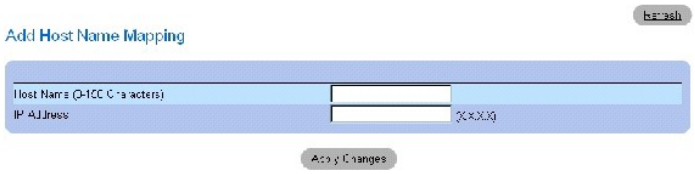
Remove Host Name (Удалить имя хоста)- Если отмечено флажком, удаляет привязку хоста DNS.

Как добавить имя домена хоста

1. Откройте страницу Host Name Mapping (Привязка хоста домена) .
2. Нажмите кнопку **Add** (Добавить).

Откроется страница **Add Host Name Mapping (Добавить привязку имени хоста)**:

Рисунок 6-33. Add Host Name Mapping (Добавить привязку имени хоста)



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

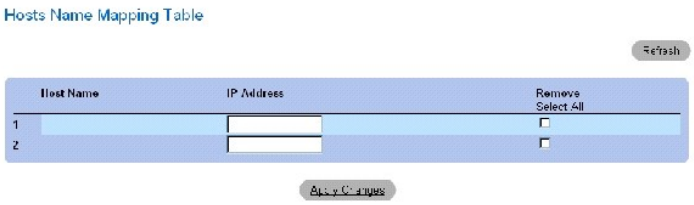
IP-адрес привязан к имени хоста, а устройство обновлено.

Вывод на экран страницы Hosts Name Mapping Table

1. Откройте страницу Host Name Mapping (Привязка хоста домена) .
2. Нажмите кнопку **Show All** (Показать все).

Откроется страница **Hosts Name Mapping Table** (Таблица привязки имени хоста):

Рисунок 6-34. Страница Hosts Name Mapping Table



Удаление имени хоста из привязки IP-адреса

1. Откройте страницу Host Name Mapping (Привязка хоста домена) .
2. Нажмите кнопку **Show All** (Показать все).
3. Откроется страница **Host Mapping Table** (Таблица привязки хоста):
4. Выберите запись **Host Name Mapping Table** (Таблица привязки имени хоста).
5. Установите флажок **Remove** (Удалить).
6. Нажмите кнопку **Apply Changes** (Применить изменения).

Запись **Host Mapping Table** (Таблица привязки хоста) будет удалена, а устройство обновлено.

Команды для привязки IP-адресов к именам хоста домена в режиме командной строки

В следующей таблице перечислены команды для привязки IP-адресов к именам хоста домена.

Таблица 6-24. Команды страницы Domain Host Name

Команды консоли	Описание
ip host *name address*	Определяет статическую привязку «имя хоста-адрес» в кэше хоста
no ip host name	Удаляет привязку «имя хоста-адрес».

clear host {name | *}	Удаляет записи из кэша «имя хоста - адрес».
show hosts [name]	Отображает имя домена по умолчанию, список имен хостов сервера, статический и кэшированный списки имен хостов и адресов.

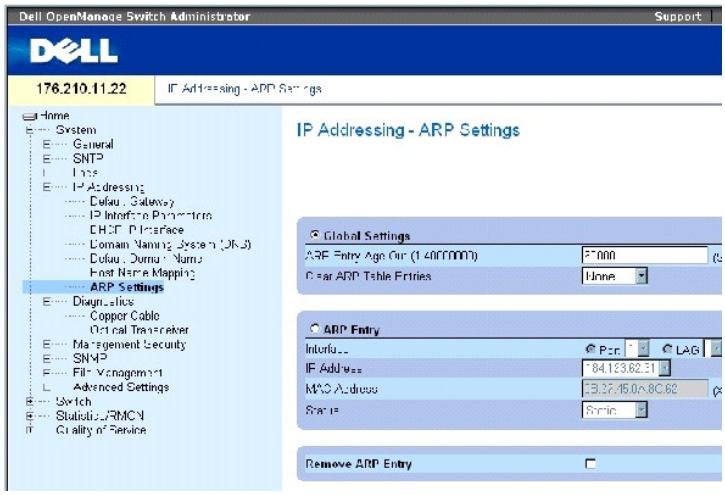
Ниже приведен пример команд консоли:

```
console(config)# ip host
accounting.abc.com
176.10.23.1
```

Определение параметров ARP

Протокол Address Resolution Protocol (ARP) (Протокол разрешения адресов) преобразует IP-адреса в физические и привязывает IP-адреса к MAC-адресам. Протокол ARP позволяет хосту связываться с другими хостами только при условии, что известен IP-адрес его соседей. Чтобы открыть страницу **Параметры ARP** , нажмите System (Система) → IP Addressing (IP-адресация) → ARP в панели дерева.

Рисунок 6-35. Параметры ARP



На странице **Параметры ARP** есть следующие поля:

Global Settings (Глобальные параметры) - Выберите это поле, чтобы активировать поля общих параметров ARP.

ARP Entry Age Out (1-40000000) (Срок хранения записи ARP)- Для всех устройств это интервал времени (в секундах) между запросами таблицы ARP с сервера . По истечении этого периода запись удаляется из таблицы. Диапазон значений: от 1 до 40000000. Значение по умолчанию: 60000 секунд.

Clear ARP Table Entries (Удалить записи таблицы ARP) - Указывает тип удаляемых записей ARP. Возможные значения:

None (Нет) - Указывает, что записи ARP не удаляются.

All (Все) - Указывает, что все записи ARP удаляются.

Dynamic (Динамические) - Указывает, что удаляются только динамические записи ARP.

Static (Статические) - Указывает, что удаляются только статические записи ARP.

ARP Entry (Запись ARP) - Выберите это поле, чтобы активировать поля параметров ARP на устройствах Ethernet.

Interface (Интерфейс) - Номер интерфейса порта, LAG или VLAN, который подключен к устройству.

IP Address (IP-адрес) - IP-адрес рабочей станции, который ассоциируется с MAC-адресом, приведенном ниже.

MAC Address (MAC-адрес) - MAC-адрес рабочей станции, который ассоциируется в таблице ARP с IP-адресом .

Status (Состояние) - Состояние записи таблицы ARP . Возможные значения поля:

Dynamic (Динамический)- Запись ARP создана динамически.

Static (Статический) - Запись ARP является статической.

Remove ARP Entry (Удалить запись ARP) - Если выбран этот вариант, запись ARP удаляется.

Добавление статической записи таблицы ARP:

1. Откройте страницу **Параметры ARP**.
2. Нажмите кнопку **Add** (Добавить).

Откроется страница **Add ARP Entry** (Добавить запись ARP).

3. Выберите тип интерфейса.
4. Определите поля.
5. Нажмите кнопку Apply Changes (Применить изменения).

Запись **ARP Table** (Таблицы ARP) будет добавлена, а устройство обновлено.

Вывод таблицы ARP

1. Откройте страницу **Параметры ARP**.
2. Нажмите кнопку **Show All** (Показать все).

Откроется страница **ARP Table** (Таблица ARP).

Удаление записи таблицы ARP

1. Откройте страницу **Параметры ARP**.
2. Нажмите кнопку **Show All** (Показать все).

Откроется страница **ARP Table** (Таблица ARP).

3. Выберите запись таблицы.
4. Установите флажок в поле **Remove** (Удалить).
5. Нажмите кнопку Apply Changes (Применить изменения).

Запись **ARP Table** ((Таблица ARP) будет удалена, а устройство обновлено.

Настройка серверов ARP с помощью командной строки

В следующей таблице приведены команды консоли, соответствующие полям на странице **Параметры ARP**.

Таблица 6-25. Команды страницы ARP Settings

Команды консоли	Описание
arp ip_addr hw_addr {ethernet interface-number | vlan vlan-id | port-channel number}	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.

Ниже 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

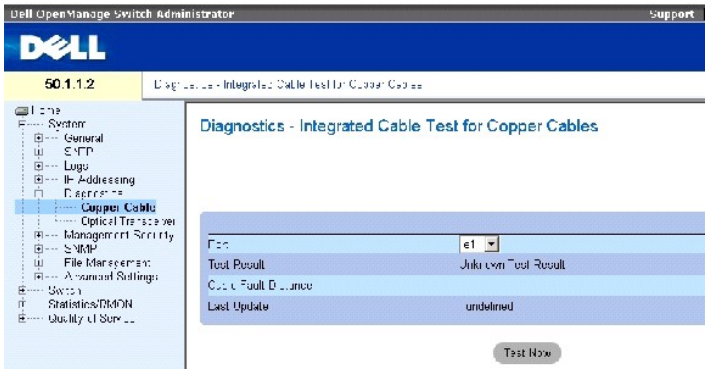
На странице **Diagnostics (Диагностика)** имеются ссылки на страницы, на которых можно выполнять виртуальное тестирование медных кабелей. Чтобы открыть страницу **Diagnostics (Диагностика)**, нажмите **System (Система)** → **Diagnostics (Диагностика)** в панели дерева.

Обзор страницы Copper Cable Diagnostics (Диагностика медных кабелей)

На странице **Медные кабели** содержатся поля, позволяющие выполнять тестирование медных кабелей. Тестирование кабелей предоставляет информацию об ошибках, произошедших в кабеле, времени проведения последнего тестирования кабеля и типе ошибки кабеля. При тестировании используется технология измерения коэффициента отражения (TDR), которая выполняет тестирование качества и технических характеристик медных кабелей, подключенных к порту. Можно тестировать кабели длиной до 120 метров. Тестирование кабелей выполняется, когда порты находятся в неактивном состоянии; исключение составляет тестирование приблизительной длины кабеля.

Чтобы открыть страницу **Медные кабели**, нажмите **System (Система)** → **Diagnostics (Диагностика)** →**Copper Cable (Медный кабель)** в панели дерева.

Рисунок 6-36. Медные кабели



На странице **Медные кабели**есть следующие поля:

Port (Порт). Порт, к которому подключен кабель.

Test Result (Результат тестирования). Определение результатов тестирования кабеля. Возможные значения поля:

No Cable (Нет кабеля). Кабели, подключенные к данному порту, отсутствуют.

Open Cable (Открытый кабель). Кабель не подключен с другой стороны.

Short Cable Короткое замыкание в кабеле). В кабеле произошло короткое замыкание.

OK. Тестирование кабеля выполнено успешно

Cable Fault Distance (Расстояние до кабеля со сбоем). Определение расстояния от порта, в котором произошла ошибка кабеля.

Last Update (Последние обновление). Время последнего тестирования кабеля.

Approximate Cable Length (Приблизительная длина кабеля). Приблизительная длина кабеля. Этот тест может быть выполнен, только если порт включен и работает со скоростью 1 Гбит/с.

Тестирование кабеля

1. Убедитесь, что оба конца медного кабеля подключены к устройству.
2. Откройте страницу **Медные кабели**.
3. Выберите тестируемый интерфейс.
4. Нажмите **Test Now** (Протестировать сейчас).

Выполняется тестирование медного кабеля, а результаты отображаются на странице **Медные кабели**.

Отображение таблицы результатов виртуального тестирования кабеля

1. Откройте страницу **Медные кабели**.
2. Нажмите кнопку **Show All** (Показать все).

Откроется страница **Integrated Cable Test Results Table (Таблица результатов виртуального тестирования кабеля)**.

ПРИМЕЧАНИЕ. На этом экране показаны результаты только что выполненного теста, но не ход выполнения теста на портах.

Кроме полей на странице **Медные кабели** , в таблице **Integrated Cable Test Results Table (Таблица результатов виртуального тестирования кабеля)** содержится следующее поле:

Unit No (Номер блока). - Номер устройства, которому соответствует показанный кабель.

Команды консоли для выполнения тестирования медного кабеля

В следующей таблице приведены команды для выполнения тестирования медного кабеля.

Таблица 6-26. Команды страницы Copper Cable Test

Команды консоли	Описание
test copper-port tdr *interface*	Выполняет виртуальный тест кабеля VCT.
show copper-port tdr *interface*	Показывает результаты последнего тестирования кабелей портов.
show copper-port cable-length *interface*	Примерная длина медного кабеля, подключенного к порту.

Ниже 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
```

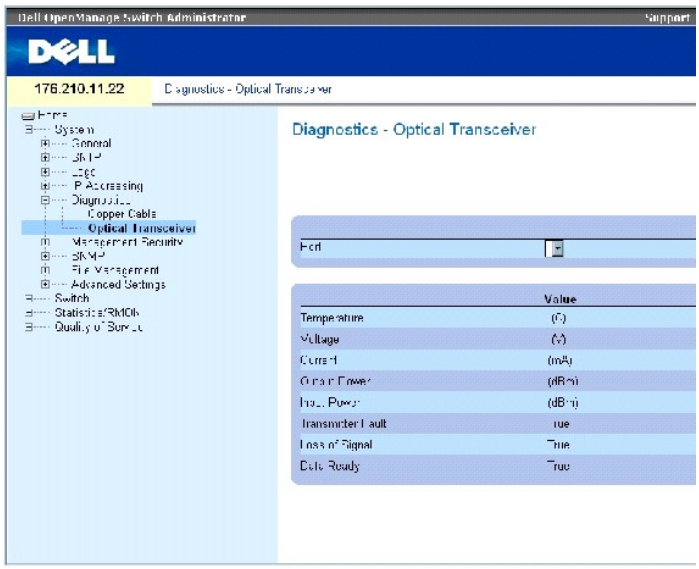
ПРИМЕЧАНИЕ. Возвращаемая длина кабеля (по результатам теста ICT)- это приближенное значение в следующих диапазонах: до 50 метров, от 50 до 80 м, от 80 до 110 м, от 110 до 120 м или более 120 м. Погрешность может составлять до 20 метров, и измерение длины не выполняется для кабелей со скоростью передачи данных 10 Мбит/с.

Обзор страницы Optical Transceiver Diagnostics (Диагностика оптического трансивера)

Используйте страницу Оптический трансивер для тестирования оптоволоконных кабелей. Чтобы открыть страницу Оптический трансивер, нажмите **System (Система)** → **Diagnostics (Диагностика)** →**Optical Transceiver** (Оптический трансивер) в панели дерева.

ПРИМЕЧАНИЕ. Диагностику оптического трансивера можно проводить только при наличии соединения.

Рисунок 6-37. Оптический трансивер



На странице Оптический трансивер есть следующие поля:

Port (Порт) - IP-адрес порта, на котором тестируется кабель.

Temperature (Температура) - Температура (C), при которой работает кабель.

Voltage (Напряжение) - Напряжение, с которым работает кабель.

Current (Ток) - Ток, от которого работает кабель.

Output Power (Выходная мощность) - Скорость передачи мощности на выходе.

Input Power (Входная мощность) - Скорость передачи мощности на входе.

Transmitter Fault (Сбой передатчика) - Указывает на то, что произошел сбой при передаче данных.

Loss of Signal (Потеря сигнала) - Указывает на потерю сигнала в кабеле.

Data Ready (Данные готовы) - На оптический трансивер подано питание, и данные готовы.

Отображение результатов диагностики оптического трансивера

1. Откройте страницу Оптический трансивер.
2. Нажмите кнопку **Show All** (Показать все).

Выполняется тест, и открывается страница **Optical Transceiver Diagnostics Table** (Таблица диагностики оптического трансивера).

Кроме поля на странице **Оптический трансивер** ,, на странице **Optical Transceiver Diagnostics Table (Таблица диагностики оптического трансивера)** имеется следующее поле:

Unit No (Номер блока). - Номер устройства, которому соответствует показанный кабель.

- **N/A (-)** - Отсутствует, N/S - не поддерживается, W - предупреждение, E - ошибка

ПРИМЕЧАНИЕ. Передатчики Finisar не поддерживают тестирование сбоев передатчиков при диагностике.

ПРИМЕЧАНИЕ. Функция тестирования оптоволоконных кабелей работает только для серверов SFP, которые поддерживают цифровую диагностику по стандарту SFF-872.

Команды консоли для выполнения тестирования оптоволоконного кабеля

В следующей таблице приведены команды для выполнения тестирования оптоволоконного кабеля.

Таблица 6-27. Команды страницы Optic Cable Test

Команды консоли	Описание
show fiber-ports optical- transceiver [*interface*] [*detailed*]	Отображение диагностики оптического трансивера.

Ниже 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/e1	48	5.15	50	1.789	1.789	No	No
1/e2	43	5.15	10	1.789	1.789	No	No

Управление защитой коммутатора

Страница **Management Security (Безопасность управления)** предоставляет доступ к страницам безопасности, которые содержат поля, позволяющие настроить параметры безопасности для портов, методов управления устройствами, пользователей и защиты сервера. Чтобы открыть страницу**Management Security (Безопасность управления)** , нажмите System (Система) →Management Security (Безопасность управления) в панели дерева.

Определение профилей доступа

Страница **Access Profiles**(Профили доступа) содержит поля, позволяющие определять профили и правила для доступа к устройству. Доступ к управлению для указанной группы пользователей может быть ограничен по входным портам, IP-адресу источника и маскам подсети.

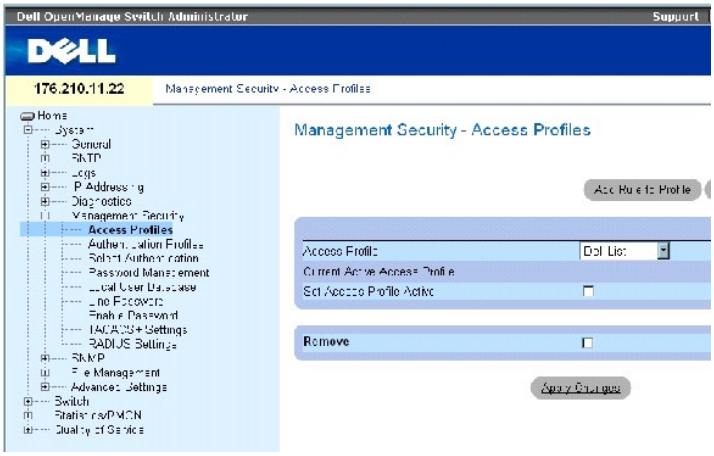
Методы доступа к управлению коммутатором могут быть определены для каждого метода, включая доступ к Интернету (HTTP), безопасный доступ к Интернету (HTTPS), Telnet, и безопасный доступ к Telnet.

Доступ к различным методам управления может варьироваться в зависимости от группы пользователей. Например, ползователи группы User Group 1 получают доступ к устройству только через протокол HTTPS, а пользователи User Group 2 - как через протокол HTTPS, так и через Telnet.

В списках Management Access Lists описаны до 256 правил, которые определяют, какие пользователи имеют право управлять устройством, и с использоваением каких методов. Пользователям также может быть запрещен доступ к устройству.

На странице **Access Profiles (Профили доступа)** имеются поля для конфигурации списков доступа к управлению, которые также позволяют применять их к конкретным интерфейсам. Чтобы открыть страницу **Access Profiles (Профили доступа)**нажмите **System (Система)** → **Management Security (Безопасность управления)** → **Access Profiles (Профили доступа)** в панели дерева.

Рисунок 6-38. Профили доступа



На странице **Access Profiles** (Профили доступа) есть следующие поля:

Access Profile (Профиль доступа) - Список пользовательских профилей доступа. Список Access Profile (Профиль доступа) содержим значение по умолчанию **Console Only (Только консоль)**. При выборе данного профиля доступа активное управление устройством выполняется только через консоль.

Current Active Access Profile - Текущий активный профиль доступа.

Set Access Profile Active - Активизирует выбранный профиль доступа.

Remove (Удалить) - Удаляет профиль доступа из списка **Access Profile Name (Имя профиля доступа)**.

Активация профиля

1. Откройте страницу **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

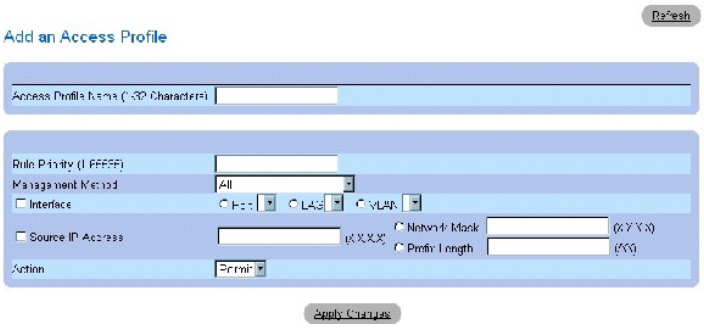
Правила служат фильтрами для определения приоритетов правил, метода управления устройством, типа интерфейса, IP-адреса источника и сетевой маски, а также действия при доступе для управления устройством. Доступ пользователей для управления может быть разрешен или заблокирован. Приоритет правил задает порядок применения правил профиля .

Определение правил для профиля доступа:

1. Откройте страницу **Access Profiles** (Профили доступа).
2. Нажмите кнопку **Add Profile (Добавить профиль).**

Откроется страница Add An Access Profile (Добавление профиля доступа).

Рисунок 6-39. Добавление профиля доступа



На странице Добавление профиля доступа есть следующие дополнительные поля:

Access Profile Name (1-32 Characters) (Имя профиля доступа, 1-32 символов) - Пользовательское имя профиля доступа). Имя профиля доступа может содержать не более 32 символов.

Rule Priority (1-65535) - Приоритет правила. При соответствии пакета определенному правилу, пользовательской группе может быть разрешен или запрещен доступ к управлению устройством. Порядок следования правил определяется в зависимости от установленного в этом поле значения приоритета правила. Номер правила важен для соотнесения пакетов определенному правилу, так как для пакетов применяется схема первого совпадения. Приоритеты правил можно просмотреть в таблице **Profile Rules Table (Таблица правил профиля)**.

Management Method - Метод управления, для которого определяется профиль доступа. Пользователям с данным профилем доступа отказывается или разрешается доступ к некоторым методам управления устройством.

Interface - Интерфейс, к которому применяется правило. Это поле является необязательным. Это правило можно применить к некоторым портам, LAG или VLAN, отметив соответствующее поле флажком и выбрав нужный переключатель и интерфейс.

ПРИМЕЧАНИЕ. Назначение профиля доступа к одному интерфейсу приводит к отказу при попытке доступа через другие интерфейсы. Если профиль доступа не назначен ни для одного интерфейса, доступ к устройству можно получить со всех интерфейсов.

Source IP Address (Исходный IP-адрес) (X.X.X.X) - Исходный IP-адрес интерфейса, к которому применяется правило. Это поле является необязательным и указывает на то, что правило действительно в подсети.

Network Mask (Маска сети) (X.X.X.X) - IP-адрес маски подсети.

Prefix Length (/XX) (Длина префикса) - Количество битов, составляющих исходный префикс IP-адреса, или маска сети исходного IP-адреса.

Action (Действие) - Определяет, разрешить или отказать в доступе к управлению определенным интерфейсом.

3. Определите поле **Access Profile Name** (Имя профиля доступа).
4. Определите соответствующие поля.
5. Нажмите кнопку **Apply Changes** (Применить изменения).

Новый интерфейс будет добавлен, а устройство обновлено.

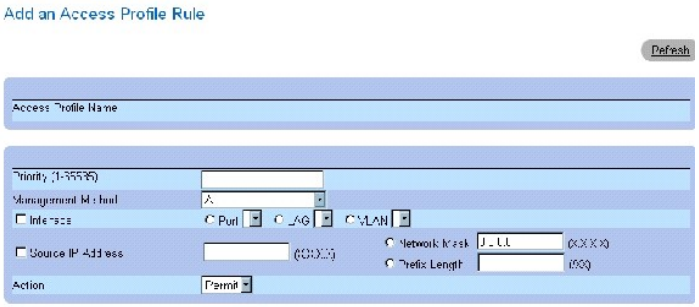
Добавление правил для профиля доступа

ПРИМЕЧАНИЕ. Первое правило нужно определить, чтобы начать соответствующий трафик для профилей доступа.

1. Откройте страницу **Access Profiles** (Профили доступа).
2. Нажмите кнопку **Add Rule to Profile** (Добавить правило для профиля).

Откроется страница **Add An Access Profile Rule** (Добавление правила профиля доступа).

Рисунок 6-40. Добавление правила профиля доступа



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

Правило будет добавлен в профиль доступа, а устройство обновлено.

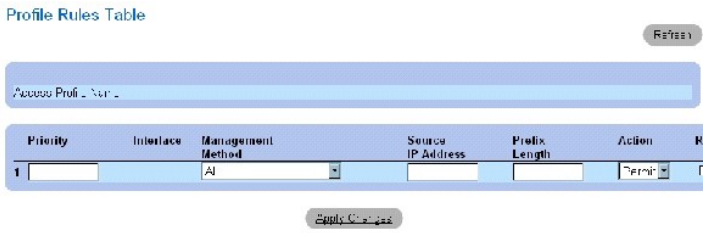
Просмотр таблицы правил профиля

ПРИМЕЧАНИЕ. Порядок, в котором правила отображаются в Profile Rules Table (Таблице правил профиля) важен. Пакеты сопоставляются первому правилу, которое отвечает критерию правила.

1. Откройте страницу **Профили доступа**.
2. Нажмите кнопку **Show All** (Показать все).

Откроется страница **Profile Rules Table (Таблица правил профиля)**.

Рисунок 6-41. Profile Rules Table (Таблица правил профиля)



Удаление правила

1. Откройте страницу **Access Profiles** (Профили доступа).
2. Нажмите кнопку **Show All** (Показать все).

Откроется страница **Profile Rules Table** (Таблица правил профиля).

3. Выберите правило.
4. Установите флажок в поле **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, соответствующие полям на странице Профили доступа.

Таблица 6-28. Команды страницы Access Profiles

Команды консоли	**Описание**
management access-list имя	Определяет список доступа для управления и вводит контекст списка доступа для конфигурации.
permit [ethernet interface-number | vlan vlan-id | port-channel number] [service service]	Задает разрешающие условия списка доступа для управления для порта.
permit ip-source ip-address [mask mask | prefix-length] [ethernet interface-number | vlan vlan-id | port-channel number] [service service]	Задает разрешающие условия списка доступа для управления для порта и выбранный метод управления.
deny [ethernet interface-number | vlan vlan-id | port-channel number] [service service]	Задает запрещающие условия списка доступа для управления для порта и выбранный метод управления.
deny ip-source ip-address [mask mask | prefix-length] [ethernet interface-number | vlan vlan-id | port-channel number] [service service]	Задает запрещающие условия списка доступа для управления для порта и выбранный метод управления.
management access-class {console-only | name}	Определяет, условия из какого списка доступа используются в качестве активных условий управления.
show management access-list [name]	Выводит активные списки доступа для управления.
show management access-class	Выводит сведения о классе доступа для управления.

Ниже 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 идентификации

На странице Профили идентификации имеются поля, позволяющие выбирать метод идентификации пользователя на устройстве. Идентификация пользователя происходит:

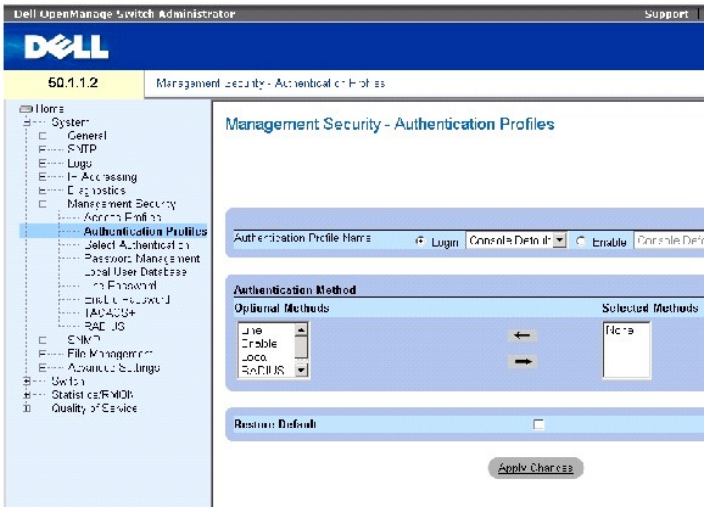
- Локально
- Через внешний сервер

Для идентификации пользователя также можно задать значение None (Нет).

Идентификация пользователя происходит в том порядке, в каком выбраны методы. Например, если выделены сразу и параметр Local (Локально), и параметр RADIUS, пользователи сначала идентифицируются локально. Если локальная пользовательская база данных пуста, то пользователь идентифицируется через сервер RADIUS. Если происходит сбой в процессе идентификации с использованием первого метода, процесс идентификации заканчивается.

Если при идентификации происходит ошибка, используется следующий выбранный метод. Чтобы открыть страницу Профили идентификации нажмите System (Система) → Management Security (Безопасность управления) → Authentication Profiles (Профили идентификации) в панели дерева.

Рисунок 6-42. Профили идентификации



На странице Профили идентификации есть следующие поля:

Authentication Profile Name (Имя профиля идентификации) - пользовательские списки профилей идентификации, к которым добавляются задаваемые пользователем профили. Значения по умолчанию: **Network Default (Сетевые значения по умолчанию)** и **Console Default (Консольные значения по умолчанию)**.

- Login (Вход) - Определяет заданный пользователем список профилей идентификации для входных паролей.
- Enable (Включить) - Определяет заданный пользователем список профилей идентификации для включения паролей.

Optional Methods (Необязательные методы) - Список пользовательских методов идентификации. Возможные значения:

None (Нет) - Указывает, что идентификация пользователя не проводится.

Local (Локально) - Идентификация пользователя проводится на уровне устройства. Для идентификации устройство проверяет имя пользователя и пароль.

RADIUS - Идентификация пользователя проводится на сервере RADIUS. Дополнительную информацию см. в разделе Настройка параметров RADIUS.

Line (Линия) - Указывает, что для идентификации используется пароль линии.

Enable (Включение) - Указывает, что для идентификации используется пароль включения.

TACACS+ - Идентификация пользователя проводится на сервере TACACS+.

Restore Default (Восстановить метод по умолчанию) - Восстанавливает метод идентификации пользователя на устройстве, заданный по умолчанию. Эта фунция доступна только для профиля по умолчанию.

Remove (Удалить) - Если отметить это поле флажком, выбранный профиль будет удален. Активные профили не могут быть удалены. Эта фунция доступна только для профилей, заданных пользователями.

Выбор профиля идентификации:

1. Откройте страницу **Профили идентификации**.
2. Выберите профиль в поле **Authentication Profile Name** (Имя профиля идентификации).
3. Выберите метод идентификации, используя значки со стрелками. Идентификация происходит в том порядке, в каком выбраны методы.
4. Нажмите кнопку Apply Changes (Применить изменения).

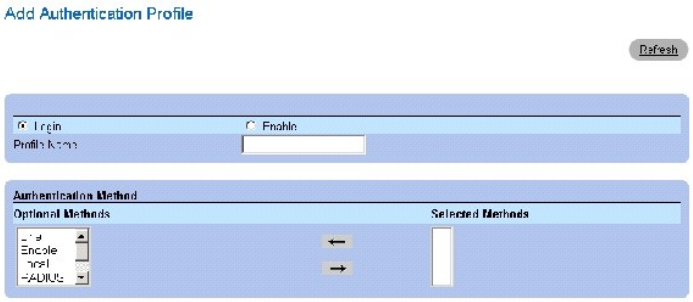
Профиль идентификации для этого устройства будет изменен.

Добавление профиля идентификации:

1. Откройте страницу **Профили идентификации**.
2. Нажмите кнопку Add (Добавить).

Откроется страница **Open the Authentication Profile** (Открыть профиль идентификации).

Рисунок 6-43. Добавьте профиль идентификации



3. Выполните конфигурацию профиля.

ПРИМЕЧАНИЕ. Имя нового профиля не должно содержать знаки пробела.

4. Нажмите кнопку Apply Changes (Применить изменения).

Профиль идентификации для этого устройства будет обновлен.

Вывод на экран таблицы профилей идентификации:

1. Откройте страницу **Профили идентификации**.
2. Нажмите кнопку **Show All** (Показать все).

Откроется страница **Authentication Profiles Table** (Таблицы профилей идентификации).

Удаление профиля идентификации:

1. Откройте страницу **Профили идентификации**.
2. Нажмите кнопку **Show All** (Показать все).

Откроется страница **Authentication Profiles Table** (Таблицы профилей идентификации).

3. Выберите профиль идентификации.
4. Установите флажок в поле **Remove** (Удалить).
5. Нажмите кнопку **Apply Changes** (Применить изменения).

Профиль идентификации будет удален.

Настройка профиля идентификации с помощью команд консоли

В следующей таблице приведены команды консоли, соответствующие полям на странице **Профили идентификации**.

Таблица 6-29. Команды страницы Authentication Profile

Команды консоли	Описание
aaa authentication login {default | list-name} method1 [method2.]	Настраивает идентификацию для входа в систему.
no aaa authentication login {default | list-name}	Удаляет профиль идентификации для входа в систему.

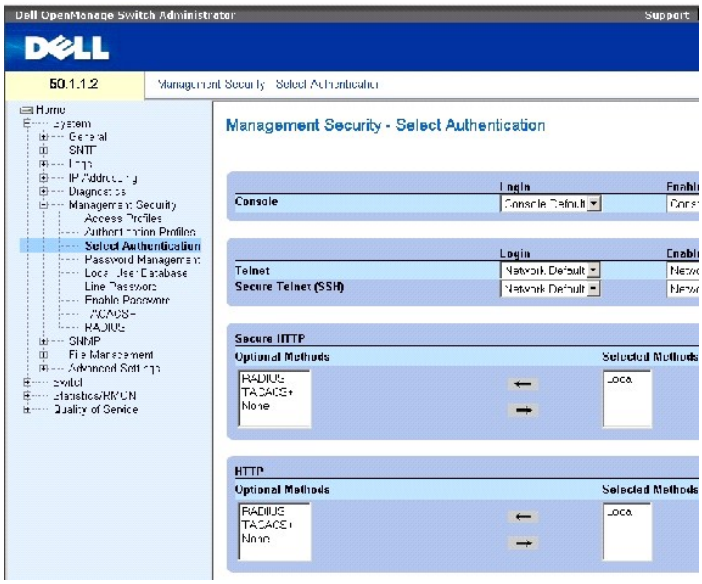
Ниже приведен пример команд консоли:

```
console(config)# aaa
authentication login
default radius local
enable none



console(config)# no aaa
authentication login
default
```

Выбор профилей идентификации

После того, как профили идентификации определены, их можно применить к методам доступа для управления. Например, пользователи консоли могут идентифицироваться по спискам методов идентификации 1, а пользователи Telnet - по спискам 2. Чтобы открыть страницу **Выбор идентификации** щелкните System (Система)→ Management Security (Безопасность управления)→ Select Authentication (Выбор идентификации) в панели дерева.

Рисунок 6-44. Выбор идентификации



На странице **Выбор идентификации** есть следующие поля:

Console (Консоль) - Отображает профили идентификации, используемые для идентификации пользователей консоли.

Login (Вход) - Отображает профили идентификации, используемые для регистрации пользователей, вошедших в интерфейс консоли.

Enable (Включен) - Определяет профили идентификации пользователей, включающих режим Privileged EXEC с консоли.

Telnet - Отображает профили идентификации, используемые для идентификации пользователей Telnet.

Secure Telnet (SSH) (Защищенная связь Telnet)- Профили идентификации, используемые для идентификации пользователей Secure Shell (SSH). Протокол Secure Shell (SSH) обеспечивает безопасную удаленную связь устройства с клиентом.

HTTP and **Secure HTTP (HTTP и защищенный HTTP)** - Метод идентификации доступа к протоколу HTTP и защищенному протоколу HTTP соответственно. Возможные значения поля:

None (Нет) - Для доступа не используется метод идентификации.

Local (Локальная) - Указывает, что идентификация происходит локально.

RADIUS - Идентификация пользователя проводится на сервере RADIUS.

TACACS+ - Идентификация пользователя проводится на сервере TACACS+.

Применение списка идентификаций к сеансам консоли

1. Откройте страницу **Выбор идентификации**.
2. Выберите профиль идентификации в поле **Console** (Консоль).
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Сеансам консоли будет назначен список идентификаций.

Применение списка идентификаций к сеансам Telnet

1. Откройте страницу **Выбор идентификации**.
2. Выберите профиль идентификации в поле **Telnet**.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Сеансам Telnet будет назначен список идентификаций.

Применение списка идентификаций к сеансам Secure Telnet (SSH)

1. Откройте страницу **Выбор идентификации**.
2. Выберите профиль идентификации в поле **Secure Telnet (SSH)**.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Сеансам Secure Telnet (SSH) будет назначен профиль идентификации.

Назначение сеансам HTTP последовательности идентификации

1. Откройте страницу **Выбор идентификации**.
2. Выберите последовательность идентификации в поле **HTTP**.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Сеансам HTTP будет назначена последовательность идентификаций.

Назначение сеансам защищенного HTTP последовательности идентификации

1. Откройте страницу **Выбор идентификации**.
2. Выберите последовательность идентификации в поле **Secure HTTP**.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Сеансам Secure HTTP будет назначена последовательность идентификаций.

Назначение профилей или последовательностей идентификаций доступа с помощью команд консоли

В следующей таблице приведены команды консоли, соответствующие полям на странице **Выбор идентификации**.

Таблица 6-30. Команды страницы Select Authentication

Команды консоли	Описание
enable authentication [default | list-name]	Указывает список методов идентификации при доступе на уровень с более высокими привилегиями с удаленного подключения Telnet, консоли или SSH.
login authentication [default | list-name]	Указывает список методов идентификации для входа в систему с удаленного подключения Telnet, консоли или SSH.
ip http authentication method1 [method2.]	Указывает методы идентификации для серверов HTTP.
ip https authentication method1 [method2.]	Указывает методы идентификации для серверов HTTPS.
show authentication methods	Выводит сведения о методах идентификации.

Ниже 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	Default	Default
Telnet	Default	Default
SSH	Default	Default

http	: Local	
https	: Local	
dot1x	:	

Управление паролями

Управление с помощью паролей гарантирует повышенный уровень защиты в сети. Пароли для доступа к SSH, Telnet, HTTP, HTTPS и SNMP являются назначенными функциями защиты, включающими:

- Определение минимального количества символов в пароле
- Дата окончания действия пароля
- Предотвращение частого использования одного и того же пароля
- Запрещение повторного ввода пароля в случае нескольких неудачных попыток

Срок действия пароля начинает действовать сразу же после его активации. Срок действия пароля задается пользователем и включает дату и время, до которой пароль является действительным. За десять дней до истечения срока действия пароля в устройстве выдается соответствующее предупреждение.

После истечения срока действия пароля пользователь имеет право войти в систему еще три раза. При каждом из этих трех раз выдается соответствующее предупреждение и предложение изменить пароль. Если пароль не изменен, пользователи могут войти в систему только через консоль. Предупреждения о смене пароля заносятся в файл системного журнала.

При изменении уровня привилегии необходимо также переопределить пользователя. Тем не менее, срок действия пароля заканчивается в соответствии с исходной заданной датой.

Чтобы открыть страницу **Управление паролями** нажмите System (Система) → Management Securit (Безопасность управления) → Password Management (Управление паролями) в панели дерева.

Рисунок 6-45. Управление паролями

На странице **Управление паролями** есть следующие поля:

Password Minimum Length (8-64) (Минимальное количество символов в пароле) - Если это поле отмечено флажком, оно указывает минимальную длину пароля. Например, администратор может задать минимальную длину паролей, равную 10 символам.

Consecutive Passwords Before Re-use (Последовательное повторное использование паролей) - Указывает, сколько раз необходимо изменить пароль перед тем, как использовать его повторно. Возможные значения поля: 1-10**.**

ПРИМЕЧАНИЕ. Перед тем, как срок действия пароля истекает, пользователь получает извещение о необходимости его изменить. Но это сообщение не выводится на экран для веб-пользоваетелей.

Enable Login Attempts (Попытки входа в систему) - Если это поле отмечено, оно позволяет отказать пользователю во входе в систему после нескольких попыток ввести недействительный пароль. Например, если в поле задано число 5, и пользователь вводит неправильный пароль пять раз, шестая попытка входа в систему блокируется. Возможные значения поля: 1-5.

Определение управления паролями

1. Откройте страницу **Управление паролями**.
2. Определите поля.
3. Нажмите кнопку Apply Changes (Применить изменения).

Управление паролями определено, а устройство обновлено.

Команды консоли для управления паролями

В следующей таблице приведены команды консоли, соответствующие полям на странице **Управление паролями**.

Таблица 6-31. Команды консоли для управления паролями

Команды консоли	Описание
password min-length *длина*	Определяет минимальную длину пароля
password history число	Указывает, сколько раз необходимо изменить пароль перед тем, как использовать его повторно.
password lock-out *число*	Определяет после скольки попыток ввода неправильного пароля происходит блокировка устройства.
show password configuration	Информация об управлении паролями

Ниже приведен пример команд консоли:

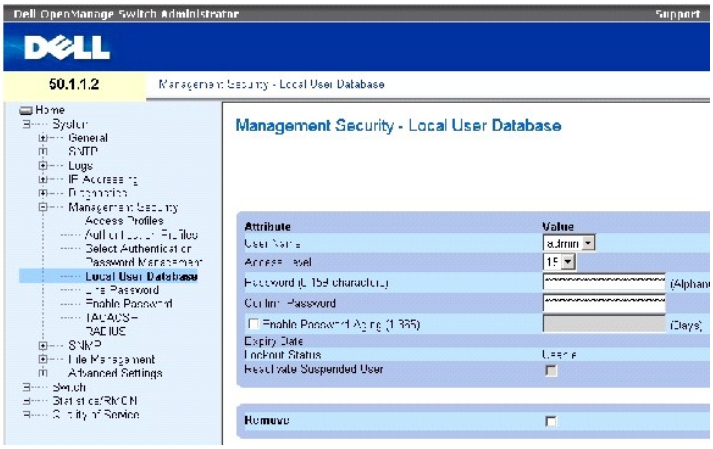
```
console # show passwords configuration

Minimal length: 0

History: Disabled

History hold time: no limit

Lockout control: disabled

Enable Passwords
```

Level	Password Aging	Password Expiry date	Lockout	
-----	--------	----------	-------	
1	-	-	-	
15	-	-	-	
Line Passwords				
Line	Password Aging	Password Expiry date	Lockout	
-------	--------	----------	-------	
Telnet	-	-	-	
SSH	-	-	-	
Console	-	-	-	
console # **show users accounts**				
Username	Privilege	Password Aging	Password Expiry Date	Lockout
--------	---------	--------	----------	-------
nim	15	39	18-Feb-2005	

Определение локальных пользовательских баз данных

На странице **Локальная пользовательская база данных** содержатся поля для определения пользователей, паролей и уровней доступа. Чтобы открыть страницу **Локальная пользовательская база данных** , нажмите System (Система) → Management Security (Безопасность управления) → Local User Databas (локальных пользовательских баз данных) в панели дерева.

Рисунок 6-46. Локальная пользовательская база данных



На странице **Локальная пользовательская база данных** есть следующие поля:

User Name (Имя пользователя) - Список пользователей.

Access Level (Уровень доступа) - Определяет уровень доступа пользователя. Самый низкий уровень доступа - **1**, а **15** - самый высокий. Пользователи с уровнем доступа 15 называются Privileged Users (Привилегированные пользователи), и только они имеют право доступа к программе OpenManage Switch Administrator.

Password (Пароль) (от 0 до 159 символов)- Определенный пользователем пароль.

Confirm Password (Подтвердите пароль). Подтверждение определенного пользователем пароля.

Enable Password Aging (1-365) (Включить срок использования пароля) - Указывает, через сколько дней закончится срок действия пароля.

Expiry Date (Срок действия) - Указывает дату истечения срока действия пароля, заданного пользователем.

Lockout Status (Состояние блокировки) - Указывает количество неудачных попыток идентификации со времени последнего успешного входа пользователя в систему, если отмечено флажком поле **Enable Login Attempts (Попытки входа в систему)** на странице **Управление паролями**. Выдает **LOCKOUT**, когда регистрация пользователя заблокирована.

Reactivate Suspended User (Восстановить заблокированного пользователя) - Восстановление прав доступа для пользователя, регистрационная запись которого была заблокирована. Отказ в правах доступа может произойти вследствие нескольких неудачных попыток входа в систему.

Remove (Удалить) - Удаляет пользователей из списка **User Name** (Имя пользователя).

Назначение прав доступа пользователю

1. Откройте страницу **Локальная пользовательская база данных**.
2. Выберите пользователя в поле **User Name** (Имя пользователя).
3. Определите поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

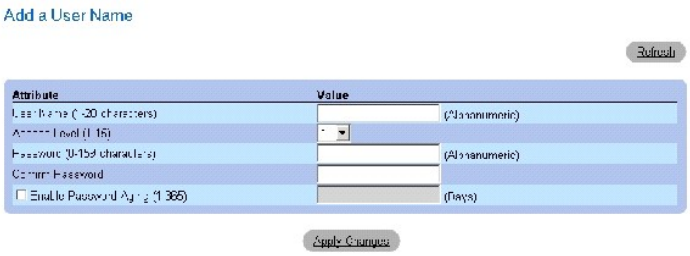
Права доступа пользователя и пароли будут определены, а устройство обновлено.

Определение нового пользователя:

1. Откройте страницу **Локальная пользовательская база данных**.
2. Нажмите кнопку **Add** (Добавить).

Откроется страница **Add User** (Добавить пользователя):

Рисунок 6-47. Добавьте пользователя



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

Новый пользователь будет добавлен, а устройство обновлено.

Вывод таблицы локальных пользователей :

1. Откройте страницу **Локальная пользовательская база данных**.
2. Нажмите кнопку **Show All** (Показать все).

Откроется страница Local User Table (Таблица локальных пользователей).

Рисунок 6-48. Таблица локальных пользователей

Восстановление прав заблокированного пользователя:

1. Откройте страницу **Локальная пользовательская база данных**.
2. Нажмите кнопку **Show All** (Показать все).

Откроется страница Local User Table (Таблица локальных пользователей).

3. Выберите **User Name** (Имя пользователя).
4. Установите флажок в поле **Reactivate Suspended User (Восстановить заблокированного пользователя)**
5. Нажмите кнопку **Apply Changes** (Применить изменения).

Права доступа пользователя будут восстановлены, а устройство обновлено.

Удаление пользователей:

1. Откройте страницу **Локальная пользовательская база данных**.
2. Нажмите кнопку **Show All (Показать все).**

   Откроется страница **Таблица локальных пользователей**.
3. Выберите **User Name** (Имя пользователя).
4. Установите флажок в поле **Remove** (Удалить).
5. Нажмите кнопку **Apply Changes** (Применить изменения).

   Пользователь будет удален, а устройство обновлено.

Назначение пользователей с помощью команд консоли

В следующей таблице приведены команды консоли, соответствующие полям на странице **Локальная пользовательская база данных**.

Таблица 6-32. Команды страницы Local User Database

Команды консоли	Описание
username name [password password] [level level] [encrypted]	Устанавливает идентификацию по имени пользователя
set username name active	Восстанавливает права доступа для «заблокированного» пользователя.

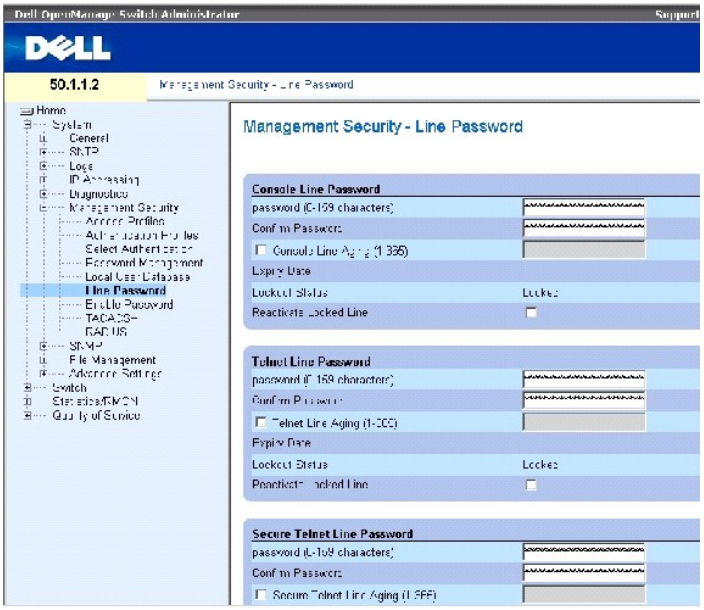
Ниже приведен пример команд консоли:

```
console(config)# username
bob password lee level 15


console# set username bob
active
```

Определение паролей линий

На странице Line Passwords (Пароли на линиях) имеются поля для определения паролей линий для методов управления. Чтобы открыть страницу Line Passwords (Пароли на линиях) , нажмите System (Система) → Management Security (Безопасность управления) →Line Passwords (Пароли линии) в панели дерева.

Рисунок 6-49. Line Passwords (Пароли на линиях)



На странице Line Passwords (Пароли на линиях) есть следующие поля:

Line Password for Console / Telnet / Secure Telnet - Пароль линии для доступа к устройству через сеанс консоли, Telnet или Secure Telnet.

Confirm Password for Console / Telnet / Secure Telnet - Подтверждение нового пароля линии. Пароль отображается в формате *****.

Line Aging (1-365) for Console / Telnet / Secure Telnet - Указывает, через сколько дней закончится срок действия пароля линии.

Expiry Date for Console / Telnet / Secure Telnet - Указывает дату истечения срока действия пароля линии.

Lockout Status for Console / Telnet / Secure Telnet (Состояние блокировки) - Указывает количество неудачных попыток идентификации со времени последнего успешного входа пользователя в систему, если отмечено флажком поле **Enable Login Attempts (Попытки входа в систему)** на странице **Управление паролями**. Выдает **LOCKOUT**, когда регистрация пользователя заблокирована.

Reactivate Locked Line for Console / Telnet / Secure Telnet - Восстанавливает активацию пароля линии для сеанса консоли/Telnet/Secure Telnet. Отказ в правах доступа может произойти вследствие нескольких неудачных попыток входа в систему.

Определение паролей линий для сеансов консоли:

1. Откройте страницу **Line Passwords (Пароли на линиях)**.
2. Определите поле **Line Password for Console** (Пароль линии для консоли).
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Пароль линии для сеансов консоли будет определен, а устройство обновлено.

Определение паролей линий для сеансов Telnet:

1. Откройте страницу **Line Passwords (Пароли на линиях)**.
2. Определите поле Telnet Line Password (Пароль линии Telnet).
3. Нажмите кнопку Apply Changes (Применить изменения).

Пароль линии для сеансов Telnet будет определен, а устройство обновлено.

Определение паролей линий для сеансов Secure Telnet :

1. Откройте страницу **Line Passwords (Пароли на линиях)**.
2. Определите поле **Secure Telnet Line Password** (Пароль линии Secure Telnet).
3. Нажмите кнопку Apply Changes (Применить изменения).

Пароль линии для сеансов Secure Telnet будет определен, а устройство обновлено.

Назначение паролей линий с помощью команд консоли

В следующей таблице приведены команды консоли, соответствующие полям на странице **Line Passwords (Пароли на линиях)**.

Таблица 6-33. Команды страницы Line Password

Команды консоли	Описание
password password [encrypted]	Указывает пароль линии.

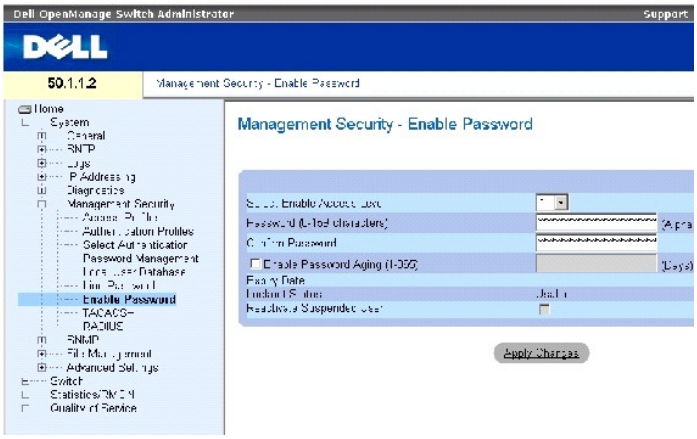
Ниже приведен пример команд консоли:

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

Определение пароля включения

На странице**Enable Passwords (Включение паролей)** задается локальный пароль для управления доступом на уровень Normal и Privilege. Чтобы открыть страницу локальный пароль **Enable Passwords (Включение паролей)** , нажмите System (Система) → Management Security (Безопасность управления) → Enable Passwords (Включение паролей) в панели дерева.

Рисунок 6-50. Enable Passwords (Включение паролей)



На странице **Enable Passwords (Включение паролей)** есть следующие поля:

Select Enable Access Level - Уровень доступа, связанный с паролем включения. Возможные значения поля: 1-15.

Password (Пароль) (от 0 до 159 символов)- Определенный пользователем пароль.

Confirm Password (Подтвердите пароль). Подтверждение определенного пользователем пароля. Пароль отображается в формате *****.

Enable Password Aging (1-365) (Включить срок использования пароля) - Указывает, через сколько дней закончится срок действия пароля.

Expiry Date (Срок действия) - Указывает дату истечения срока действия пароля, заданного пользователем.

Lockout Status (Состояние блокировки) - Указывает количество неудачных попыток идентификации со времени последнего успешного входа пользователя в систему, если отмечено флажком поле **Enable Login Attempts (Попытки входа в систему)** на странице **Управление паролями**. Выдает **LOCKOUT**, когда регистрация пользователя заблокирована.

Reactivate Suspended User (Восстановить заблокированного пользователя) - Восстановление прав доступа для пользователя, регистрационная запись которого была заблокирована. Отказ в правах доступа может произойти вследствие нескольких неудачных попыток входа в систему.

Определение нового пароля включения:

1. Откройте страницу **Enable Passwords (Включение паролей)**.
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 команды консоли, соответствующие полям на странице **Enable Passwords (Включение паролей)**.

Таблица 6-34. Команды консоли для изменения и включения пароля

Команды консоли	Описание
enable password [level level] password [encrypted]	Задает локальный пароль для управления доступом для уровней пользователей и полномочий.

Ниже приведен пример команд консоли:

```
console(config)# enable
password level 15 secret
```

Определение параметров TACACS+

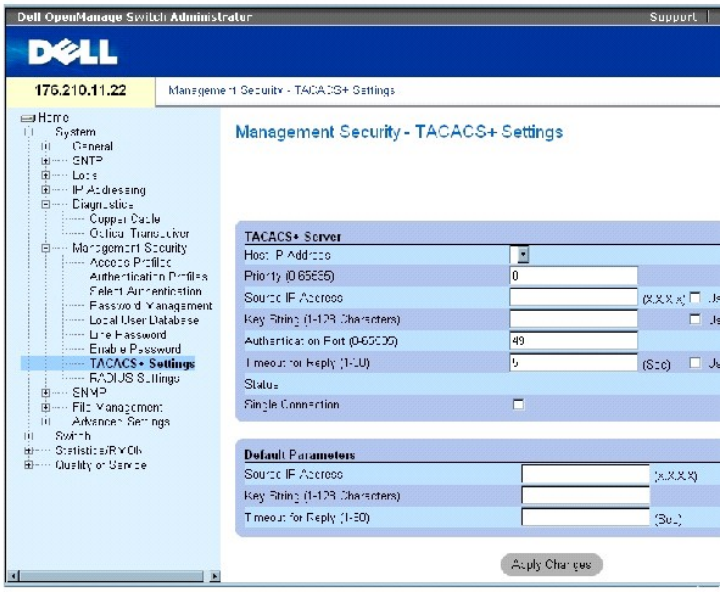
Коммутаторы обеспечивают поддержку клиента Terminal Access Controller Access Control System (TACACS+). TACACS+ предоставляет централизованную защиту при проверке пользователя, пытающегося получить доступ к устройству.

TACACS+ предоставляет централизованную систему управления, обеспечивая согласованность с сервером RADIUS и другими процедурами идентификации. TACACS+ предлагает следующие службы:

- Authentication (Идентификация) - Выполняет идентификацию на входе на основании имени пользователя и паролей.
- Authorization (Авторизация)- Выполняется на входе. Как только заканчивается сеанс идентификации, начинается процесс авторизации с использованием идентифицированного имени пользователя. На сервере TACACS+ выполняется проверка прав доступа пользователя.

Протокол TACACS+ гарантирует целостность сети благодаря шифрованию данных, передаваемых с устройства на сервер TACACS+ и обратно. Чтобы открыть страницу **Параметры TACACS+**, нажмите **System (Система)** → **Management Security (Безопасность управления)** →**TACACS+** в панели дерева.

Рисунок 6-51. Параметры TACACS+



На странице **Параметры TACACS+** есть следующие поля:

Host IP Address (IP-адрес хоста) - Указывает IP-адрес сервера TACACS+.

Priority (0-65535) (Приоритет) - Указывает в какой последовательности используются серверы TACACS+. Значение по умолчанию - 0.

Source IP Address (Исходный IP-адрес) - Исходный IP-адрес устройства, который используется для сеанса TACACS+ при обмене данными между устройством и сервером TACACS+.

Key String (0-128 Characters) (Ключ шифрования, 0-128 бит)- Определяет ключ идентификации и шифрования для связи между устройством и сервером TACACS+. Этот ключ должен соответствовать ключу шифрования на сервере TACACS+. Этот ключ закодирован.

Authentication Port (0-65535) (Порт идентификации)- Номер порта, через который протекает сеанс TACACS+. Значение по умолчанию - 49.

Timeout for Reply (1-30) (Время на ответ) - время, в течение которого устройство ожидает ответа от сервера TACACS+. Значение поля: 1-30 секунд.

Status (Состояние) - Состояние связи между устройством и сервером TACACS+. Возможные значения поля:

Connected (Подключен) - Текущее состояние связи между устройством и сервером TACACS+.

Not Connected (Не подключен) - Временно связь между устройством и сервером TACACS+ отсутствует.

Single Connection (одно подключение) - Поддерживает одно открытое соединение между устройством и сервером TACACS+

Параметры по умолчанию для сервера TACACS+ задаются пользователем. Параметры по умолчанию применяются к вновь определенным серверам TACACS+. Если параметры по умолчанию не заданы, к новым серверам TACACS+ применяются системные значения параметров по умолчанию.

Далее перечислены параметры TACACS+ по умолчанию:

Source IP Address (Исходный IP-адрес) - Исходный IP-адрес устройства по умолчанию, который используется для сеанса TACACS+ при обмене данными между устройством и сервером TACACS+. Исходный IP-адрес по умолчанию: 0.0.0.0.

Key String (0-128 Characters) (Ключ шифрования, 0-128 бит) - Строка ключа по умолчанию, используемая для идентификации и кодирования всех связей между устройством и сервером TACACS+. Этот ключ закодирован.

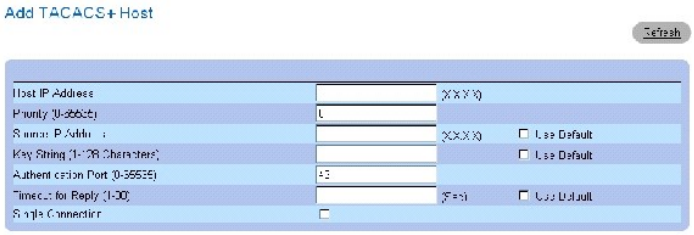
Timeout for Reply (1-30) (Время на ответ) - Время по умолчанию, в течение которого устройство ожидает ответа от сервера TACACS+. Значение по умолчанию: 5 секунд.

Добавление сервера TACACS+

1. Откройте страницу **Параметры TACACS+**.
2. Нажмите кнопку Add (Добавить).

Откроется страница **Add TACACS+ Host (Добавить хост TACACS+)** :

Рисунок 6-52. Add TACACS+ Host (Добавить хост TACACS+)



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

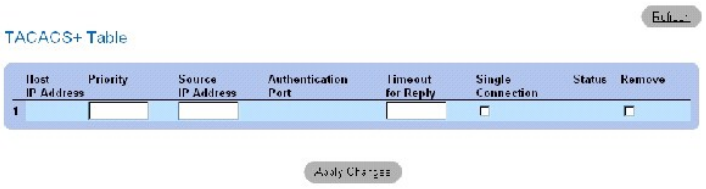
Сервер TACACS+ добавлен, а устройство обновлено.

Отображение таблицы Таблица TACACS+

1. Откройте страницу **Параметры TACACS+**.
2. Нажмите кнопку Show All (Показать все).

Откроется страница **Таблица TACACS+**.

Рисунок 6-53. Таблица TACACS+



Удаление сервера TACACS+

1. Откройте страницу **Таблица TACACS+**.
2. Нажмите кнопку Show All (Показать все).

   Откроется страница **Таблица TACACS+**.
3. Выберите запись **Таблица TACACS+**.
4. Установите флажок в поле **Remove** (Удалить).
5. Нажмите кнопку Apply Changes (Применить изменения).

   Сервер TACACS+ удален, а устройство обновлено.

Определение параметров TACACS+ с помощью командной строки

В следующей таблице приведены команды консоли, соответствующие полям на странице **Параметры TACACS+**.

Таблица 6-35. Команды TACACS+

Команды консоли	Описание
tacacs-server host {*ip-address* | *hostname*} [**single-connection**] [**port** *port-number*] [**timeout** *timeout*] [**key** *key-string*] [**source** *source*] [**priority** *priority*]	Указывает хост TACACS+
tacacs-server key key-string	Задает идентификацию и ключ кодирования для всех связей TACACS+ между устройством и сервером TACACS+. Этот ключ должен соответствовать ключу шифрования на сервере TACACS+. (Длина: 0 - 128 битов.)
tacacs-server timeout timeout	Указывает значение паузы в секундах. (Значение: 1 - 30.)
tacacs-server source-ip source	Указывает исходный IP-адрес. (Значение: Действительный IP-адрес.)
show tacacs [*ip-address*]	Отображение конфигурации и статистики для сервера TACACS+.

Ниже приведен пример команд консоли:

```
console# show tacacs

Device Configuration

IP address    Status    Port  Single Connection  TimeOut  Source IP  Priority
------------  --------  ----  -----------------  -------  ---------  --------
12.1.1.2      Not       49    Yes                1        12.1.1.1   1
```

	Connected					
Global values						

TimeOut : 5						
Device Configuration ----------						
Source IP : 0.0.0.0						
console#						

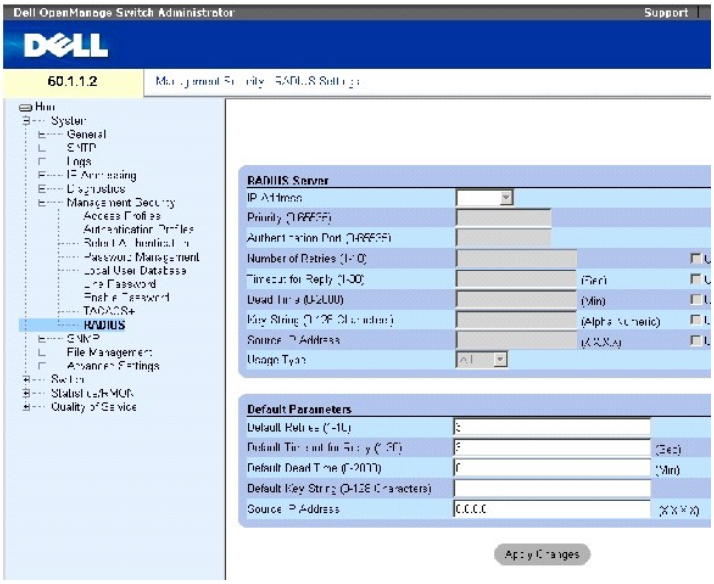
Настройка параметров RADIUS

Серверы RADIUS (Remote Authorization Dial-In User Service) обеспечивают дополнительную защиту сетей. Можно задать до четырех серверов RADIUS. Они обеспечивают централизованный метод идентификации:

- для доступа по Telnet;
- для доступа к защищенной оболочке Secure Shell;
- для доступа по Интернету;
- для доступа с консоли

Чтобы открыть страницу Параметры RADIUS , нажмите System (Система) → Management Security (Безопасность управления) → RADIUS в панели дерева.

Рисунок 6-54. Параметры RADIUS



На странице Параметры RADIUS есть следующие поля:

IP Address - Список IP-адресов сервера идентификации.

Priority (0-65535) - Приоритет сервера. Возможные значения: от 0 до 65535, где 0 - наибольшее значение. Используется для настройки порядка, в котором серверы выстраиваются в очередь.

Authentication Port - Порт идентификации. Порт идентификации используется для подтверждения идентификации сервера RADIUS.

Number of Retries (1-10) - Число запросов, отправляемых серверу RADIUS прежде, чем происходит ошибка. Возможные значения поля: 1-10.

Timeout for Reply (1-30) (Время на ответ) - Время в секундах, в течение которого устройство ожидает ответа от сервера RADIUS перед повторной попыткой или переключением на следующий сервер. Возможные значения поля: 1-30.

Dead Time (0-2000) (Последний срок) - Время в секундах, в течение которого запросы не принимают во внимание сервер RADIUS. Диапазон значений: от 0 до 2000.

Key String (1-128 Characters) - Строка ключа, используемая для идентификации и кодирования всех связей RADIUS между устройством и сервером RADIUS. Этот ключ закодирован.

Source IP Address - Исходный IP-адрес, используемый для связи с серверами RADIUS.

Usage Type - Указывает тип использования сервера. Им может быть одно из значений: login, 802.1x или all. Если значение не указано, по умолчанию используется значение all.

Следующие поля задают значения по умолчанию для RADIUS:

ПРИМЕЧАНИЕ. Если значения Timeouts (Паузы), Retries (Повтор) или Dead time (Последний срок) не указаны, к каждому хосту применяются общие значения (по умолчанию).

Default Retries (1-10) (Число повторных попыток по умолчанию) - Число запросов, отправляемых серверу RADIUS прежде, чем происходит ошибка.

Default Timeout for Reply (1-30) (Время на ответ по умолчанию) - Время (в секундах), в течение которого устройство ожидает ответа от сервера RADIUS. Значение по умолчанию: 5 секунд.

Default Dead time (0-2000) (Последний срок) - Время в секундах по умолчанию, в течение которого запросы не принимают во внимание сервер RADIUS. Диапазон значений: от 0 до 2000.

Default Key String (1-128 Characters) - Строка ключа по умолчанию (1-16 символов), используемая для идентификации и кодирования всех связей RADIUS между устройством и сервером RADIUS. Этот ключ закодирован.

Source IP Address - Исходный IP-адрес, используемый для связи с серверами RADIUS. Исходный IP-адрес по умолчанию: 0.0.0.0.

Определение параметров RADIUS:

1. Откройте страницу 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 Параметры RADIUS.
2. Нажмите кнопку Add (Добавить).

Откроется страница **Add RADIUS Server** (Добавить сервер RADIUS):

Рисунок 6-55. Add RADIUS Server (Добавление сервера RADIUS)

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

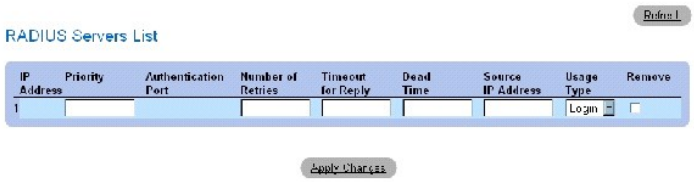
Новый сервер RADIUS будет добавлен, а устройство обновлено.

Вывод списка серверов RADIUS:

1. Откройте страницу Параметры RADIUS.
2. Нажмите кнопку **Show All** (Показать все).

Откроется страница Список серверов RADIUS.

Рисунок 6-56. Список серверов RADIUS



Удаление сервера RADIUS

1. Откройте страницу Параметры RADIUS.
2. Нажмите кнопку Show All (Показать все).

   Откроется страница Список серверов RADIUS.
3. Выберите запись Список серверов RADIUS.
4. Установите флажок в поле **Remove** (Удалить).
5. Нажмите кнопку Apply Changes (Применить изменения).

   Сервер RADIUS удален, а устройство обновлено.

Определение серверов RADIUS с помощью команд консоли

В следующей таблице приведены команды консоли, соответствующие полям на странице **Параметры RADIUS**.

Таблица 6-36. Команды для сервера RADIUS

Команды консоли	Описание
radius-server timeout *timeout*	Задает промежуток времени для каждого устройства, в течение которого маршрутизатор ожидает ответа сервера.
radius-server retransmit *retries*	Определяет, сколько раз программа обращается к списку хостов с серверами RADIUS.
radius-server deadtime êîëè÷åñòâî_ñåêóíä	Настраивает недоступные серверы так, чтобы они пропускались.
radius-server key *key-string*	Задает идентификацию и ключ кодирования для всех связей RADIUS между маршрутизатором и окружением RADIUS.
radius-server host *ip-address* [**auth-port** *auth-port-number*] [**timeout** timeout] [**retransmit** *retries*] [**deadtime** *deadtime*] [**key** *key-string*] [**source** *source*] [**priority** *priority*]	Задает хост сервера RADIUS.
show radius-servers	Выводит параметры сервера RADIUS.

Ниже приведен пример команд консоли:

```
Console(config)# radius-
server timeout 5


Console(config)# radius-
```

```
server retransmit 5



Console(config)# radius-
server deadtime 10



Console(config)# radius-
server key 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
```

Определение параметров SNMP

Протокол SNMP (Simple Network Management Protocol) обеспечивает способ управления устройствами в сети. Коммутатор поддерживает следующие версии SNMP:

- SNMPv1 (версия 1)
- SNMPv2 (версия 2)
- SNMPv3 (версия 3)

SNMP v1 и v2

Агенты SNMP поддерживают 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 v3

SNMP v3 также применяет управление доступом и новый механизм прерываний для SNMPv1 и SNMPv2 PDU. Кроме того, для SNMPv3 определяется модель User Security Model (USM), которая включает:

- **Authentication (Идентификация)** - Обеспечивает целостность данных и ндентификацию исходных данных.
- **Privacy (Неприкосновенность)** - Защита содержимого сообщения от несанкционированного доступа. Cipher Block-Chaining (CBC) используется

для шифрования. На сервере SNMP включена либо только идентификация, либо идентификация и неприкосновенность. Функцию неприкосновенности нельзя включить при выключенной функции идентификации.

- **Timeliness (Своевременность)** - Защита от задержек сообщений илиих избыточного резервирования. Агент SNMP сравнивает входящее сообщение с его информацией о времени.
- **Key Management (Управление ключами)** - Определяет создание, обновление и использование ключей.

Коммутатор поддерживает фильтры уведомлений SNMP, основанные на Object IDs (OID). Фильтры OID используются в системе для управления функциями коммутатора. SNMP v3 поддерживает следующие функции:

- Защита
- Управление доступом к функциям
- Системные прерывания

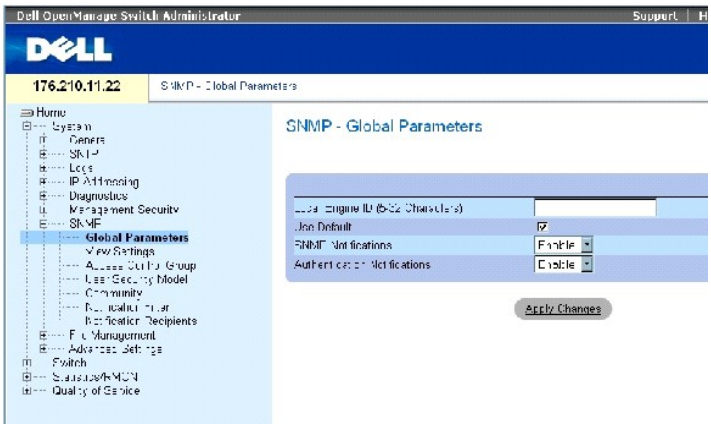
Идентификация или Privacy Keys (ключи секретности) модифицируются в модели User Security Model (USM) (Модель защиты пользователя).

SNMPv3 можно включить при включенной функции Local Engine ID (локальная идентификация).

Определение общих параметров SNMP

На странице **Общие параметры SNMP** можно включить как извещения SNMP, так и извещения идентификации. Чтобы открыть страницу **Общие параметры SNMP**, выберите System (Система) → SNMP → Global Parameters (Глобальные параметры) на панели дерева.

Рисунок 6-57. Общие параметры SNMP



На странице **Общие параметры SNMP** есть следующие поля:

Local Engine ID (Локальный идентификатор механизма) - Указывает локальный идентификатор механизма коммутатора. Значение поля представлено в шестнадцатиричной системе. Каждый байт символа шестнадцатиричной строки представлен двумя шестнадцатиричными числами. Знак разделителя байтов - точка или двоеточие. Идентификатор механизма необходимо задать перед включением SNMPv3.

Для коммутаторов, работающих в автономном режиме, выберите идентификатор Engine ID по умолчанию, который состоит из номера производителя (Enterprise number) и MAC-адреса по умолчанию.

Для стековых систем настройте идентификатор Engine ID и убедитесь, что домену администратора присвоен уникальный идентификатор. Это предотвращает наличие в сети двух разных устройств с одинаковым идентификатором.

Use Defaults (Использовать значения по умолчанию) - Использует идентификатор, созданный устройством. По умолчанию значение идентификатора Engine ID имеет в своей основе MAC-адрес устройства и определяется в соответствии со следующими стандартами:

Первые 4 байта - первый бит = 1, остальные представляют собой номер производителя IANA = 674.

Пятый байт - Задано значение 3, чтобы указать, что далее следует MAC-адрес.

Последние 6 байтов - MAC-адрес устройства.

SNMP Notifications (Уведомления SNMP)- Включает или выключает маршрутизатор, отправляющий уведомления SNMP.

Authentication Notifications (Уведомления идентификации)- Включает или выключает маршрутизатор, отправляющий прерывания SNMP при сбое идентификации.

Включение уведомлений SNMP

1. Откройте страницу **Общие параметры SNMP**.
2. Выберите значение **Enable** в поле **SNMP Notifications**.
3. Нажмите кнопку Apply Changes (Применить изменения).

Уведомления SNMP включены, а устройство обновлено.

Включение уведомлений идентификации

1. Откройте страницу **Общие параметры SNMP**.
2. Выберите значение **Enable** в поле **Authentication Notifications**.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Включение уведомлений SNMP в режиме командной строки

В следующей таблице приведены команды консоли, соответствующие полям на странице SNMP Global Parameters (Общие параметры SNMP).

Таблица 6-37. Команды идентификации SNMP

Команды консоли	Описание
snmp-server enable traps	Включает маршрутизатор для отправки прерываний протокола SNMP
snmp-server trap authentication	Включает маршрутизатор для отправки прерываний протокола SNMP в случае сбоя идентификации
show snmp	Выводит состояние передач по протоколу SNMP.
snmp-server engine ID local {*engineid-string* | **default**}	Указывает локальный идентификатор механизма. Значение поля представлено в шестнадцатиричной системе. Каждый байт символа шестнадцатиричной строки представлен двумя шестнадцатиричными числами. Знак разделителя байтов - точка или двоеточие. Идентификатор механизма необходимо задать перед включением SNMPv3.

Ниже 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 страницы SNMP View

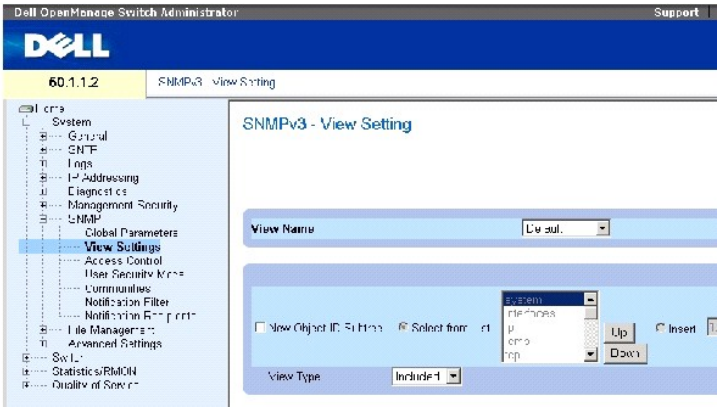
Со страницы SNMP Views предоставляется доступ к функциям устройства или их аспектам. Например, можно задать вид, который указывает, что SNMP group A имеет доступ только для чтения многоадресной группы, а SNMP group B - доступ для чтения и записи. Доступ к функциям предоставляется по имени MIB или MIB Object ID (идентификатор объекта MIB).

Стрелки вверх и вниз позволяют перемещаться по дереву MIB и его ветвям.

Чтобы открыть страницу **Страница SNMPv3 View Settings**, выберите **System (Система)** → **SNMP** → **View Settings (Параметры вида)** на панели

дерева.

Рисунок 6-58. Страница SNMPv3 View Settings



На странице **Страница SNMPv3 View Settings** есть следующие поля:

View Name (Имя вида) - Список пользовательских видов. Имя вида может содержать максимум 30 буквенных символов.

New Object ID Subtree (Новое поддерево OID) - Указывает функцию устройства OID, включенную или выключенную из выбранного вида SNMP.

Selected from List (Выбран из списка) - Выбор функции устройства OID с использованием клавиш **Up (Вверх)** и **Down (Вниз)** для навигации по списку всех OID устройства.

Insert (Вставить)- Указывает идентификатор функции устройства.

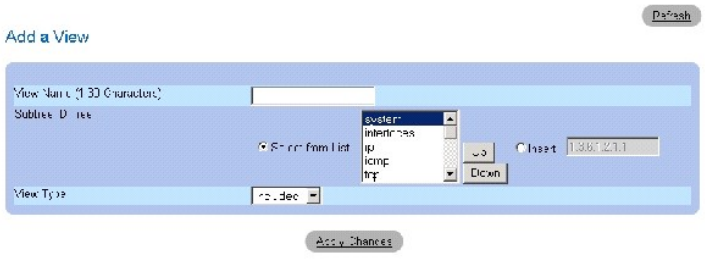
View Type (Тип вида)- Указывает, будет ли определенная ветвь OID включена или выключена из выбранного вида SNMP.

Добавление вида

1. Откройте страницу **Страница SNMPv3 View Settings**.
2. Нажмите кнопку Add (Добавить).

Откроется страница **Добавление вида**.

Рисунок 6-59. Добавление вида



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

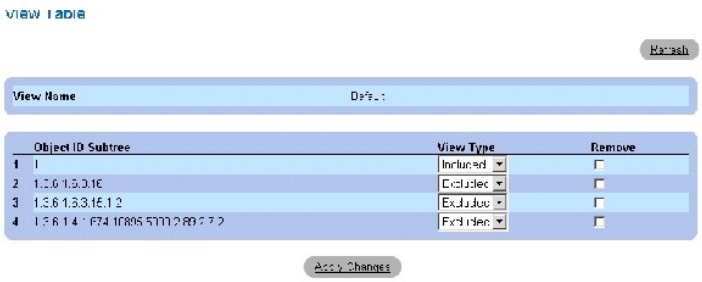
Вид SNMP добавлен, а устройство обновлено.

Вывод таблицы вида

1. Откройте страницу **Страница SNMPv3 View Settings**.
2. Нажмите кнопку Show All (Показать все).

Откроется страница **View Table (Таблица видов)**.

Рисунок 6-60. View Table (Таблица видов)



Команды консоли для определения видов SNMPv3

В следующей таблице приведены команды консоли, соответствующие полям на странице **Страница SNMPv3 View Settings**.

Таблица 6-38. Команды страницы SNMP View

Команды консоли	Описание
snmp-server view *view-name oid-tree* {**included** | **excluded**}	Создает или обновляет запись вида.
show snmp views [*viewname*]	Отображение конфигурации видов.

Ниже приведен пример команд консоли:

```
Console(config)# snmp-server view user1
1 included

Console(config)# end

Console# show snmp views
```

Name	OID Tree	Type
----------	----------	----------

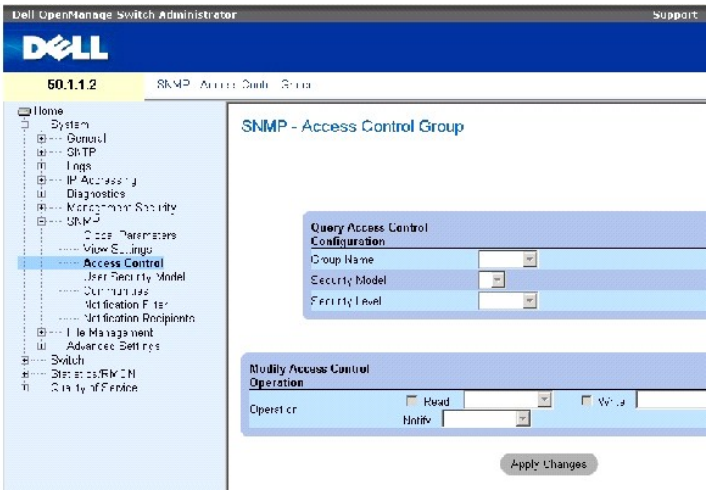
user1	iso	included
Default	iso	included
Default	snmpVacmMIB	excluded
Default	usmUser	excluded
Default	rndCommunityTable	excluded
DefaultSuper	iso	included

Определение контроля доступа к SNMP

На странице Access Control (Контроль доступа) предоставлена информация по созданию групп SNMP и назначению им привилегий контроля прав доступа к SNMP. Группы дают возможность администраторам сети назначать права доступа для определенных функций устройства или его аспектов.

Чтобы открыть страницу **Access Control Group (Группа контроля доступа)** нажмите System (Система) → SNMP → Access Control (Контроль доступа) в панели дерева.

Рисунок 6-61. Access Control Group (Группа контроля доступа)



На странице **Access Control Group (Группа контроля доступа)** есть следующие поля:

Group Name (Имя группы) - Пользовательская группа, к которой применяются правила контроля доступа. Значение поля: до 30 символов.

SNMP Version (Версия SNMP) - Определяет версию SNMP, назначенную для группы. Возможные значения поля:

SNMPv1 - Для группы определен SNMPv1.

SNMPv2 - Для группы определен SNMPv2.

SNMPv3 - Для группы определен SNMPv3.

Security Level (Уровень защиты) - Уровень защиты, определенный для группы. Уровни защиты применяются только для SNMPv3. Возможные значения поля:

No Authentication (Без идентификации) - Группе не назначаются уровни защиты Authentication (Идентификация) или Privacy (Неприкосновенность).

Authentication (Идентификация) - Идентифицирует сообщения SNMP и гарантирует, что будет выполнена идентификация происхождения сообщений SNMP.

Privacy (Неприкосновенность) - Шифрует сообщения SNMP.

Operation (Действие) - Определяет права доступа группы. Возможные значения поля:

Read (Чтение) - Указывает, что доступ к управлению ограничивается доступом только для чтения (изменения в вид SNMP внести нельзя).

Write (Запись) - Указывает, что доступ к управлению является доступом для чтения и записи (можно вносить изменения в вид SNMP).

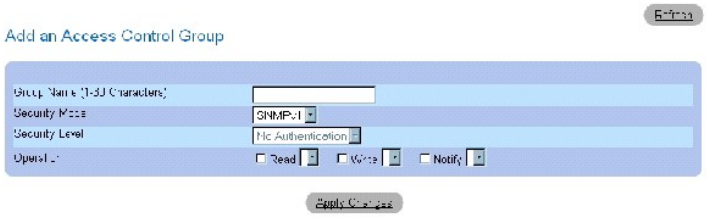
Notify (Извещение) - Отправляет прерывания для определенного вида SNMP.

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).

Рисунок 6-62. Добавление группы контроля доступа



3. Определите поля на странице Добавление группы контроля доступа.
4. Нажмите кнопку Apply Changes (Применить изменения).

Группа будет добавлена, а устройство обновлено.

Вывод таблицы доступа

1. Откройте страницу Access Control Group (Группа контроля доступа).
2. Нажмите кнопку Show All (Показать все).

Откроется страница Access Table (Таблица доступа).

Рисунок 6-63. 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 к SNMP с помощью командной строки

В следующей таблице приведены команды консоли, соответствующие полям на странице Access Control Group.

Таблица 6-39. Команды страницы SNMP Access Control

Команды консоли	Описание
snmp-server group *groupname* {**v1 | v2 | v3** {**noauth** | **auth** | **priv**}} [**read** *readview*] [**write** *writeview*] [**notify** *notifyview*]	Конфигурация новой группы протокола SNMP или таблица соответствия пользователей SNMP и видов SNMP.
show snmp groups [*groupname*]	Отображение конфигурации групп

Ниже приведен пример команд консоли:

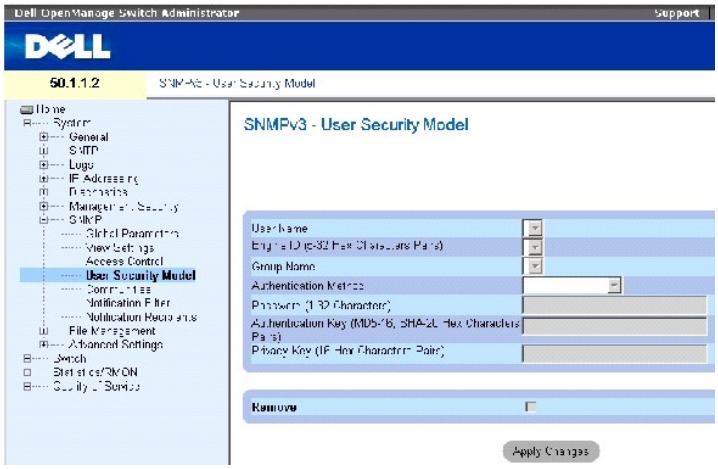
```
console (config)# snmp-
server group user-group v3
priv read user- view
```

Назначение защиты пользователей SNMP

На странице **Модель защиты пользователей SNMPv3 (USM)** можно назначить пользователей системы в группы SNMP, а также определить метод идентификации пользователей.

Чтобы открыть страницу **Модель защиты пользователей SNMPv3 (USM)**, выберите **System (Система)** → **SNMP** → **User Security Model** (Модель защиты пользователей) на панели дерева.

Рисунок 6-64. Модель защиты пользователей SNMPv3 (USM)



На странице **Модель защиты пользователей SNMPv3 (USM)** есть следующие поля:

User Name (Имя пользователя) - Список имен пользователей. Значение поля: до 30 символов.

Engine ID (Идентификатор) - Указывает локальную или отдаленную запись SNMP, к которой подключен пользователь. Изменение или удаление локального идентификатора механизма SNMP приводит к удалению пользовательской базы данных SNMPv3.

Local (Локально) - Пользователь подключен к локальной записи SNMP.

Remote (Отдаленно) - Пользователь подключен к отдаленной записи SNMP. Если задан идентификатор механизма, отдаленные устройства получают соответствующее сообщение.

Group Name (Имя группы) - Список пользовательских групп SNMP. Группы SNMP определены на странице Access Control Group (Группа контроля доступа).

Authentication Method (Метод идентификации) - Мотод идентификации пользователей. Возможные значения поля:

MD5 Key (Ключ MD5)- Пользователи идентифицируются по алгоритму HMAC-MD5.

SHA Key (Ключ SHA)- Пользователи идентифицируются по алгоритму HMAC-SHA-96.

MD5 Password (Пароль MD5) - Для идентификации пользователей используется пароль по алгоритму HMAC-MD5-96. Пользователь должен ввести пароль.

SHA Password (Пароль SHA)- Пользователи идентифицируются по алгоритму HMAC-SHA-96. Пользователь должен ввести пароль.

None (Нет) - Указывает, что идентификация пользователя не проводится.

Password (0-32 Characters) (Пароль, 0-32 символа) - Изменяет пользовательский пароль группы. Пароль должен состоять максимум из 32 буквенных символов.

Authentication Key (MD5-16; SHA-20 hexa chars) (Ключ идентификации) - Определяет уровень идентификации HMAC-MD5-96 или HMAC-SHA-96. Ключи идентификации и неприкосновенности вводятся для определения ключа идентификации. Если требуется только идентификация, для MD5 определяются 16 байтов. При необходимость использовать ключи идентификации и неприкосновенности для MD5 задаются 32 байта. Каждый байт символа шестнадцатиричной строки представлен двумя шестнадцатиричными числами. Знак разделителя байтов - точка или двоеточие.

Privacy Key (16 hexa characters) (ключ секретности, 16 символов) - Если требуется только идентификация, определяются 20 байтов. При необходимость использовать ключи идентификации и неприкосновенности задаются 16 байтов. Каждый байт символа шестнадцатиричной строки представлен двумя шестнадцатиричными числами. Знак разделителя байтов - точка или двоеточие.

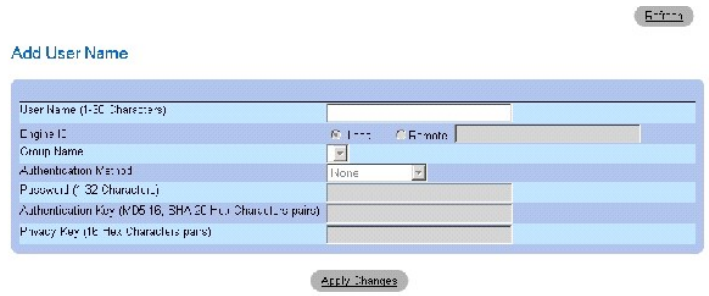
Remove (Удалить). Если данный флажок установлен, пользователи удаляются из определенной группы.

Добавление пользователей в группу

1. Откройте страницу Модель защиты пользователей SNMPv3 (USM).
2. Нажмите кнопку Add (Добавить).

Откроется страница Add SNMPv3 User Name (Добавить имя пользователя SNMPv3).

Рисунок 6-65. Add SNMPv3 User Name (Добавить имя пользователя SNMPv3)



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

Пользователь добавлен в группу, а устройство обновлено.

Отображение User Security Model Table (Таблица модели защиты пользователя)

1. Откройте страницу **Модель защиты пользователей SNMPv3 (USM)**.
2. Нажмите кнопку Show All (Показать все).

Откроется страница **User Security Model Table (Таблица модели защиты пользователя)**.

Рисунок 6-66. User Security Model Table (Таблица модели защиты пользователя)

Удаление записи из таблицы User Security Model

1. Откройте страницу **Модель защиты пользователей SNMPv3 (USM)**.
2. Нажмите кнопку Show All (Показать все).

   Откроется страница **User Security Model Table (Таблица модели защиты пользователя)**.
3. Выберите запись **User Security Model Table (Таблица модели защиты пользователя)**.
4. Установите флажок **Remove** (Удалить).
5. Нажмите кнопку Apply Changes (Применить изменения).

   Запись **User Security Model Table (Таблица модели защиты пользователя)** удалена, а устройство обновлено.

Команды консоли для определения пользователей SNMPv3

В следующей таблице приведены команды консоли, соответствующие полям на странице **Модель защиты пользователей SNMPv3 (USM)**.

Таблица 6-40. Команды для пользователей SNMPv3

Команды консоли	Описание
snmp-server user *username groupname* [**remote** engineid- string][**auth-md5** password | **auth-sha password** | **auth- md5-key** *md5-des-key* | **auth- sha-key** *sha-des-key*]	Конфигурация нового пользователя SNMP V3.
show snmp users [*username*]	Отображение конфигурации пользователей.

Ниже приведен пример команд консоли:

```
console (config)# snmp-server user John user-group auth-md5 1234

console (config)# end

console# show snmp users
```

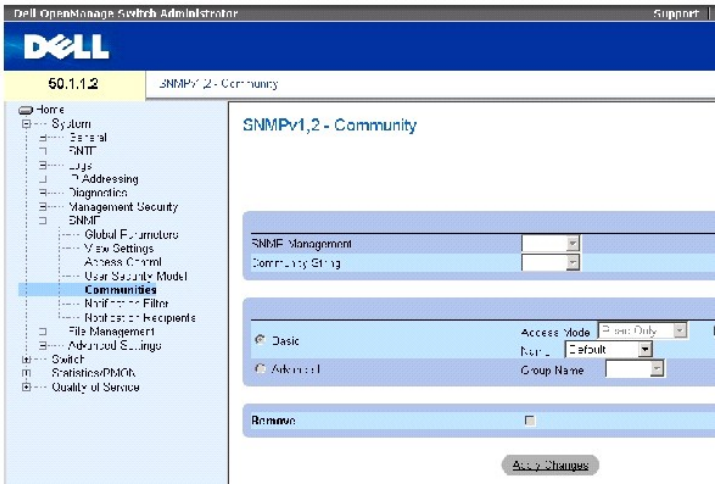
Name	Group Name	Auth Method	Remote
----	-----	------	------
John	user-group	md5	

Определение сообществ SNMP

Управление правами доступа выполняется с помощью определения сообществ на странице **Сообщества SNMPv1,2**. При изменении имен сообществ

изменяются также и права доступа. Сообщества SNMP определяются только для SNMP v1 и SNMP v2. Чтобы открыть страницу **Сообщества SNMPv1,2** нажмите **System (Система)** → **SNMP**→ **Communities (Сообщества)** в панели дерева.

Рисунок 6-67. Сообщества SNMPv1,2



На странице **Сообщества SNMPv1,2** **есть следующие поля:**

SNMP Management Station (Станция управления SNMP) - IP-адрес станции управления, для которой определено сообщество SNMP.

Community String (Строка сообщества) - Действует как пароль и используется для идентификации выбранной станции управления для устройства.

Basic (Базовый) - Включение режима Basic для выбранного сообщества SNMP. Возможные значения поля:

Access Mode (Режим доступа) - Определяет права доступа для сообщества. Возможные значения поля:

Read Only (Только чтение) - Указывает, что доступ к управлению ограничивается доступом только для чтения (изменения в сообщество внести нельзя).

Read Write (Чтение и запись) - Указывает, что при доступе к управлению можно выполнять чтение и запись и вносить изменения в конфигурацию устройства, но не сообщества.

SNMP Admin (Администратор SNMP) - Указывает, что пользователь имеет доступ ко всем параметрам конфигурации устройства и к изменению сообщества.

View Name (Имя вида) - Список пользовательских видов SNMP.

Name (Имя) - Имя сообщества, используемое для SNMPv1,v2.

Advanced - Список пользовательских групп. При выборе режима Advanced (Расширенный) для выбранного сообщества включаются правила управления доступом к SNMP, определенные для группы. В этом режиме также активируются группы SNMP в определенных сообществах SNMP. Режим Advanced определяется только для SNMPv3. Возможное значение поля:

Group Name (Имя группы) - Указывает имя группы при работе в расширенном режиме SNMP (Advanced mode).

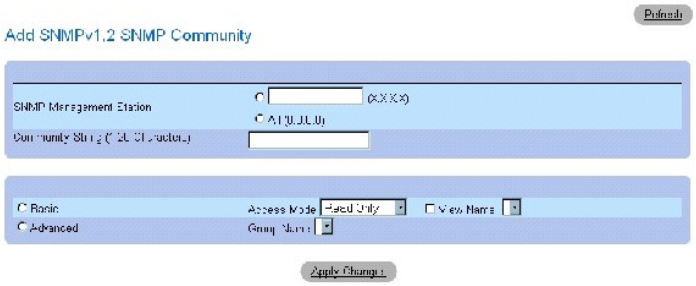
Remove (Удалить) - Если включено, сообщество удаляется.

Определение нового сообщества:

1. Откройте страницу **Сообщества SNMPv1,2**.
2. Нажмите кнопку **Add** (Добавить).

Откроется страница **Add SNMP Community** (Добавление сообщества SNMP).

Рисунок 6-68. 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 **Сообщества SNMPv1,2**.
2. Нажмите кнопку **Show All** (Показать все).

Откроется страница **Community Table** (Таблица сообществ).

3. Выберите сообщество и отметьте флажком поле **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 **Сообщества SNMPv1,2**.

Таблица 6-41. Команды страницы SNMP Community

Команды консоли	Описание
snmp-server community *community* [**ro** | **rw** | **su**] [*ip-address*][**view** *view-name*]	Задает строку доступа к сообществу для разрешения доступа по протоколу SNMP.
snmp-server community-group *community group-name* [*ip-address*]	Задает строку доступа к сообществу для разрешения доступа по протоколу SNMP на основании групповых прав доступа.

show snmp	Отображает текущую конфигурацию устройства SNMP.

Ниже приведен пример команд консоли:

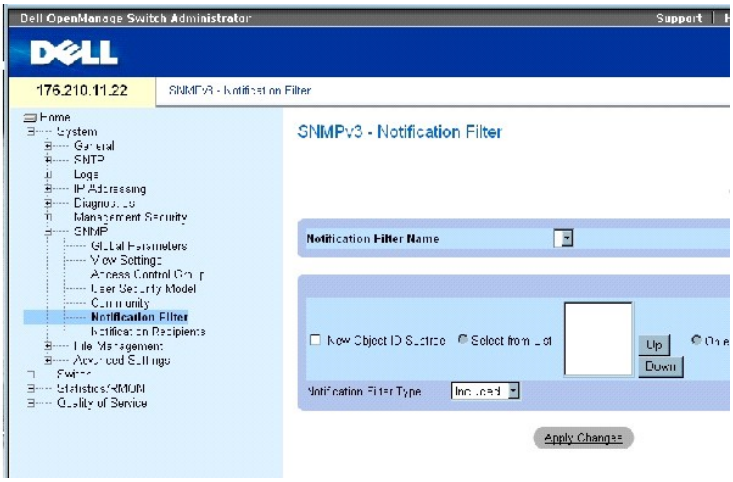
```
Console (config)# snmp-server community dell ro 10.1.1.1
```

Определение фильтров извещений SNMP

На странице **Фильтр извещений** имеется возможность фильтровать прерывания на основе идентификатора OID. Каждый идентификатор OID связан с функцией устройства или с ее аспектом. Также на странице **Фильтр извещений** администраторы сети могут фильтровать извещения.

Чтобы открыть страницу **Фильтр извещений**, выберите **System (Система) → SNMP → Notification Filters (Фильтры извещений)** *на панели дерева*.

Рисунок 6-69. Фильтр извещений



На странице **Фильтр извещений** есть следующие поля:

Notification Filter Name (Имя фильтра извещений) - Пользовательский фильтр извещений.

New Object Identifier Tree (Новое дерево OID) - Идентификатор OID, для которого отправляются или блокируются извещения. Если за OID закреплен фильтр, то создаются прерывания, которые отправляются получателям системных прерываний. Идентификаторы объектов (OID) выбираются либо из поля *Select from List*, либо из списка *Object ID List*.

Notification Filter Type (Тип фильтра извещений)- Указывает, отправляются или нет прерывания относительно OID.

Excluded (Исключен)- Ограничивает отправку прерываний OID.

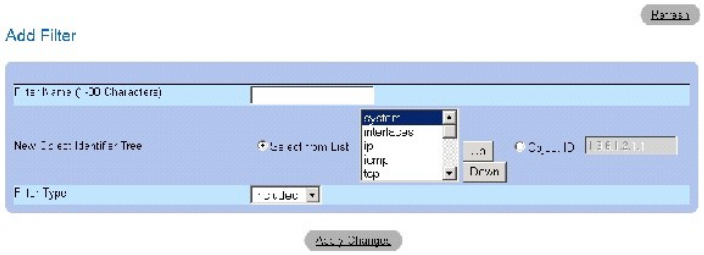
Included (Включен)- Отправляет прерывания OID.

Добавление фильтров SNMP

1. Откройте страницу Фильтр извещений.
2. Нажмите кнопку Add (Добавить).

Откроется страница Add Filter (Добавить фильтр).

Рисунок 6-70. Add Filter (Добавить фильтр)



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

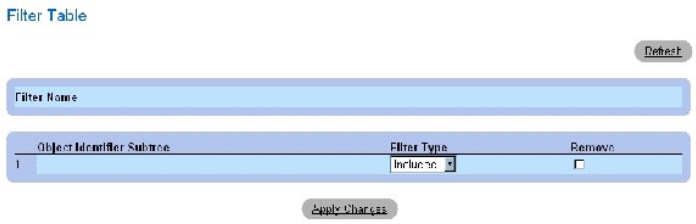
Новый фильтр добавлен, а устройство обновлено.

Вывод таблицы фильтра

1. Откройте страницу **Фильтр извещений**.
2. Нажмите кнопку Show All (Показать все).

Откроется страница **Filter Table (Таблица фильтра)**.

Рисунок 6-71. Filter Table (Таблица фильтра)



Удаление фильтра

1. Откройте страницу **Фильтр извещений**.
2. Нажмите кнопку Show All (Показать все).

Откроется страница **Filter Table (Таблица фильтра)**.

3. Выберите запись **Filter Table (Таблица фильтра)**.
4. Установите флажок **Remove** (Удалить).

Выбранный фильтр удален, а устройство обновлено.

Настройка фильтров извещений с помощью командной строки

В следующей таблице приведены команды консоли, соответствующие полям на странице **Фильтр извещений**.

Таблица 6-42. Команды страницы SNMP Notification Filter

Команды консоли	Описание
snmp-server filter filter-name oid-tree {**included** | **excluded**}	Создает или обновляет фильтр извещений SNMP.
show snmp filters [filtername]	Показывает конфигурацию фильтров извещений SNMP

Ниже 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
```

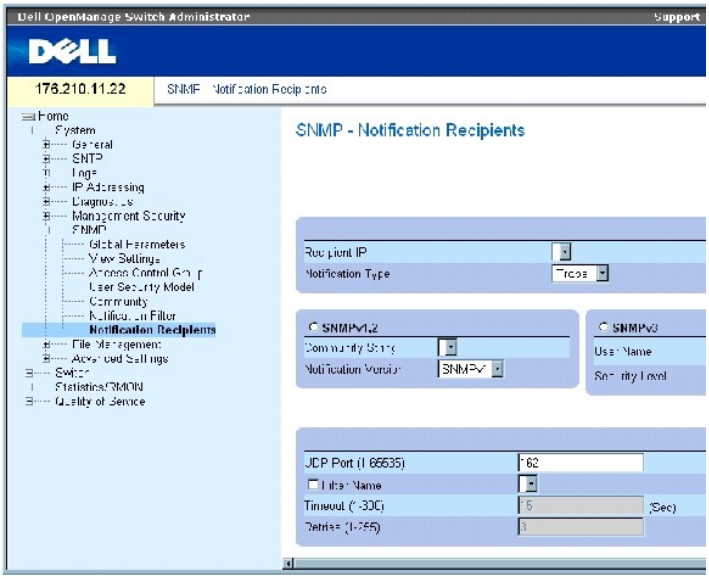
Определение получателей извещений SNMP

На странице **Получатели извещений** содержится информация по заданию фильтров, которые определяют, отправляются ли прерывания определенным пользователям, и задают тип отправляемых прерываний. Фильтры извещений SNMP предоставляют следующие службы:

- Идентификация получателей системных прерываний
- Фильтрация прерываний
- Выбор параметров создания прерываний
- Выполнение проверки управления доступом

Чтобы открыть страницу **Получатели извещений** нажмите **System (Система)** → **SNMP**→ **Notification Recipient (Получатель извещения)** в панели дерева.

Рисунок 6-72. Получатели извещений



На странице **Получатели извещений** есть следующие поля:

Recipient IP (IP-адрес получателя) - Указывает IP-адрес, по которому отправляются системные прерывания.

Notification Type (Тип извещения) - Отправленное извещение. Возможные значения поля:

Trap (Прерывание) - Отправляются прерывания.

Inform (Сообщение) - Отправляются сообщения.

SNMPv1,2 - Для выбранных получателей включаются версии 1 и 2 протокола SNMP. Для SNMPv1 и SNMPv2 определите следующие поля:

Community String (1-20 Characters) (Строка сообщества, 1-20 символов) - Определяет строку сообщества менеджера системных прерываний.

Notification Version (Версия извещения) - Определяет тип прерывания. Возможные значения поля:

SNMP V1 - Указывает, что отправляются системные прерывания SNMP Version 1.

SNMP V2 - Указывает, что отправляются системные прерывания SNMP Version 2.

SNMPv3 - Для отправления и получения прерываний используется SNMPv3. Для SNMPv3 определите следующие поля:

User Name (Имя пользователя) - Пользователь, которому отправляется извещение SNMP.

Security Level (Уровень защиты) - Определяет метод идентификации пакета. Возможные значения поля:

No Authentication (Без идентификации) — Пакет не идентифицируется и не шифруется.

Authentication (Идентификация)— Пакет идентифицируется.

Privacy (Неприкосновенность)— Пакет идентифицируется и шифруется.

UDP Port (1-65535) (Порт UDP) - Для отправки извещений используется порт UDP. Значение по умолчанию - 162.

Filter Name (Имя фильтра) - Включает или исключает фильтры SNMP.

Timeout (1-300) (Пауза)- Интервал времени ожидания (в секундах), по истечении которого устройство повторно отправляет сообщение. Значение по умолчанию: 15 секунд.

Retries (1-255) (Повторные попытки)- Количество раз повторной отправки сообщений. Значение по умолчанию - 3.

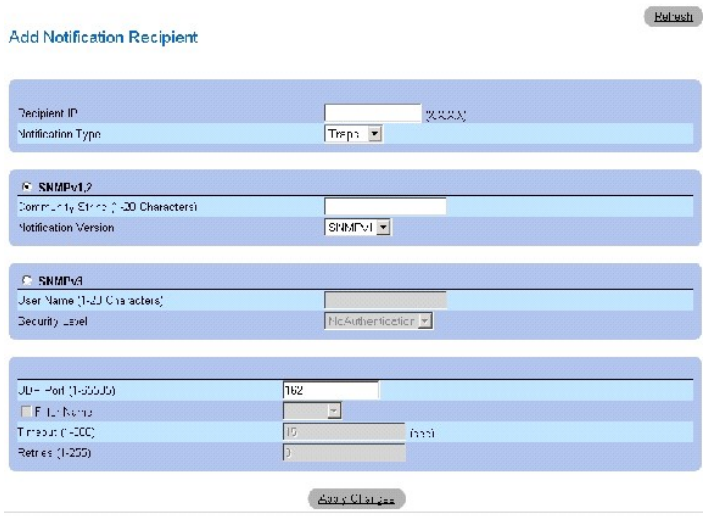
Remove Notification Recipient (Удалить получателя извещения) - Если поле отмечено, выбранный получатель извещения удаляется.

Добавление нового получателя системного прерывания

1. Откройте страницу **Получатели извещений**.
2. Нажмите кнопку Add (Добавить).

Откроется страница **Добавить получателей извещений**.

Рисунок 6-73. Добавить получателей извещений



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

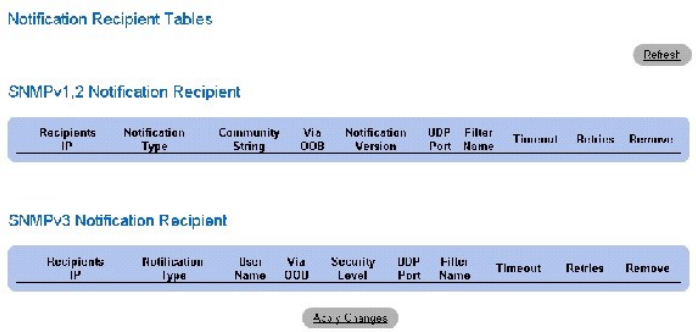
Получатель извещений добавлен, а устройство обновлено.

Отображение Notification Recipients Tables (Таблицы получателей извещений)

1. Откройте страницу **Получатели извещений**.
2. Нажмите кнопку Show All (Показать все).

Откроется страница **Таблицы получателей извещений**.

Рисунок 6-74. Таблицы получателей извещений



Удаление получателей извещений

1. Откройте страницу **Получатели извещений**.
2. Нажмите кнопку Show All (Показать все).

Откроется страница **Таблицы получателей извещений**.

3. Выберите получателя извещений либо из поля **SNMPV1,2 Notification Recipient** либо **SNMPv3 Notification Recipient Tables**.
4. Установите флажок **Remove** (Удалить).
5. Нажмите кнопку Apply Changes (Применить изменения).

Получатель удален, а устройство обновлено.

Настройка получателей извещений с помощью командной строки

В следующей таблице приведены команды консоли, соответствующие полям на странице **Получатели извещений**.

Таблица 6-43. Команды страницы SNMP Community

Команды консоли	Описание
snmp-server host {ipaddress | hostname} *community-string* [**traps** | **informs**] [**1** | **2**] [**udp-port** port] [**filter** filtername] [**timeout** seconds] [**retries** retries]	Создает или обновляет получателей извещений по протоколу SNMP version 1 или 2.
snmp-server v3-host {ip-address | hostname} *username* [**traps** | **informs**] {**noauth** | **auth** | **priv**} [**udp-port** *port*] [**filter** filtername] [**timeout** seconds] [**retries** retries]	Создает или обновляет получателей извещений по протоколу SNMP version 3.
show snmp	Показывает текущую конфигурацию SNMP

Ниже 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	user-view	All
private	read write	default	172.16.1.1
private	su	DefaultSuper	172.17.1.1

Управление файлами

Используйте страницу **File Management (Управление файлами)** для управления программным обеспечением устройства, файлами изображений и файлами конфигурации. Файлы можно загрузить с сервера TFTP.

Обзор файла управления

Структура файла управления состоит из следующих файлов:

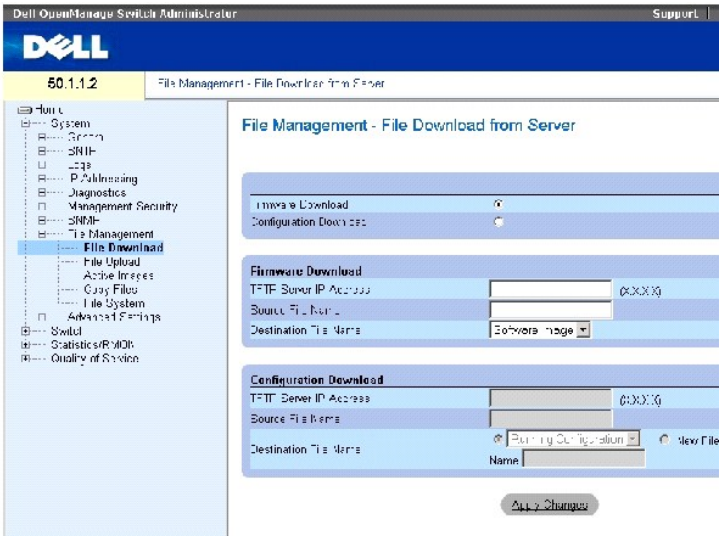
- Startup Configuration File (Конфигурация для запуска) - Содержит команды, необходимые для конфигурации устройства при запуске или перезагрузке. Файл конфигурации для запуска создан посредством копирования команд конфигурации из файла рабочей конфигурации или из резервного файла конфигурации.
- Файл рабочей конфигурации- Содержит все команды файла для запуска, а также все команды, введенные во время последнего сеанса. После отключения или перезагрузки устройства все команды, сохраненные в файле рабочей конфигурации, теряются. В ходе запуска все команды файла для запуска копируются в файл рабочей конфигурации и применяются к устройству. Во время сеанса все новые введенные команды добавляются к существующим командам файла рабочей конфигурации. Чтобы изменить файл запуска, нужно перед отключением устройства скопировать файл рабочей конфигурации в файл конфигурации для запуска.
- Резервный файл конфигурации - Содержит резервную копию конфигурации устройства. В устройстве можно сохранить до пяти резервных файлов конфигурации. Имена этих файлов задаются пользователем. Эти файлы создаются, когда пользователь копирует файл рабочей конфигурации или файл конфигурации для запуска в файл с пользовательским именем. Содержимое резервного файла можно скопировать либо в файл рабочей конфигурации, либо в файл конфигурации для запуска.
- Image Files - Системные образы сохраняются в двух FLASH-файлах, называемых Image 1 и Image 2. Активный образ хранит активную копию, остальные - вторичную копию. Устройство загружается и запускается из активного образа. Если активный образ поврежден, система автоматически загружается из неактивного образа. Эта функция безопасности для сбоев, происходящих в процессе обновления программного обеспечения.

Чтобы открыть страницу File Management (Управление файлами) , нажмите System (Система) → File Management (Управление файлами) в панели дерева.

Загрузка файлов

На странице **Загрузка файлов с сервера**есть поля для загрузки образа и файлов конфигурации с сервера TFTP на устройство. Чтобы открыть страницу **Загрузка файлов с сервера**нажмите System (Система) Ж File Managemen (Управление файлами) Ж File Download (Загрузка файлов) в панели дерева.

Рисунок 6-75. Загрузка файлов с сервера



На странице **Загрузка файлов с сервера** есть следующие поля:

Firmware Download (Загрузка встроенных программ) - Указывает, что загружается файл встроенных программ. Если поле Firmware Download (Загрузка встроенных программ) выделено, то поля Configuration Download (Загрузка конфигурации) неактивны (серые).

Configuration Download (Загрузка конфигурации) - Указывает, что загружается файл конфигурации. Если поле Configuration Download (Загрузка встроенных программ) выделено, то поля Firmware Download (Загрузка конфигурации) неактивны (серые).

Загрузка встроенных программ

TFTP Server IP Address (IP-адрес сервера TFTP). IP-адрес сервера TFTP, с которого загружаются файлы.

Source File Name (Имя исходного файла) - Указывает файл, который нужно загрузить.

Destination File Name (Файл назначения). Тип файла назначения, в который загружается файл. Возможные значения поля:

Software Image (Образ программного обеспечения). Загрузка файла образа программного обеспечения.

Boot Code - Загружает файл Boot.

Загрузка конфигурации

TFTP Server IP Address (IP-адрес сервера TFTP). IP-адрес сервера TFTP, с которого загружаются файлы конфигурации.

Source File Name (Имя исходного файла) - Указывает файл конфигурации, который нужно загрузить.

Destination File Name (Файл назначения). Тип файла назначения, в который загружается файл конфигурации. Возможные значения поля:

Running Configuration (Рабочая конфигурация) - Загружает команды в файлы рабочей конфигурации.

Startup Configuration- (Конфигурация для запуска) - Загружает файл конфигурации для запуска и переписывает его.

User Defined Backup Configuration (Файл резервной пользовательской конфигурации)- Загружает файл резервной пользовательской конфигурации и переписывает его.

New File Name (Имя нового файла)- Загружает новый файл резервной конфигурации.

ПРИМЕЧАНИЕ. Файл образа замещает неактивный образ. Необходимо отметить, что -неактивный образ станет активным после перезагрузки, также рекомендуется перезагрузить устройство сразу после загрузки файла.

Во время загрузки файла образа за ходом загрузки можно наблюдать в диалоговом окне загрузки. По окончании процесса это диалоговое окно автоматически закрывается.

Загрузка файлов

1. Откройте страницу **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.

ПРИМЕЧАНИЕ. Для активизации выбранного файла-образа перезагрузите устройство. Информацию о перезагрузке устройства см. в разделе **Переключение главных устройств**.

Загрузка файлов с сервера с помощью команд консоли

В следующей таблице приведены команды консоли, соответствующие полям на странице **Загрузка файлов с сервера**.

Таблица 6-44. Команды консоли для загрузки файла

Команды консоли	Описание
copy source-url destination-url	Копирует любой файл из исходного местоположения в место назначения.

Ниже приведен пример команд консоли:

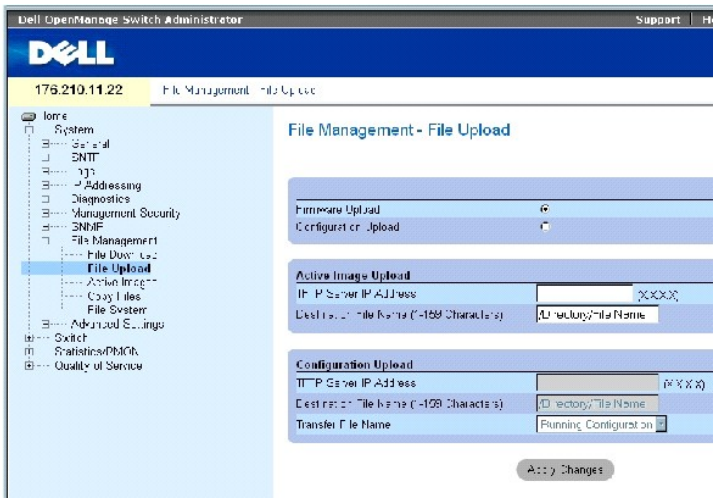
```
console# copy
tftp://10.6.6.64/pp.txt
startup-config



....!



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.

Загрузка файлов на сервер

На странице **Страница File Upload to Server** есть поля для загрузки программного обеспечения на сервер TFTP с устройства. Файлы образов можно также загрузить на сервер со страницы **Страница File Upload to Server**. Чтобы открыть страницу **Страница File Upload to Server**, нажмите System (Система) Ж File Management (Управление файлами) Ж File Upload (Загрузка файлов на сервер) в панели дерева.

Рисунок 6-76. Страница File Upload to Server



На странице **Страница File Upload to Server** есть следующие поля:

Firmware Upload (Загрузка на сервер встроенных программ) - Указывает, что загружается файл встроенных программ. Если поле **Firmware Upload** (Загрузка на сервер встроенных программ) выделено, то поля **Configuration Download** (Загрузка конфигурации) становятся недоступны.

Configuration Upload (Загрузка конфигурации на сервер) - Указывает, что загружается файл конфигурации. Если поле **Configuration Upload** (Загрузка конфигурации на сервер) выделено, то поля **Active Image Upload** (Загрузка активного образа на сервер) становятся недоступны.

Загрузка активного образа на сервер

TFTP Server IP Address (IP-адрес сервера TFTP) - Указывает IP-адрес, для которого загружается образ программы.

Destination File Name (1-159 Characters) (Имя файла назначения, 1-159 символов)- Указывает путь к файлу с образом программы, куда загружается файл.

Загрузка конфигурации на сервер

TFTP Server IP Address (IP-адрес сервера TFTP) - Указывает IP-адрес сервера TFTP, для которого загружается файл конфигурации.

Destination File Name (1-159 Characters) (Имя файла назначения, 1-159 символов)- Указывает путь к файлу конфигурации, куда загружается файл.

Transfer File Name (Имя файл передачи). Тип файла программы, в который загружается файл конфигурации. Возможные значения поля:

Running Configuration (Рабочая конфигурация) - Загружает файл рабочей конфигурации.

Startup Configuration (Конфигурация для запуска) - Загружает файл конфигурации для запуска.

List of User Defined Configuration Files (Список пользовательских файлов конфигурации) - Загружает список пользовательских файлов конфигурации на сервер.

ПРИМЕЧАНИЕ. Список пользовательских файлов конфигурации виден при условии, что пользователь создал архивные копии файлов конфигурации. Например, если пользователь скопировал файл рабочей конфигурации в пользовательский файл конфигурации, названный BACKUP-SITE-1, этот спиок появляется на странице **Страница File Upload to Server**, а файл конфигурации BACKUP-SITE-1 заносится в список.

Загрузка файлов на сервер

1. Откройте страницу **Страница File Upload to Server**.
2. Определите тип файла для загрузки.
3. Определите поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Программное обеспечение будет загружено на сервер TFTP.

Загрузка файлов на сервер с помощью команд консоли

В следующей таблице приведены команды консоли, соответствующие полям на странице **Страница File Upload to Server**.

Таблица 6-45. Команды консоли для загрузки файла на сервер

Команды консоли	Описание
copy source-url destination-url	Копирует любой файл из исходного местоположения в место назначения.

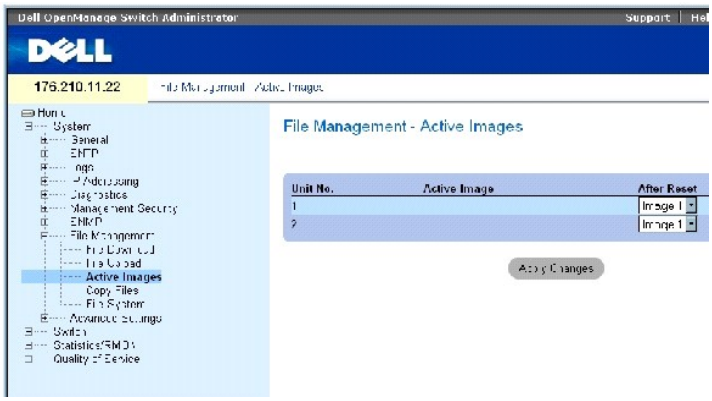
Ниже приведен пример команд консоли:

```
console# copy image tftp://10.6.6.64/uploaded.ros

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

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

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

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

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

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


Copy: 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
```

Активация файлов образа

Страница **Активные образы** позволяет менеджерам сети выбирать и перенастраивать файлы-образы. Файл с активным образом для каждого устройства в конфигурации стека можно выбрать отдельно. Чтобы открыть страницу **Активные образы**, нажмите System (Система) → File Management (Управление файлами) → Active Images (Активные образы) в панели дерева.

Рисунок 6-77. Активные образы



На странице **Активные образы** есть следующие поля:

Unit No. - Номер устройства, для которого выбран файл-образ.

Active Image - Файл-образ, который в данный момент активен на устройстве.

After Reset (После сброса параметров) - Файл-образ, который активен на устройстве после сброса параметров. Возможные значения поля:

Image 1 - Активирует файл Image 1 после перезапуска устройства.

Image 2 - Активирует файл Image 2 после перезапуска устройства.

Выбор файла-образа

1. Откройте страницу **Активные образы**.
2. Выберите файл-образ для указанного устройства в поле **After Reset** (После сброса параметров).
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Файл-образ будет выбран. Файл-образ перезагружается только после следующего сброса параметров. Файл-образ, выбранный на данный момент, продолжает работать до следующего сброса параметров устройства.

Работа с активным файлом-образом с помощью команд консоли

В следующей таблице приведены команды консоли, соответствующие полям на странице **Активные образы**.

Таблица 6-46. Команды консоли для загрузки файла на сервер

Команды консоли	Описание
boot system [**unit** | *unit*] {**image-1** | **image-2**}	Указывает образ системы, загружаемое устройством при начале работы.
show version [**unit** *unit*]	Выводит информацию о версии системы.

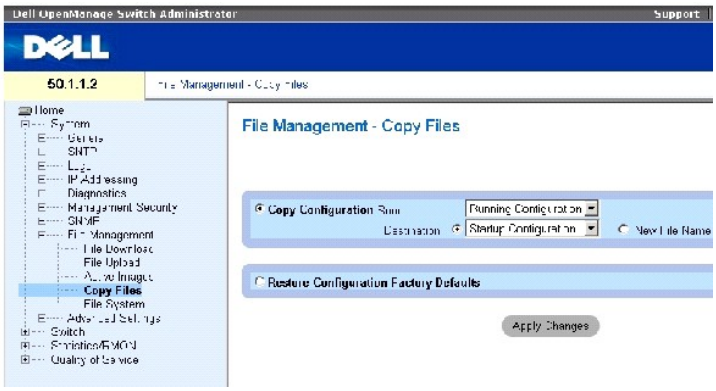
Ниже приведен пример команд консоли:

```
Console# boot system
image-1
```

Копирование файлов

Файлы можно копировать и удалять на странице **Копирование файлов**. Чтобы открыть страницу **Копирование файлов**, нажмите System (Система) → File Management (Управление файлами) → Copy Files (Копирование фалов) в панели дерева.

Рисунок 6-78. Копирование файлов



На странице **Копирование файлов** есть следующие поля:

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 требуется скопировать в файл назначения. Выберите файл рабочей конфигурации, конфигурации для запуска или один из пользовательских файлов резервной конфигурации.

Destination (Назначение) - Указывает файл конфигурации, в который будет скопирован исходный файл. Файлы нельзя скопировать в резервный файл главного резервного устройства. Резервные файлы появляются в поле **Destination Unit (Устройство назначения)** при условии, что эти резервные файлы были определены. Выберите поле New File Name (Новое имя файла)и укажите имя нового файла, чтобы скопировать исходный файл в новый резервный файл конфигурации.

New File Name (Новое имя файла) - Указывает имя вновь созданного резервного файла конфигурации.

Restore Configuration Factory Defaults (Восстановить фабричные стандартные файлы конфигурации) - Указывает, что текущие параметры конфигурации необходимо заменить на фабричные параметры конфигурации по умолчанию. Если поле не отмечено, это значит, что можно продолжать применять текущие параметры конфигурации.

Копирование файлов

1. Откройте страницу **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 **Копирование файлов**.
2. Click **Restore Configuration Factory Defaults (Восстановление заводских настроек по умолчанию)**.
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, соответствующие полям на странице **Копирование файлов**.

Таблица 6-47. Команды консоли для копирования файлов

Команды консоли	Описание
copy *source-url destination-url*	Копирует любой файл из исходного местоположения в место назначения.
delete startup-config	Удаляет файл конфигурации для запуска.

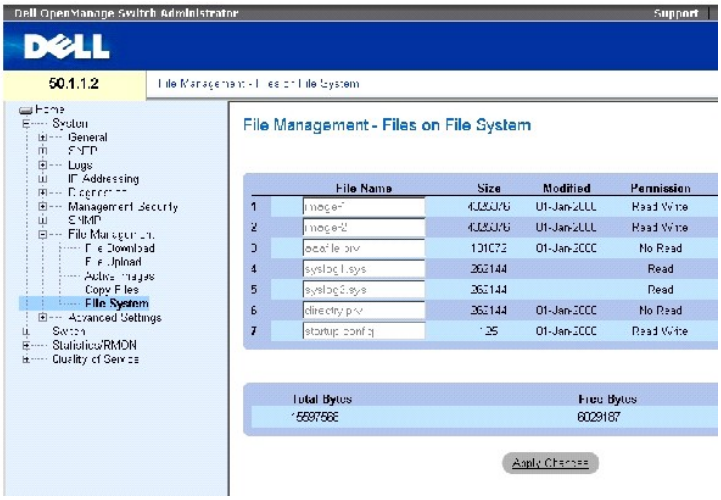
Ниже приведен пример команд консоли:

```
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 Файлы на странице File System приводится информация о файлах, сохраненных в системе, включая имена файлов, их размер, дату внесения изменений и права доступа. Файловая система позволяет управлять пятью файлами, общим размером 3 МБ. Чтобы открыть страницу Файлы на странице File System, нажмите System (Система) → File Management (Управление файлами) → File System (Система файлов) в панели дерева.

Рисунок 6-79. Файлы на странице File System



На странице Файлы на странице File System есть следующие поля:

File Name (Имя файла) -Указывает файл, сохраненный в настоящий момент в системе управления файлами.

Size (Размер) - Размер файла.

Modified (Изменен) - Дата изменения файла.

Permission (Права доступа) - Тип прав доступа, назначенный для файла. Возможные значения поля:

Read Only (Только для чтения) - Указывает файлы с атрибутом «только для чтения».

Read Write (Чтение и запись) - Указывает файлы с правами на чтение и запись.

Remove (Удалить) - Если отмечено флажком, файл удаляется.

Rename (Переименовать) - Позволяет изменить имя файла. Новое имя файла вводится в поле **File Name (Имя файла)**.

Total Bytes (Всего байтов) - Общее занимаемое пространство.

Free Bytes (Свободно байтов) - Значение оставшегося свободного пространства.

Управление файлами в режиме командной стоки

В следующей таблице перечислены команды для управления системными файлами.

Таблица 6-48. Команды консоли для копирования файлов

Команды консоли	Описание
dir	Отображает список файлов во флэш-памяти системы

Ниже приведен пример команд консоли:

```
console# dir

Directory of flash:

File Name       Permis-sion  Flash Size  Data Size  Modified
--------------  ------       ------      ------     ------------------
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
```

Total size of flash: 16646144 bytes				
Free size of flash: 4456448 bytes				

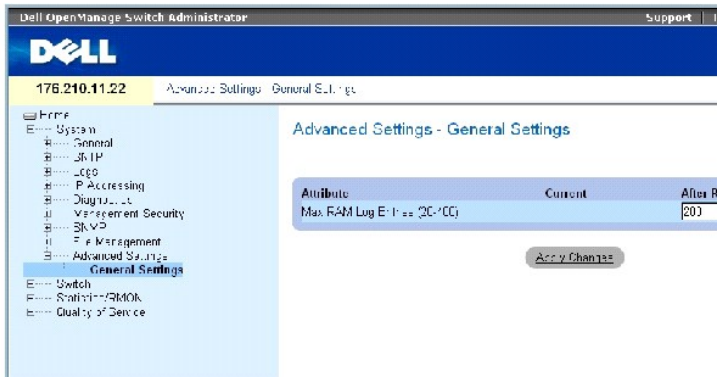
Настройка общих параметров

Используйте страницу Advanced Settings (Дополнительные настройки) для настройки различных общих атрибутов коммутатора. Внесенные изменения вступают в силу только после перезагрузки коммутатора. Выберите **System (Система)**→ **Advanced Settings (Дополнительные настройки)** в панели дерева, чтобы открыть страницу **Advanced Settings (Дополнительные настройки)**.

На странице **Advanced Settings (Дополнительные настройки)**имеются ссылки для настройки общих параметров.

На странице **Общие параметры**предоставлена информация по определению общих параметров коммутатора. Чтобы открыть страницу **Общие параметры**, нажмите System (Система) → Advanced Settings (Дополнительные настройки) → General Settings (Общие параметры) в панели дерева.

Рисунок 6-80. Общие параметры



На странице **Общие параметры** приводится следующая информация:

Attribute - Атрибут общего параметра.

Current - Текущее значение.

After Reset (После сброса) - Будущее значение (после сброса параметров). 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. Когда журнал заполнен, он очищается и файл журнала перезагружается.

Просмотр счетчика записей журнала ОЗУ с помощью команд консоли

В следующей таблице приведены команды консоли, соответствующие полям на странице **Общие параметры**.

Таблица 6-49. Команды страницы General Settings

Команды консоли	Описание
logging buffered size число	Задает число системных сообщений, хранящихся во внутреннем буфере (ОЗУ).

Ниже приведен пример команд консоли:

```
console(config)# logging
buffered size 300
```

Назад на страницу Содержание

Назад на страницу Содержание

Информация о настройке коммутатора

Системы Dell™ PowerConnect™ 34XX Руководство пользователя

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 параметров защиты сети с помощью списков управления доступом (ACL) и заблокированных портов. Чтобы открыть страницу **Network Security (Безопасность сети)** , выберите **Switch (Коммутатор)** → **Network Security (Безопасность сети)**.

Страница Port Based Authentication (Идентификация на основе портов)

Идентификация на основе портов позволяет определять системных пользователей индивидуально для каждого порта через внешний сервер. Только известные и утвержденные системой пользователи могут передавать и получать данные. Идентификация портов происходит на сервере RADIUS по протоколу Extensible Authentication Protocol (EAP, Наращиваемый протокол идентификации). Порт идентификации включает:

- **Authenticators (Удостоверения)** - Определяют порт устройства, идентификация которого происходит перед предоставлением доступа к системе.
- **Supplicants (Податели запроса)** - Определяют хост, подключенный к идентифицируемому порту, который запрашивает доступ к системным службам.
- **Authentication Server (Сервер идентификации)** - Указывает внешний сервер, например, RADIUS, который выполняет идентификацию на правах удостоверения и определяет, имеет ли податель запроса право на доступ к системным службам.

Идентификация на основе данных порта создает два состояния:

- **Controlled Access (Контролируемый доступ)** - Предоставляет возможность коммуникации между подателем запроса и системой, если податель запроса идентифицирован.
- **Uncontrolled Access (Неконтролируемый доступ)** - Предоставляет возможность неконтролируемой коммуникации вне зависимости состояния порта.

В настоящий момент коммутатор поддерживает идентификацию по портам через сервер RADIUS.

Расширенная идентификация на основе портов

Расширенная идентификация на основе портов:

- Дает возможность подсоединения нескольких хостов к одному порту.
- Для того, чтобы все хосты получили доступ к системе, только один из них должен быть идентифицирован. Если идентификацию порта выполнить не удалось, всем подключенным хостам будет отказано в доступе к сети.
- Включает идентификацию пользователя. Некоторые сети устройства VLAN всегда доступны, даже если некоторые подсоединенные порты не идентифицированы.
- Например, трафик голосовой информации по IP не требует идентификации, а для трафика данных она обязательна. Можно определить сети

VLAN, для которых не требуется идентификация. Неидентифицированные сети VLAN доступны для пользователей, даже если подключенные к ним порты определены как требующие идентификации.

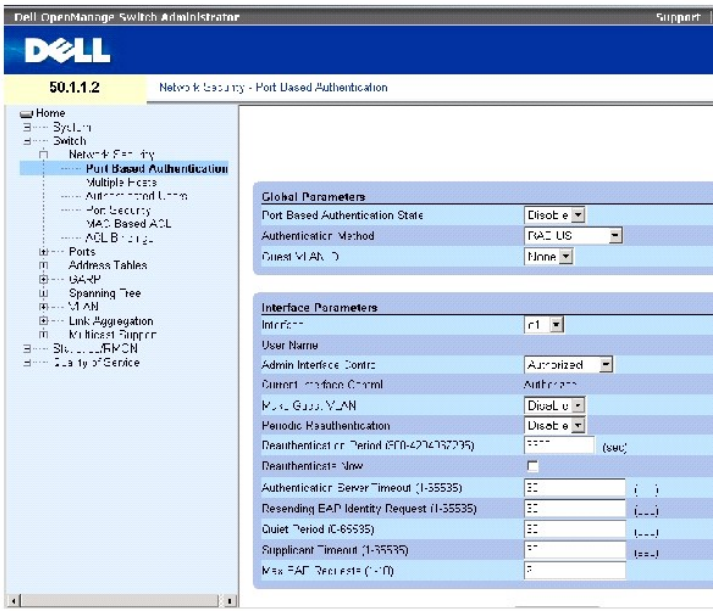
Расширенная идентификация на основе портов применяется в следующих режимах:

- **Single Host Mode (Режим одного хоста)** - Только один идентифицированный хост может получить доступ на порт.
- **Multiple Host Mode (Режим нескольких хостов)** - К одному порту можно подсоединить несколько хостов. Необходимо, чтобы только один хост был идентифицирован, чтобы все хосты получили доступ к сети. Если идентификацию хоста выполнить не удалось, или получено сообщение EAPOL о выходе из системы, подключенным клиентам отказывается в доступе к сети.
- **Guest VLANs (Гостевые VLAN)** - Предоставляет ограниченный доступ к сети для портов. Если порту отказано в досупе к сети в результате идентификации на основе порта, но включена гостевая сеть VLAN, порт получает ограниченный доступ к сети. Например, администратор сети может использовать гостевые сети VLAN, чтобы отказать в доступе к сети на основании идентификации, но предоставить доступ к Интернету неидентифицированным пользователям.

Конфигурация идентификации на основе портов

Страница Страница Port Based Authentication (Идентификация на основе портов) предоставляет администраторам сети настраивать идентификацию на основе портов. Чтобы открыть страницу Страница Port Based Authentication (Идентификация на основе портов) , щелкните **Switch (Коммутатор)** → **Network Security (Безопасность сети)** → **Port Based Authentication (Идентификация на основе портов).**

Рисунок 7-1. Страница Port Based Authentication (Идентификация на основе портов)



На странице Страница Port Based Authentication (Идентификация на основе портов) есть следующие поля:

Port Based Authentication State (Состояние идентификации на основе портов) - Позволяет выполнять идентификацию на основе портов в устройстве. Возможные значения поля:

Enable (Включить) - Включает идентификацию на основе портов в устройстве.

Disable (Отключить) - Отключает идентификацию на основе портов в устройстве.

Authentication Method (Режим идентификации) - Указывает, какой метод идентификации используется. Возможные значения поля:

None (Отсутствует) - Указывает, что метод идентификации портов отсутствует.

RADIUS - Указывает, что идентификация порта выполняется на сервере RADIUS.

RADIUS, None (RADIUS, Отсутствует) - Указывает, что сначала идентификация порта выполняется на сервере RADIUS. Если порт определен как неидентифицируемый, то метод идентификации не применяется, и дается разрешение на проведение сеанса.

Guest VLAN (Гостевая сеть VLAN) - Разрешает использование гостевых сетей VLAN для неидентифицированных портов. При включении режима Guest VLAN неидентифицированный порт автоматически подсоединяется к сети VLAN, выбранной в поле VLAN List (Список VLAN). По умолчанию поле отключено.

Interface (Интерфейс) - Список интерфейсов, для которых включена функция идентификации на основе портов.

User Name (Имя пользователя) - Указывает имя пользователя подателя запроса.

Admin Interface Control (Управление интерфейсом) - Определяет состояние идентификации порта. Возможные значения поля:

Auto (Автоматически) - Включает идентификацию на основе портов в устройстве. Интерфейс переключается из санкционированного состояния в санкционированное на основе обмена данными идентификации между устройством и клиентом.

Authorized (Санкционированный) - Переводит интерфейс в санкционированное состояние без его идентификации. Интерфейс отправляет и получает обычный трафик без идентификации на основе портов клиента.

Unauthorized (Несанкционированный) - Отказывает в доступе к системе выбранному интерфейсу, переводя его в несанкционированное состояние. Устройство не может предоставить клиенту службы идентификации через интерфейс.

Current Interface Control (Текущее управление интерфейсом) - Определяет текущего состояния идентификации порта.

Make Guest VLAN (Доступ к гостевой VLAN) - При его включении указывает, что неполномочные пользователи, подключенные к этому интерфейсу, могут получить доступ к сетевой VLAN.

Periodic Reauthentication (Периодическая переидентификация) - Позволяет выполнение немедленной повторной идентификации порта.

Reauthentication Period (300-4294967295) (Период переидентификации) - Указывает промежуток времени, по истечении которого выполняется повторная идентификация выбранного порта. Значение поля указано в секундах. Значение по умолчанию: 3600 секунд.

Reauthenticate Now (Переидентифицировать сейчас) - Позволяет выполнение немедленной повторной идентификации порта, если отметить поле флажком.

Authentication Server Timeout (1-65535) (Пауза сервера идентификации) - Определяет промежуток времени, по истечении которого устройство отправляет повторный запрос на сервер идентификации. Значение поля указано в секундах. Значение по умолчанию: 30 секунд.

Resending EAP Identity Request (1-65535) (Повторный запрос идентификатора с протокола EAP) - Определяет промежуток времени, по истечении которого устройство отправляет повторный запрос на протокол EAP. Значение по умолчанию: 30 секунд.

Quiet Period (0-65535) (Интервал бездействия) - Указывает количество секунд, в течение которых устройство остается в бездействии после неудачной попытки идентификации. Возможное значение поля: 0-65535. Значение по умолчанию: 60 секунд.

Supplicant Timeout (1-65535) (Пауза подателя запроса) - Определяет промежуток времени, по истечении которого подателю запроса отправляется повторный ответ с протокола EAP. Значение поля указано в секундах. Значение по умолчанию: 30 секунд.

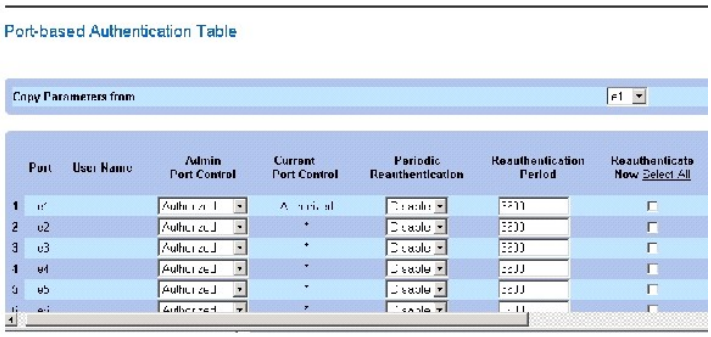
Max EAP Requests (1-10) (Максимальное количество запросов) - Указывает общее количество запросов, отправленных на протокол EAP. При отсутствии ответа в течение определенного промежутка времени процедура идентификации начинается заново. Значение по умолчанию: 2 попытки.

Отображение страницы Port Based Authentication Table (Таблица идентификации на основе портов)

1. Откройте страницу Страница Port Based Authentication (Идентификация на основе портов) .
2. Нажмите кнопку Show All (Показать все).

Откроется страница Port Based Authentication Table:

Рисунок 7-2. Port Based Authentication Table (Таблица идентификации на основе портов)



Кроме полей на странице , страница **Port Based Authentication Table (Таблица идентификации на основе портов)** содержит следующие поля:

Unit No. (Номер устройства) - Выбор компонента стека.

Copy Parameters from Port No. (Скопировать параметры из порта №) - Копирует параметры выбранного порта.

Копирование параметров на странице Port Based Authentication Table (Таблица идентификации на основе портов)

1. Откройте страницу .
2. Нажмите кнопку Show All (Показать все).

Откроется страница **Port Based Authentication Table (Таблица идентификации на основе портов)**.

3. Выберите интерфейс в поле Copy Parameters from Port No. (Скопировать параметры из порта №).
4. Выберите интерфейс в поле **Port Based Authentication Table (Таблица идентификации на основе портов)**.
5. Отметьте флажком поле Copy to (Скопировать в) , чтобы задать интерфейс, в который требуется скопировать параметры идентификации на основе порта.
6. Нажмите кнопку Apply Changes (Применить изменения).

Включение идентификации на основе порта с использованием командной строки.

В следующей таблице перечислены команды для включения идентификации на основе порта, как показано в таблице Страница Port Based Authentication (Идентификация на основе портов) .

Таблица 7-1. Команды страницы Port Authentication

Команды консоли	Описание
aaa authentication dot1x default *method1* [*method2*.]	Определяет один или более методов Идентификации - авторизации - учета (AAA) для использования на интерфейсах, работающих по стандарту IEEE 802.1X.
dot1x max-req *count*	Определяет сколько раз устройство отправляет данные протокола EAP на клиент перед выполнением повторной идентификации.
dot1x re-authenticate [ethernet *interface*]	Вручную включает повоторную идентификацию для всех (или определенных) портов с включением 802.1X.
dot1x re-authentication	Включает периодическую повторную идентификацию клиента.
dot1x timeout quiet-period seconds	Устанавливает количество секунд, в течение которых устройство остается в бездействии после неудачной попытки идентификации.
dot1x timeout re-authperiod *seconds*	Устанавливает промежуток времени в секундах, который проходит перед повторной попыткой идентификации.
dot1x timeout server-timeout *seconds*	Устанавливает время повторной отправки пакетов на сервер идентификации.
dot1x timeout supp-timeout *seconds*	Устанавливает время повторной отправки запроса EAP на клиент.
dot1x timeout tx-period *seconds*	Устанавливает промежуток времени в секундах, в течение которых устройство ожидает ответ EAP с клиента перед тем, как отправить повторный запрос.
show dot1x [ethernet *interface*]	Отображает состояние 802.1X для устройства или определенного интерфейса.
show dot1x users [username username]	Отображает пользователей 802.1X для устройства.
dot1x guest-vlan enable	Включает использование гостевых сетей VLAN для неидентифицированных портов. При включении режима Guest VLAN неидентифицированный порт автоматически подсоединяется к сети VLAN, выбранной в поле VLAN List (Список VLAN). По умолчанию поле отключено.
dot1x guest-vlan	Содержит список сетей VLAN. Гостевая сеть VLAN выбирается из списка VLAN List

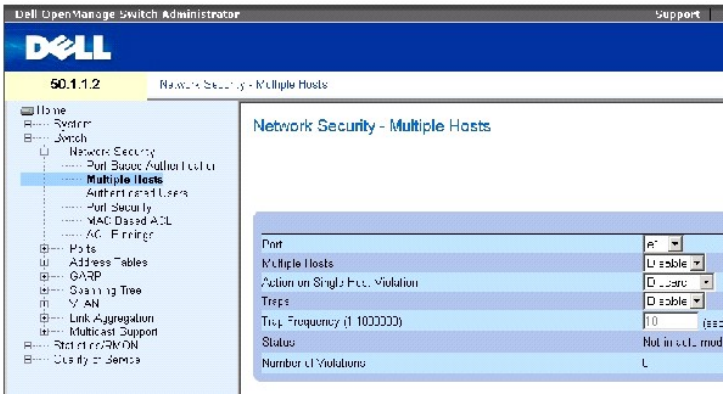
Ниже приведен пример команд консоли:

```
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
```

Конфигурация расширенной идентификации на основе портов

На странице **Multiple Hosts (Множественные хосты)** предоставлена информация по определению расширенной идентификации на основе портов для определенных портов и сетей VLAN. Более подробную информацию по расширенной идентификации на основе портов см. в разделе **Расширенная идентификация на основе портов**. Чтобы открыть страницу **Multiple Hosts (Множественные хосты)**, щелкните Switch (Коммутатор) →Network Security (Безопасность сети) → Multiple Hosts (Множественные хосты).

Рисунок 7-3. Multiple Hosts (Множественные хосты)



На странице **Multiple Hosts (Множественные хосты)** есть следующие поля:

Port (Порт) - Номер порта, для которого включена расширенная идентификация.

Multiple Hosts (Множественные хосты) - Включает или выключает функцию предоставления доступа к системе для нескольких портов по результатам идентификации одного из них. Этот параметр должен быть включен, чтобы отключить входной фильтр или использовать параметры безопасности заблокированных портов для выбранного порта.

Action on Single Host Violation (Действие при нарушении режима одного хоста) - Определяет действие, которое будет применено к пакету, отправленного в режиме идентификации по одному -хосту, с хоста, MAC-адрес которого не является адресом клиента (просителя запроса). Возможные значения поля:

Forward - Пересылает пакеты из неизвестного источника, но MAC-адрес при этом не опознается.

Discard - Игнорирует пакеты от любого неопознанного источника. Это значение по умолчанию.

Shutdown (Завершить работу) - Игнорирует пакеты от любого неопознанного источника и блокирует порт. Порты остаются заблокированными до тех пор, пока они не будут активированы, или коммутатор не будет перезагружен.

Traps (Прерывания) - Включает или отключает отправление прерываний на хост в случае нарушений в работе.

Trap Frequency (1-1000000) (Sec) (Частрота прерываний, в сек.) - Определяет частоту, с которой прерывания отправляются на хост. Значение в поле Trap Frequency (1-1000000) можно задать, только если в поле Multiple Hosts установлено значение Disable. Значение по умолчанию: 10 секунд.

Status - Состояние хоста. Возможные значения поля:

Unauthorized (Несанкционированный) - Указывает, что управление портом находится в режиме *Force Unauthorized*, связь с портом отключена или управление находится в режиме Auto (Автоматический), но клиент на был идентифицирован через порт.

Not in Auto Mode (Не в автоматическом режиме) - Указывает, что управление портом находится в режиме *Forced Authorized (Вынужденно санкционированный)*, а клиент имеет полное право доступа к порту.

Single-host Lock (Блокировка одного порта) - Указывает, что управление портом находится в режиме *Auto (Автоматический)* , и одни клиент был идентифицирован через порт.

No Single Host (Не один хост) - Указывает, что включен режим Multiple Host (Множественные хосты).

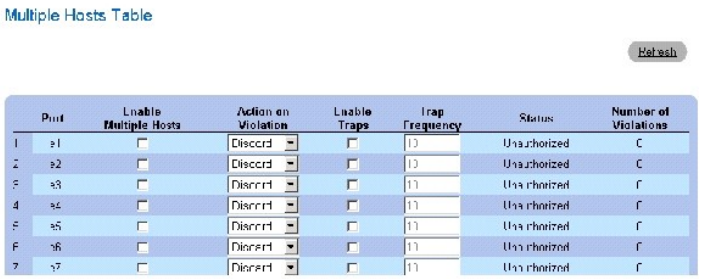
Number of Violations (Количество нарушений) - Количество пакетов, отправленных на интерфейс в режиме идентификации одного хоста, с хоста, MAC-адрес которого не является адресом клиента (просителя запроса).

Отображение таблицы Multiple Hosts Table (Таблица множественных хостов)

1. Откройте страницу **Multiple Hosts (Множественные хосты)**.
2. Нажмите кнопку Show All (Показать все).

Откроется страница **Multiple Hosts Table (Таблица множественных хостов)**.

Рисунок 7-4. Multiple Hosts Table (Таблица множественных хостов)



Включение режима множественных хостов командами консоли

В следующей таблице перечислены команды для включения расширенной идентификации на основе порта, как показано в таблице **Multiple Hosts (Множественные хосты)**.

Таблица 7-2. Команды страницы Multiple Hosts

Команды консоли	Описание
dot1x multiple-hosts	Допускает несколько хостов (клиентов) на порт, авторизированный по стандарту 802.1X, команда конфигурации итерфейса dot1x которого установлена в автоматический режим.
dot1x single-host-violation {forward |discard |discard-shutdown}[trap seconds]	Выполняет действие с системы, MAC-адрес которой не является адресом клиента (подателя запроса), предпринимает попытки доступа к интерфейсу.

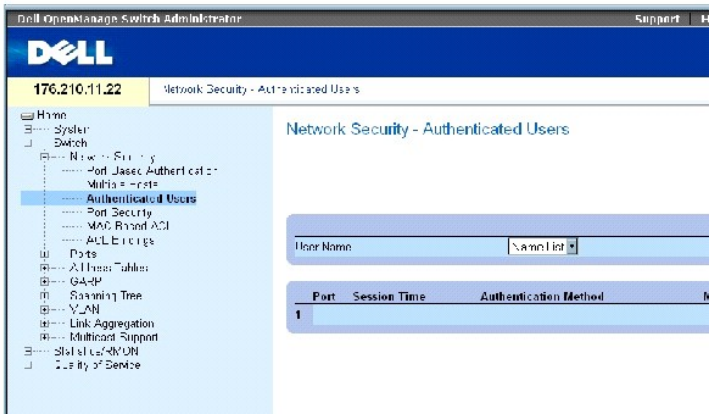
Ниже приведен пример команд консоли:

```
Console(config)# interface
ethernet 1/e1


Console(config-if)# dot1x
multiple-hosts
```

Идентификация пользователей

На странице Authenticated Users (Полномочные пользователи) приводится список доступа пользователей к портам. Списки User Access Lists задаются на странице Add User Name (Добавить имя пользователя) . Чтобы открыть страницу Authenticated Users (Полномочные пользователи), щелкните Switch (Коммутатор) → Network Security (Безопасность сети) → Authenticated Users (Полномочные пользователи).

Рисунок 7-5. Authenticated Users (Полномочные пользователи)



На странице Authenticated Users (Полномочные пользователи) есть следующие поля:

User Name (Имя пользователя) - Список пользователей, идентифицированных через сервер RADIUS.

Port (Порт) - Номер порта, использованного для идентификации, задается для каждого имени пользователя.

Session Time (Время сеанса) - Время с момента входа в систему определенным пользователем. Формат поля: Day:Hour:Minute:Seconds (Дни:Часы:Минуты:Секунды), например, 3 дня: 2 часа: 4 минуты: 39 секунд.

Authentication Method (Метод идентификации) - Метод, с помощью которого был идентифицирован последний сеанс. Возможные значения поля:

Remote (Удаленно) - Пользователь был идентифицирован через удаленный сервер.

None (Нет) - Указывает, что пользователь не был идентифицирован.

MAC Address (MAC-адрес) - С использованием MAC-адреса подателя запроса.

Отображение Authenticated Users Table (Таблица полномочных пользователей)

1. Откройте страницу Authenticated Users (Полномочные пользователи) .
2. Нажмите кнопку Show All (Показать все).

Откроется страница Authenticated Users Table (Таблица полномочных пользователей):

Рисунок 7-6. Authenticated Users Table (Таблица полномочных пользователей)

Идентификация пользователей с помощью командной строки

В следующей таблице приведены команды консоли, соответствующие полям на странице Authenticated Users (Полномочные пользователи).

Таблица 7-3. Команды для добавления имени пользователя

Команды консоли	Описание
show dot1x users [username username]	Отображает пользователей 802.1X для устройства.

Ниже 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 может быть улучшена за счет разрешения доступа к определенному порту только пользователям, имеющим определенные MAC-адреса. MAC-адреса можно узнать динамически или настроить статически. Система защиты заблокированных портов отслеживает как полученные, так и распознанные пакеты, которые пришли на определенные порты. Доступ к заблокированным портам предоставляется только пользователям с определенными MAC-адресами. Эти адреса либо заданы для порта вручную, либо занесены в память порта до того, как он был заблокирован. При получении пакета, исходный MAC-адрес которого не привязан к заблокированному порту (он является неизвестным для системы), на который он отправлен, срабатывает защитный механизм, который предоставляет несколько вариантов действий. Неидентифицированные пакеты, приходящие на заблокированный порт, подвергаются одному из следующих действий:

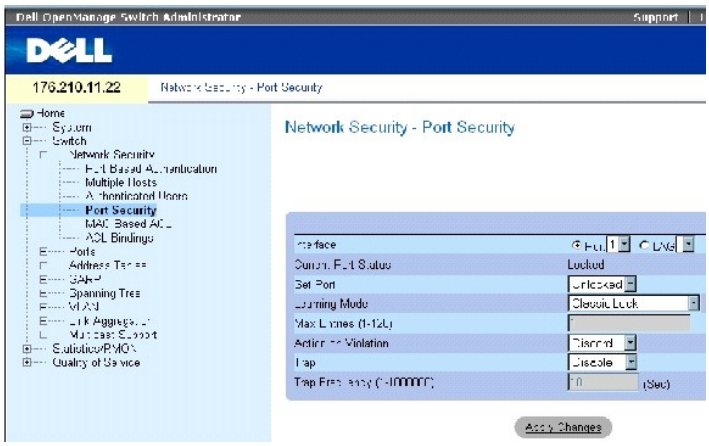
- Пересылаются
- Выбрасываются без системного прерывания
- Выбрасываются с системным прерыванием
- Порт отключается

Система защиты заблокированных портов также позволяет сохранять список MAC-адресов в файле конфигурации. Этот список можно восстановить после перезагрузки устройства.

ПРИМЕЧАНИЕ. Чтобы включить защиту заблокированных портов, включите функцию **Multiple Hosts (Множественные хосты)** на нужных портах.

Отключенные порты активизируются на странице Безопасность портов. На странице Ports (Порты) имеются ссылки для конфигурации функций порта, включая контроль "лавины", механизм зеркалирования портов и возможность их виртуального тестирования. Чтобы открыть страницу Безопасность портов, щелкните Switch (Коммутатор) → Network Security (Безопасность сети) → Port Security (Безопасность портов).

Рисунок 7-7. Безопасность портов



На странице Безопасность портов есть следующие поля:

Interface - Выбранный тип интерфейса, на котором включен заблокированный порт.

Port (Порт) - Указывает, что выбранный тип интерфейса - порт.

LAG - Указывает, что выбранный тип интерфейса - LAG.

Current Port Status - Текущее состояние конфигурации порта.

Set Port - Указывает, заблокирован порт или нет. Возможные значения поля:

Unlocked (Незаблокирован) - Снимает блокировку порта. Это значение по умолчанию.

Locked (Заблокирован) - Блокирует порт.

Learning Mode - Определяет тип заблокированного порта. Поле Learning Mode включается, если выбрано состояние Locked в поле Set Port . Возможны следующие значения поля:

Classic Lock (Классическая блокировка)- Блокирует порт с использованием классического механизма. Порт блокируется моментально, вне зависимости от количества адресов в памяти.

Limited Dynamic Lock (Ограниченная динамическая блокировка) - Блокирует порты, удаляя имеющиеся динамические MAC-адреса, ассоциированные с портом. Порт распознает максимально допустимое количество адресов. Включена функция повторного распознавания MAC-адресов, а также учет их срока действия.

Max Entries (Максимальное количество записей) - Задает количество MAC-адресов, которые будут распознаны для порта. Поле Max Entries (Максимальное количество записей) включается, только если выбран вариант Locked в поле Set Port . Кроме того, выбран режим Limited Dynamic Lock (Ограниченная динамическая блокировка). Значение по умолчанию - 1.

Action on Violation (Действие при нарушении) - Указывает действие, которое выполняется по отношению к пакетам, поступающим на заблокированный порт. Возможные значения поля:

Forward - Пересылает пакеты из неизвестного источника, но MAC-адрес при этом не опознается.

Discard - Игнорирует пакеты от любого неопознанного источника. Это значение по умолчанию.

Shutdown (Завершить работу) - Игнорирует пакеты от любого неопознанного источника и блокирует порт. Порты остаются заблокированными до тех пор, пока они не будут повторно активированы, или коммутатор не будет перезагружен.

Trap (Прерывание) - Включает отправку системных прерываний при получении пакета на заблокированном порте.

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 **Безопасность портов**.
2. Выберите тип и номер интерфейса.
3. Определите поля.
4. Нажмите кнопку Apply Changes (Применить изменения).

Порт будет добавлен в **Port Security Table (Табл. безопасности портов)**, а устройство обновлено.

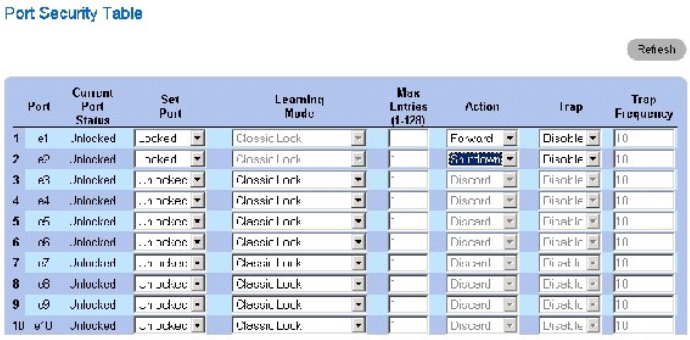
Вывод таблицы Port Security Table

1. Откройте страницу **Безопасность портов**.
2. Нажмите кнопку Show All (Показать все).

Откроется страница **Port Security Table (Табл. безопасности портов)**.

ПРИМЕЧАНИЕ. Заблокированные порты определены в **Port Security Table (Табл. безопасности портов)**.

Рисунок 7-8. Port Security Table (Табл. безопасности портов)



На странице **Port Security Table (Табл. безопасности портов)** есть следующие поля:

Unit No. (Номер устройства). - Номер стекового устройства, для которого выводится информация о заблокированном порте.

Copy Parameters from (Копировать из) - Копирует параметры в выбранный порт.

Настройка безопасности заблокированных портов с помощью команд консоли

В следующей таблице приведены команды консоли, соответствующие полям страницы для настройки безопасности заблокированных портов.

Таблица 7-4. Команды страницы Port Security

Команды консоли	Описание
shutdown	Отключает интерфейсы.
set interface active {ethernet interface | port-channel port-channel-number}	Вновь активизирует интерфейс, отключенный по причинам безопасности порта.
port security learning {disabled | dynamic}	Определяет тип блокировки порта.
port security max max-addr	Задает количество MAC-адресов, которые будут распознаны для порта.
port security [forward | discard | discard-shutdown] [trap seconds]	Блокирует функцию опознавания новых адресов для интерфейса.
show ports security {ethernet interface | port-channel port-channel-number}	Выводит состояние блокировки для порта.

Ниже 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	-	-	-	-

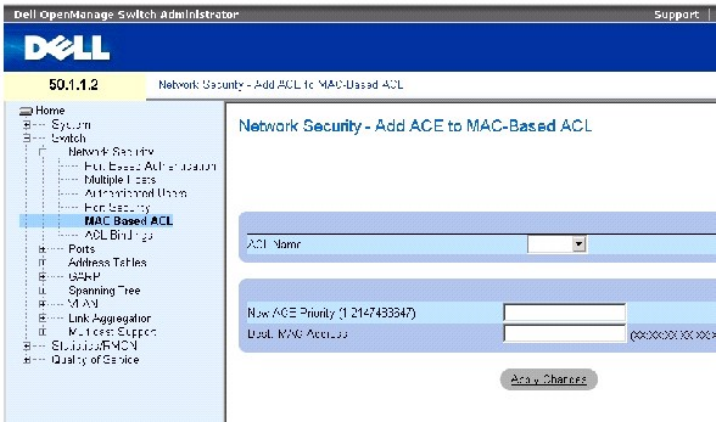
Определение ACL, основанных на MAC-адресах

Списки управления доступом Access Control Lists (ACL) позволяют менеджерам сети определять классификационные действия и правила для определнных входных портов. Списки ACL содержат множество классификационных правил и действий. Каждое классификационное правило и действие - это запись управления доступом, Access Control Element (ACE). Записи ACE - это фильтры, определяющие классификации трафиков. ACL, основанные на MAC-адресах, применяются к любым пакетам, включая те, которые не базируются на IP. Поля классификации основаны только на полях L2.

Страница Список ACL на основе MAC-адресов позволяет определяить ACL, основанные на MAC-адресах. Определение ACL дано в разделе "Определение ACL, основанных на MAC-адресах."

Чтобы открыть страницу Список ACL на основе MAC-адресов, щелкните **Switch (Коммутатор)→ Network Security (Безопасность сети) →MAC based ACL (Списки ACL на основе MAC-адресов)**.

Рисунок 7-9. Список ACL на основе MAC-адресов



На странице Список ACL на основе MAC-адресов есть следующие поля:

ACL Name (Имя ACL) - Пользовательский список ACL.

New ACE Priority (1-2147483647) (Навый приоритетACE) - Индекс правила ACE в поле ACL.

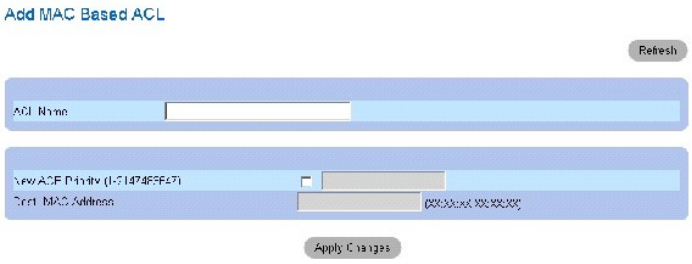
Destination MAC Address (MAC-адрес источника) - Сравнивает MAC-адрес приемника, на который адресуются пакеты, с записью ACE.

Добавление списка ACL на основе MAC-адресов:

1. Откройте страницу Список ACL на основе MAC-адресов .
2. Нажмите кнопку **Add** (Добавить).

Откроется страница Добавление ACL, основанных на MAC-адресах .

Рисунок 7-10. Добавление ACL, основанных на MAC-адресах



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

Список ACL, основанный на MAC-адресах, будет определен, а устройство обновлено.

Вывод записей ACE для указанных ACL:

1. Откройте страницу Список ACL на основе MAC-адресов .
2. Выберите ACL.
3. Нажмите кнопку **Show All** (Показать все).

Откроется страница **ACEs Associated with MAC ACL** (Записи ACE, связанные с ACL, основанным на MAC-адресах).

Удаление списков ACL

1. Откройте страницу Список ACL на основе MAC-адресов.

ПРИМЕЧАНИЕ. Списки ACL можно удалить при условии, что они не привязаны к интерфейсу.

2. Выберите ACL.
3. Нажмите кнопку **Show All** (Показать все).

Откроется страница **ACEs Associated with MAC ACL** (Записи ACE, связанные с ACL, основанным на MAC-адресах).

4. Установите флажок **Remove ACL** (Удалить ACL).

Назначение записей ACE, основанных на MAC-адресах, для списков ACL с помощью команд консоли

В следующей таблице перечислены команды для назначения ACE, основанного на MAC-адресе, для списков ACL как показано в таблице Список ACL на основе MAC-адресов.

Таблица 7-5. Команды страницы MAC-Based ACE

Команды консоли	Описание
`mac access-list;`	Создает списки ACL, основанные на MAC-адресах, на уровне 2 и включает режим настройки списка доступа, основанного на MAC-адресах.
`deny destination`	Запрещает трафик, если соблюдены условия, определенные в операторе MAC based ACL.
`show access-lists [name]`	Отображает списки ACL, определенные в устройстве.

Ниже приведен пример команд консоли:

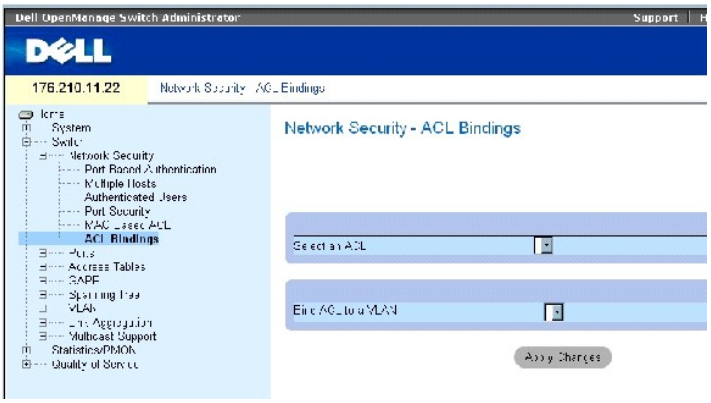
```
console (config)# mac access-list dell
```

```
console (config-mac-al)# deny 00-10-B5-F4-00-01
```

Конфигурация привязки ACL

Если список ACL привязан к интерфейсу, он применяется для данного интерфейса. Используйте страницу Привязки ACL, чтобы назначить списки ACL для методов классификации и интерфейсов. Чтобы открыть страницу Привязки ACL, щелкните **Switch (Коммутатор)**→ **Network Security (Безопасность сети)** →**ACL Binding (Привязка ACL)**.

Рисунок 7-11. Привязки ACL



На странице Привязки ACL есть следующие поля:

Select an ACL (Выбор ACL) - Тип списка ACL, с которым сравниваются входящие пакеты.

Bind ACL to VLAN (Привязка ACL к VLAN) - Сеть VLAN, с которой связан список ACL.

Назначение списка ACL для интерфейса

1. Откройте страницу Привязки ACL.
2. Выберите тип ACL в поле **Select an ACL (Выбор ACL)** .
3. Выберите сеть VLAN, с которой связан список ACL, в поле**Bind ACL to an VLAN (Привязка ACL к VLAN)** .
4. Нажмите кнопку **Apply Changes (Применить изменения)**.

Список ACL будет привязан к интерфейсу.

Удаление записи из таблицы ACL Bindings Table

1. Откройте страницу Привязки ACL.
2. Нажмите кнопку **Show All (Показать все)**.

Откроется страница **ACL Bindings Table (Таблица привязок ACL)**.

3. Отметьте флажком поле **Remove (Удалить)** той записи, которую хотите удалить.
4. Нажмите кнопку **Apply Changes (Применить изменения)**.

Запись удалена из таблицы, а устройство обновлено.

Отображение таблицы ACL Bindings Table

1. Откройте страницу Привязки ACL.
2. Нажмите кнопку **Show All (Показать все)**, чтобы открыть страницу **ACL Bindings Table (Таблица привязок ACL)**.

Поля страницы **ACL Bindings Table (Таблица привязок ACL)** такие же, как на странице **ACL Bindings (Привязки ACL)** .

Копирование параметров в таблицу ACL Bindings Table.

1. Откройте страницу Привязки ACL.

2. Нажмите кнопку **Show All (Показать все)**.

   Откроется страница **ACL Bindings Table (Таблица привязок ACL)**.

3. Выберите интерфейс в поле **Copy Parameters from (Копировать параметры из).**
4. Выберите в раскрывающемся списке **VLAN** сеть VLAN.

   Определения этого интерфейса копируются в выбранные порты/транки.

5. Отметьте флажком поле **Copy to (Копировать в)** той записи, которую хотите изменить, или чтобы скопировать определения на все порты/транки.
6. Нажмите кнопку **Select All (Выбрать все)**.
7. Нажмите кнопку **Apply Changes (Применить изменения)**.

   Параметры копируются в порты/транки в таблице *ACL Bindings Table*, а устройство обновляется.

Назначение членства в ACL с помощью команд консоли

В следующей таблице приведены команды консоли, соответствующие действиям по назначению членства в ACL страницы **ACL Binding** (Привязки ACL).

Таблица 7-6. Команды страницы ACL Binding

Команды консоли	Описание
`service-acl {input` *`acl-name`*`}`	Применяет список доступа на вход интерфейса.

Ниже приведен пример команд консоли:

```
console(config)# interface vlan 123
```

```
console(config-if)# service-acl input dell
```

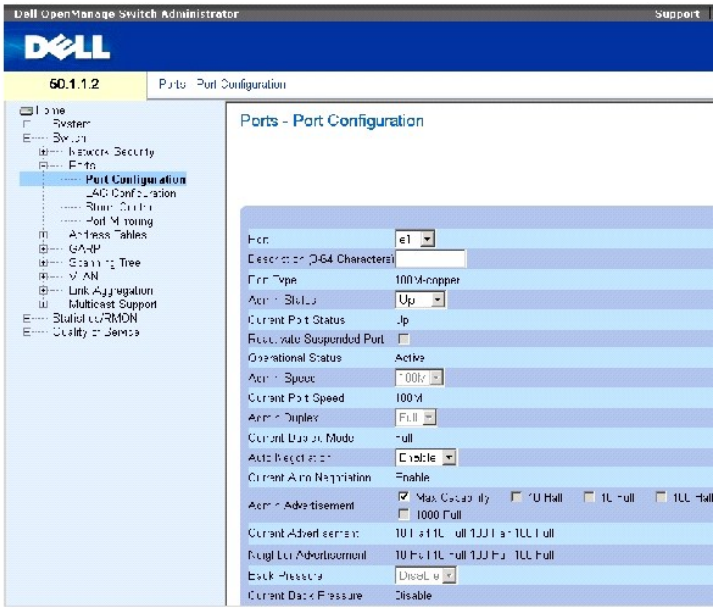
Настройка портов

На странице **Ports (Порты)** имеются ссылки для конфигурации функций порта, включая контроль "лавины", механизм зеркалирования портов и возможность их виртуального тестирования. Чтобы открыть страницу **Ports (Порты)** , выберите **Switch (Коммутатор)** → **Ports (Порты)**.

Определение конфигурации порта

Для определения параметров порта используйте страницу **Конфигурация порта**. Если конфигурация порта изменяется, пока он является членом группы LAG, изменения вступают в действие только после удаления порта из этой группы. Чтобы открыть страницу **Конфигурация порта**, **Switch (Коммутатор)** → **Ports (Порты)** → **Port Configuration (Конфигурация порта)** в панели дерева.

Рисунок 7-12. Конфигурация порта



На странице **Конфигурация порта** есть следующие поля:

Port (Порт) - Номер порта, для которого определяются параметры.

Description (0 - 64 Characters) (Описание, 0-64 символа)- Краткое описание интерфейса, например, Ethernet.

Port Type (Тип порта) - Указывает тип порта.

Admin Status (Состояние администрирования) - Включение или выключение пересылки трафика через порт.

Current Port Status (Текущее состояние порта) - Определяет, является ли порт в настоящее время рабочим или нет.

Reactivate Suspended Port (Восстановить заблокированный порт) - Вновь активизирует порт, если он был отключен параметрами безопасности.

Operational Status (Рабочее состояние) - Индикация рабочего состояния порта. Возможные значения поля:

Suspended (Приостановлен) - Порт в настоящее время активен, но не осуществляет пересылку и прием трафика.

Active (Активен) - Порт в настоящее время активен и осуществляет пересылку и прием трафика.

Disable (Выключен) - Порт в настоящее время выключен и, следовательно, не осуществляет прием и пересылку трафик.

Admin Speed (Скорость администрирования) - Скорость, заданная для данного порта. Доступные параметры скорости зависят от типа порта. Параметр "Admin Speed" можно использовать только тогда, когда порт отключен.

Current Port Speed (Текущая скорость порта) - Указывает скорость синхронизированного порта (в битах в секунду).

Admin Duplex (Администрирование дуплексного режима) - Отображает дуплексный режим порта (в битах в секунду). **Full** (Дуплексный) - Интерфейс поддерживает передачу между устройством и клиентом в двух направлениях одновременно. **Half** (Полудуплексный) - Интерфейс поддерживает передачу между устройством и клиентом только в одном направлении в одно время.

Current Duplex Mode - Текущий дуплексный режим синхронизированного порта.

Auto Negotiation (Автосогласование) - Включение автоматического согласования для порта. Автоматическое согласование - это протокол между двумя партнерами по связи, который позволяет порту оповестить партнера по связи о своей скорости передачи, возможности работы в дуплексном режиме и управления потоком.

Current Auto Negotiation - Текущая настройка автоматического согласования.

Admin Advertisement (Оповещение администрирования) - Определяет настройку автоматического согласования, которую сообщает порт. Возможные значения поля:

Max Capability (Максимальная скорость) -Указывает, что приемлемы все значения скорости порта и настройка дуплексного режима.

10 Half - Указывает, что порт заявляет скорость порта 10 Мб/с и параметры полудуплексного режима.

10 Full - Указывает, что порт заявляет скорость порта 10 Мб/с и параметры полного дуплексного режима.

100 Half - Указывает, что порт заявляет скорость порта 100 Мб/с и параметры полудуплексного режима.

100 Full - Указывает, что порт заявляет скорость порта 100 Мб/с и параметры полного дуплексного режима.

1000 Full - Указывает, что порт заявляет скорость порта 1000 Мб/с и параметры полного дуплексного режима.

Current Advertisement (Текущее оповещение) - Порт объявляет свою скорость для соседних портов, чтобы начать процесс согласования. Возможные значения поля заданы в поле Admin Advertisement.

Neighbor Advertisement (Оповещение соседних портов) - Указывает заявленные параметры соседних портов. Значения полей идентичны тем, которые заданы в поле **Admin Advertisement**.

Back Pressure - Включает режим обратного давления на устройстве. Режим обратного давления используется с полудуплексным режимом, чтобы отключить функцию получения сообщений для портов. Режим обратного давления не поддерживается в портах OOB.

Current Back Pressure - Настройки текущего обратного давления.

Flow Control (Управление потоком) - Включает или отключает управление потоком или включает автоматическое согласование управления потоком для порта.

Current Flow Control - Текущая настройка управления потоком.

MDI/MDIX - Позволяет устройству различать перекрестный и неперекрестный кабель. В концентраторах и коммутаторах специально используется схема подключения проводов, отличная от схемы на конечных станциях. Поэтому при подключении концентратора или коммутатора к конечной станции можно использовать соединение напрямую кабелем Ethernet, так как провода совпадают. При соединении двух концентраторов/коммутаторов или двух конечных станций используют перекрестный кабель, чтобы соединить правильные пары. Функция автоматического выбора MDIX не работает на портах FE, если автоматическое согласование отключено. Возможные значения поля :

Auto (Автоматически) - Автоматическое определение типа кабеля.

MDIX - Ипользуется для концентраторов и коммутаторов.

MDI - Используется для оконечных систем.

Current MDI/MDIX - Указывает текущие параметры устройства MDIX. Возможные значения поля:

MDI - Текущий параметр MDI - MDI.

MDIX - Текущий параметр MDI - MDIX.

LAG - Указывает, что порт входит в состав LAG.

ПРИМЕЧАНИЕ. Если конфигурация порта изменяется, пока он является членом группы LAG, изменения вступают в действие только после удаления порта из этой группы.

Определение параметров порта

1. Откройте страницу **Конфигурация порта**.
2. Выберите порт в поле Port (Порт).
3. Определите поля в диалоговом окне.
4. Нажмите кнопку Apply Changes (Применить изменения).

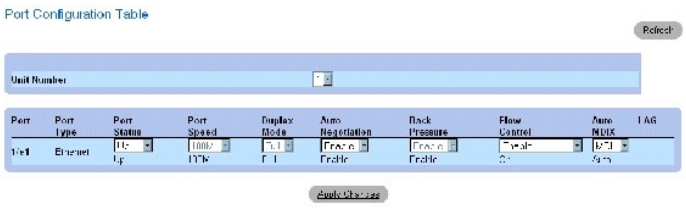
Параметры порта будут сохранены для этого устройства.

Вывод таблицы Port Table

1. Откройте страницу **Конфигурация порта**.
2. Нажмите кнопку **Show All** (Показать все).

Откроется **Port Configuration Table** (Таблица настройки портов).

Рисунок 7-13. Таблица Port Configuration Table



Настройка портов с помощью команд консоли

В следующей таблице приведены команды консоли, соответствующие конфигурации портов на странице Конфигурация порта .

Таблица 7-7. Команды страницы Port Configuration

Команды консоли	**Описание**
interface ethernet *интерфейс*	Включает режим настройки интерфейса для настройки Ethernet в качестве типа интерфейса.
description *строка*	Добавляет описание к конфигурации интерфейса.
shutdown	Выключает интерфейсы, которые входят в состав текущего заданного контекста.
set interface active {ethernet *interface* | port-channel *port-channel-number*}	Вновь активизирует интерфейс, отключенный по причинам безопасности.
speed *Mbps*	Настраивает скорость данного интерфейса Ethernet, если не используется автоматическое согласование.
duplex {half | full}	Настраивает дуплексный или полудуплексный режим для данного 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 *interface* |port-channel *port-channel-number*]	Отображает конфигурацию для всех настроенных интерфейсов.
show interface advertise	Показывает заявленные параметры согласования интерфейса.
show interfaces status [ethernet *interface* | port-channel *port-channel-number*]	Отображает состояние для всех настроенных интерфейсов.
show interfaces description [ethernet *interface* | port-channel *port-channel-number*]	Отображает описание для всех настроенных интерфейсов.

Ниже 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	Mdix Mode
----	----	------	-----	----	------	-----	------	----
1/e3	100	Full	100	Auto	On	Up	Enable	On
1/e4	100	Full	1000	Off	Off	Up	Disable	On

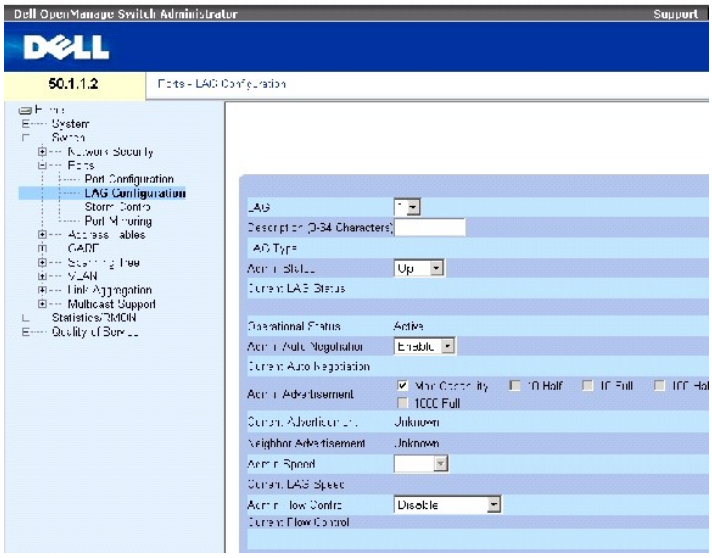
Ch	Type	Duplex	Speed	Neg	Flow Control	Back Pressure	Link State	
---	----	------	-----	-----	-------	--------	------	
1	1000	Full	1000	Off	Off	Disable	Up	

Определение параметров LAG

На странице **Конфигурация LAG** имеются поля для конфигурации параметров настроенных групп LAG. Коммутатор поддерживает до 8 портов на группу LAG и до 8 групп LAG на систему. Подробнее о объединенных группах каналов (Link Aggregated Groups, LAG) и назначении портов в эти группы см. в разделе **Объединение портов**.

Чтобы открыть страницу **Конфигурация порта**, щелкните Switch (Коммутатор) → Ports (Порты) → LAG Configuration (Конфигурация LAG) в панели дерева.

Рисунок 7-14. Конфигурация LAG



На странице **Конфигурация LAG** есть следующие поля:

LAG - Номер группы LAG.

Description (0 - 64 Characters) (Описание, 0-64 символа) - Пользовательское описание настроенной группы LAG.

LAG Type (Тип LAG) - Типы портов, интегрированных в группу LAG.

Admin Status (Состояние администрирования) - Включает или отключает выбранную группу LAG.

Current LAG Status (Текущее состояние LAG) - Указывает, работает ли группа LAG в настоящий момент.

Admin Status (Рабочее состояние) - Включение или выключение пересылки трафика через выбранную группу.

Admin Auto Negotiation (Администрирование автоматического согласования) - Включает или выключает автоматическое согласование для группы LAG. Автоматическое согласование - это протокол между двумя партнерами по связи, который позволяет группе LAG оповестить партнера по связи о своей скорости передачи, возможности работы в дуплексном режиме и управлении потоком (управление потоком по умолчанию выключено).

Current Auto Negotiation - Текущая настройка автоматического согласования.

Admin Advertisement (Оповещение администрирования) - Определяет настройку автоматического согласования, которую сообщает LAG. Возможные значения поля:

Max Capability (Максимальная скорость) -Указывает, что приемлемы все значения скорости LAG и настройка дуплексного режима.

10 Half - Указывает, что LAG заявляет скорость 10 Мб/с и параметры полудуплексного режима.

10 Full - Указывает, что LAG заявляет скорость 10 Мб/с и параметры полного дуплексного режима.

100 Half - Указывает, что LAG заявляет скорость 100 Мб/с и параметры полудуплексного режима.

100 Full - Указывает, что LAG заявляет скорость 100 Мб/с и параметры полного дуплексного режима.

1000 Full - Указывает, что LAG заявляет скорость 1000 Мб/с и параметры полного дуплексного режима.

Current Advertisement (Текущее оповещение) - LAG объявляет свою скорость для соседних LAG, чтобы начать процесс согласования. Возможные значения поля заданы в поле Admin Advertisement.

Neighbor Advertisement (Оповещение соседних портов) - Указывает заявленные параметры соседних LAG. Значения полей идентичны тем, которые заданы в поле **Admin Advertisement**.

Admin Speed (Администрирования скорости) - Указывает скорость, на которой работает LAG.

Current LAG Speed (Текущая скорость LAG) - Указывает скорость, на которой работает LAG.

Admin Flow Control (Управление потоком) - Включает или отключает управление потоком или включает автоматическое согласование управления потоком для LAG. Режим управления потоком (Flow Control) эффективен, когда порты, входящие в LAG, работают в полном дуплексном режиме.

Current Flow Control - Пользовательская настройка управления потоком.

Определение параметров LAG

1. Откройте страницу **Конфигурация 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 LAG

1. Откройте страницу **Конфигурация LAG**.
2. Выберите группу LAG в поле **LAG**.
3. Внесите изменения в соответствующие поля.
4. Нажмите кнопку **Apply Changes (Применить изменения)**.

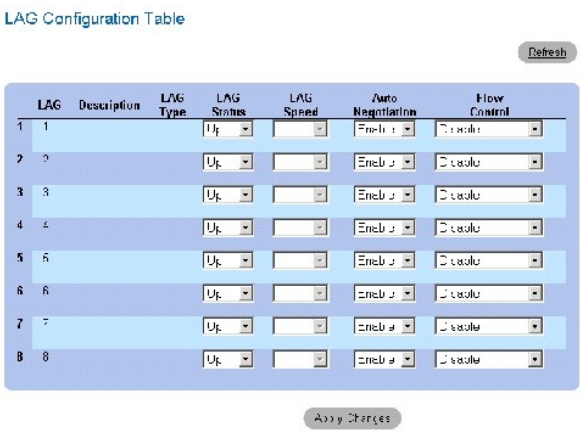
Параметры группы LAG будут сохранены для этого устройства.

Вывод таблицы настройки LAG:

1. Откройте страницу **Конфигурация LAG**.
2. Нажмите кнопку **Show All** (Показать все).

Откроется страница **Таблица LAG Configuration Table**.

Рисунок 7-15. Таблица LAG Configuration Table



Настройка групп LAG с помощью команд консоли

В следующей таблице приведены команды консоли, соответствующие конфигурации LAG на странице **Конфигурация LAG** .

Таблица 7-8. Команды страницы LAG Configuration

Команды консоли	Описание
interface port-channel *номер_канала_порта*	Вводит режим конфигурации интерфейса определенного порта-канала.
description *строка*	Добавляет описание к конфигурации интерфейса.
shutdown	Выключает интерфейсы, которые входят в состав текущего заданного контекста.
speed *bps*	Настраивает скорость данного интерфейса Ethernet, если не используется автоматическое согласование.
negotiation [capability1 [capability2...capability5]	Включает автоматическое согласование для 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** *interface* |**port-channel** *port-channel-number*]	Отображает конфигурацию для всех настроенных интерфейсов.
show interfaces status [**ethernet** *interface* | **port-channel** *port-channel-number*]	Отображает состояние для всех настроенных интерфейсов.
show interfaces description [**ethernet** *interface* |**port-channel** *port-channel-number*]	Отображает описание для всех настроенных интерфейсов.
show interfaces port-channel [*port-channel-number*]	Выводит сведения о канале порта (какие порты входят в канал порта, активны они на данный момент или нет).

Ниже 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 поступивших по сети на один порт. Ответы на пересылаемые сообщения загружаются в сеть, уменьшая ее ресурсы или вызывая простой сети.

Контроль "лавины" включается для всех портов путем определения типа пакета и частоты передачи пакетов.

Система измеряет частоту входящих кадров (широковещательных, одноадресных и многоадресных) отдельно на каждом порте и игнорирует кадры, когда частота превосходит частоту, заданную пользователем.

На странице **Контроль "лавины"** представлены поля для включения и настройки контроля "лавины". Чтобы открыть страницу **Контроль "лавины"**, щелкните Switch (Коммутатор) → Ports (Порты) → Storm Control (Контроль "лавины") в панели дерева.

Рисунок 7-16. Контроль "лавины"

На странице **Контроль "лавины"** есть следующие поля:

Port (Порт). Порт, на котором включен контроль "лавины".

Broadcast Control (Контроль широковещательных пакетов). Включение или отключение пересылки типов широковещательных пакетов на определенном интерфейсе.

Broadcast Mode (Режим трансляции) - Определяет, что в устройстве или стеке включен режим трансляции. Возможные значения поля:

Unknown Unicast, Multicast & Broadcast - Учитывает однонаправленный, многоадресный и широковещательный трафики.

Multicast & Broadcast - Учитывает объединенные многоадресные и широковещательные трафики.

Broadcast Only - Учитывает только широковещательный трафик.

Broadcast Rate Threshold (70-285000) (Порог частоты широковещательных пакетов) - Максимальное значение скорости (в килобайтах в секунду), с которой передаются неизвестные пакеты. Значение поля: 70-285000 килобайт в секунду.

Включение контроля "лавины"

1. Откройте страницу **Контроль "лавины"**.
2. Выберите интерфейс, для которого хотите реализовать контроль "лавины".
3. Определите поля.
4. Нажмите кнопку **Apply Changes (Применить изменения)**.

Контроль "лавины" включен.

Изменение параметров порта с контролем "лавины"

1. Откройте страницу **Контроль "лавины"**.
2. Внесите изменения в соответствующие поля.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

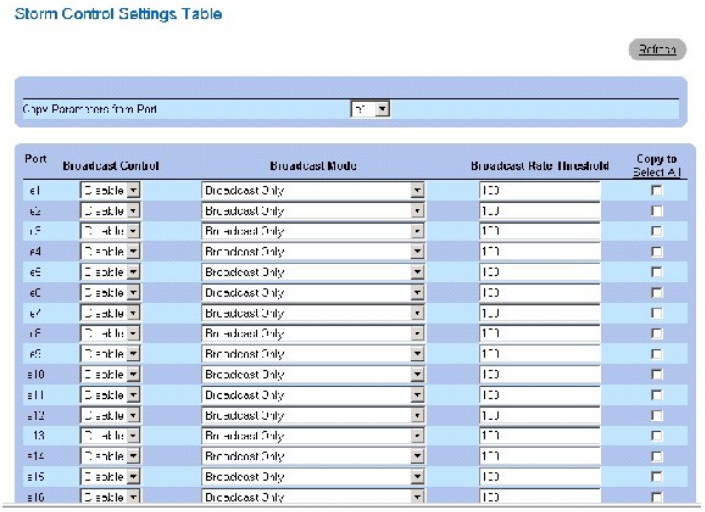
Параметры контроля "лавины" порта будут сохранены для этого устройства.

Вывод таблицы Port Parameters Table

1. Откройте страницу **Контроль "лавины"**.
2. Нажмите кнопку **Show All** (Показать все).

Откроется страница **Таблица Storm Control Settings Table**.

Рисунок 7-17. Таблица Storm Control Settings Table



Кроме полей на странице **Контроль "лавины"**, страница **Таблица Storm Control Settings Table** содержит следующие поля:

Copy Parameters from Port (Скопировать параметры из порта) - Указывает порт, из которого копируются параметры контроля "лавины".

Копирование параметров в таблицу Storm Control Settings Table

1. Откройте страницу **Контроль "лавины"**.
2. Нажмите кнопку **Show All** (Показать все).

Откроется страница **Таблица Storm Control Settings Table**.

3. Выберите порт, параметры которого хотите скопировать, из поля **Copy Parameters from Port (Скопировать параметры из порта)**.
4. Отметьте флажком поле **Copy to (Копировать в)** того интерфейса, в который хотите скопировать параметры контроля "лавины", или нажмите кнопку **Select All (Выбрать все)**, чтобы скопировать параметры во все порты.
5. Нажмите кнопку **Apply Changes (Применить изменения)**.

Параметры копируются в порты в таблице **Storm Control Settings Table**, а устройство обновляется.

Настройка контроля "лавины" с помощью команд консоли

В следующей таблице приведены команды консоли, соответствующие конфигурации контроля "лавины" на странице **Контроль "лавины"** .

Таблица 7-9. Команды страницы Storm Control

Команды консоли	Описание
	Включает общий подсчет многоадресных, однонаправленных и широковещательных пакетов.

`port storm-control include-multicast`	
`port storm-control broadcast enable`	Включает контроль широковещательной "лавины".
`port storm-control broadcast rate`	Настраивает максимальную частоту для широковещательных пакетов.
`show ports storm-control` *port*	Отображает конфигурацию контроля "лавины".

Ниже 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 портов:

- Контролирует и дублирует сетевой трафик путем пересылки копий входящих и исходящих пакетов с одного порта на другой (дублирующий).
- Зеркалирование портов можно использовать как средство диагностики и отладки.
- Оно включает характеристики устройства и мониторинг.

Зеркалирование портов можно настраивать путем выбора определенного порта для копирования всех пакетов и различных портов, с которых пакеты копируются.

Перед настройкой зеркалирования портов, учтите следующее:

- Зеркалирование портов контролирует и дублирует сетевой трафик путем пересылки копий входящих и исходящих пакетов с контролируемого порта на дублирующий.
- Контролируемые порты не могут работать быстрее, чем контролирующие.
- Все пакеты RX/TX должны контролироваться на одном порте.

К портам, настроенным как порты-приемники, применяются следующие ограничения:

- Порты нельзя настроить в качестве портов-источников.
- Порт не может входить в группу LAG.
- На этих портах не настроены интерфейсы IP.
- На этих портах не включен протокол GVRP.
- Порт не входит в сеть VLAN.
- Можно определить только один порт-приемник.

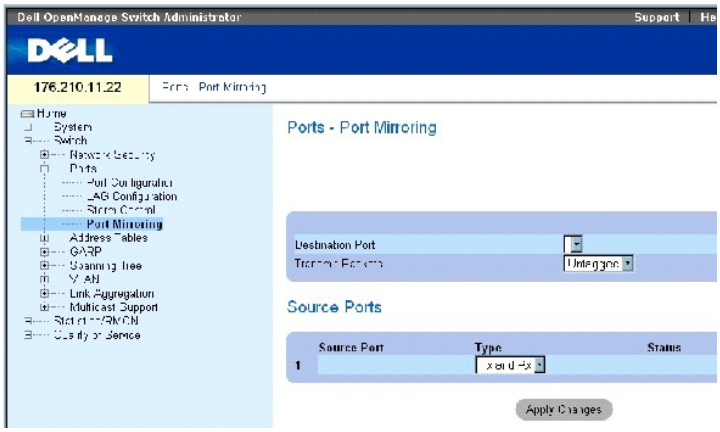
К портам, настроенным как порты-источники, применяются следующие ограничения:

- Порты-источники не могут входить в группу LAG.
- Порты нельзя настроить в качестве портов-приемников.
- Поддерживается до 8 портов-источников.

Чтобы открыть страницу **Зеркалирование портов**, щелкните **Switch (Коммутатор)** → **Ports (Порты)** → **Port Mirroring (Зеркалирование порта)** в панели дерева.

ПРИМЕЧАНИЕ. Если порт задан в качестве целевого порта для сеанса с зеркалированием портов, все обычные операции на этом порте заморожены Это касается протоколов STP и LACP.

Рисунок 7-18. Зеркалирование портов



На странице **Зеркалирование портов** **есть следующие поля:**

Destination Port (Порт-приемник). Назначение номера порта, на который копируется трафик.

Transmit Packets (Передача пакетов) - Определяет способ зеркалирования пакетов. Возможные значения поля:

Untagged (Непомеченные) - Пакеты зеркалируются как непомеченные пакеты сети vlan. Это значение по умолчанию.

Tagged (Помеченные) - Пакеты зеркалируются как помеченные пакеты сети vlan.

Type (Тип). Определение типа зеркалируемого пакета: RX, TX или RX и TX одновременно.

Status (Состояние). Указывает, выполняется ли в настоящее время мониторинг (**Active**) или нет (**Ready**).

Remove (Удалить) - Если выбрано, сеанс зеркалирования порта удаляется.

Добавление сеанса с зеркалированием портов

1. Откройте страницу Зеркалирование портов.
2. Нажмите кнопку **Add** (Добавить).

   Откроется страница **Add Source Port** (Добавление порта-источника).
3. Определите поля **Source Port** (Порт-источник) и **Type** (Тип).
4. Нажмите кнопку **Apply Changes (Применить изменения)**.
5. Выберите порт-приемник из раскрывающегося меню **Destination Port (Порт-приемник)**.
6. Нажмите кнопку **Refresh** (Обновить). Зеркалирование портов
7. Определите поле **Tagged Packets (Помеченные пакеты)**.
8. Определите поле **Type (Тип)** .
9. Нажмите кнопку **Apply Changes (Применить изменения)**.

   Новый порт-источник будет определен, а устройство обновлено.

Удаление дублирующего порта из сеанса с зеркалированием портов:

1. Откройте страницу Зеркалирование портов.
2. 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 для настройки сеанса с зеркалированием портов, как показано на странице Зеркалирование портов.

Таблица 7-10. Команды страницы Port Mirroring

Команды консоли	Описание
port monitor *src*-interface [**rx** | **tx**]	Запускает сеанс с зеркалированием портов.

Ниже 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

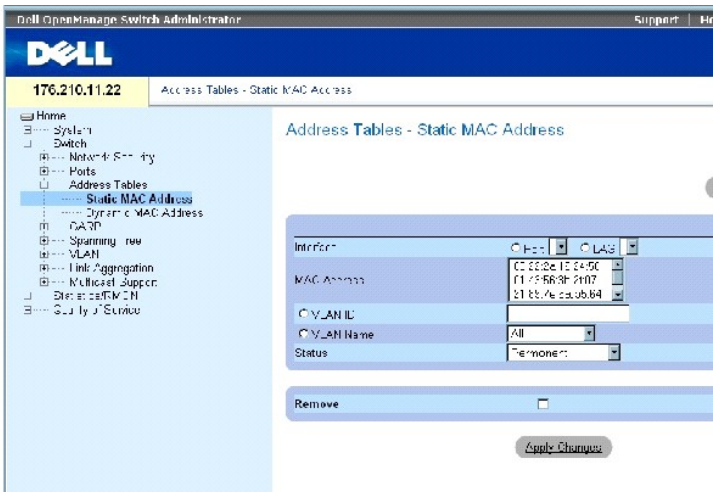
Настройка адресных таблиц

MAC-адреса хранятся в базах данных статических или динамических адресов. Пакет, адресованный приемнику, хранящемуся в одной из баз данных, немедленно пересылается на порт. Таблицы динамических адресов могут быть отсортированы по интерфейсу, VLAN и MAC-адресу. MAC-адреса опознаются динамически по мере прибытия пакетов на коммутатор. Адреса связываются с портами путем опознавания портов из исходного адреса кадра. 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 избежать переполнения таблицы связей моста, динамические MAC-адреса стираются, если в течение определенного времени на них ничего не передается. Чтобы открыть страницу Address Tables (Адресные таблицы) , нажмите Switch (Коммутатор) → Address Tables (Адресные таблицы) в панели дерева.

Определение статических адресов

На странице Таблица Static MAC Address Table приведен список всех статических MAC-адресов. Статические адреса можно добавлять и удалять со страницы Таблица Static MAC Address Table. Кроме того, можно определить несколько MAC-адресов для одного порта. Чтобы открыть страницу Таблица Static MAC Address Table, щелкните Switch (Коммутатор) → Address Tables (Адресные таблицы) →Static Address Table (Статические адресные таблицы) в панели дерева.

Рисунок 7-19. Таблица Static MAC Address Table



На странице Таблица Static MAC Address Table есть следующие поля:

Interface (Интерфейс) - Определенный порт или группа LAG, к которым применяется статический MAC-адрес.

MAC Address - MAC-адрес, приведенный в списке Current Static Addresses List (Список текущих статических адресов).

VLAN ID - Идентификатор сети VLAN, прикрепленный к MAC.

VLAN Name - Имя сети VLAN, задаваемое пользователем.

Status - Состояние MAC-адреса. Возможные значения поля:

Secure (Надежный) - Используется для определения статических MAC-адресов для заблокированных портов.

Permanent (Постоянный) - MAC-адрес является постоянным.

Delete on Reset (Удаляется при перезагрузке) - Указывает, что MAC удаляется при перезагрузке устройства.

Delete on Timeout (Удаляется при паузе ожидания) - MAC-адрес удаляется, если возникает пауза ожидания.

ПРИМЕЧАНИЕ. Чтобы избежать удаления статических адресов MAC при перегрузке устройства Ethernet, убедитесь, что порт, связанный с MAC-адресом, заблокирован.

Remove (Удалить) - Если это поле выбрано, указанные MAC-адреса удаляются из таблицы MAC Address Table.

Добавление статических MAC-адресов

1. Откройте страницу Таблица Static MAC Address Table.
2. Нажмите кнопку **Add** (Добавить).

Откроется страница **Add Static MAC Address**(Добавить статический MAC-адрес).

3. Заполните поля.

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

Новый статический адрес будет добавлен в **таблицу статических адресов**, а устройство обновлено.

Изменение параметров статических адресов в таблице Static MAC Address Table

1. Откройте страницу Таблица Static MAC Address Table.
2. Выберите тип интерфейса.
3. Внесите изменения в соответствующие поля.
4. Нажмите кнопку **Apply Changes (Применить изменения)**.

Статический MAC-адрес будет изменен, а устройство обновлено.

Удаление статического адреса из таблицы Static Address Table

1. Откройте страницу Таблица Static MAC Address Table.
2. Выберите интерфейс.
3. Нажмите кнопку **Show All** (Показать все).

Откроется страница **Static MAC Address Table** (Статический MAC-адрес).

4. Выберите запись таблицы.
5. Установите флажок в поле **Remove** (Удалить).
6. Нажмите кнопку **Apply Changes (Применить изменения)**.

Выбранный статический адрес удален, а устройство обновлено.

Настройка параметров статических адресов с помощью команд консоли

В следующей таблице приведены команды консоли для настройки параметров статических адресов, как показано на странице Таблица Static MAC Address Table.

Таблица 7-11. Команды страницы Static Address

Команды консоли	Описание
bridge address *mac-address* [permanent | delete-on-reset | delete-on-timeout | secure] {ethernet interface | port-channel *port-channel-number*}	Добавляет статический MAC-адрес станции-источника для таблицы системы связей.
show bridge address-table [**vlan** *vlan*] [**ethernet** *interface* | **port-channel** *port-channel-number*]	Отображает записи о пересылке данных через мосты.

Ниже 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
```

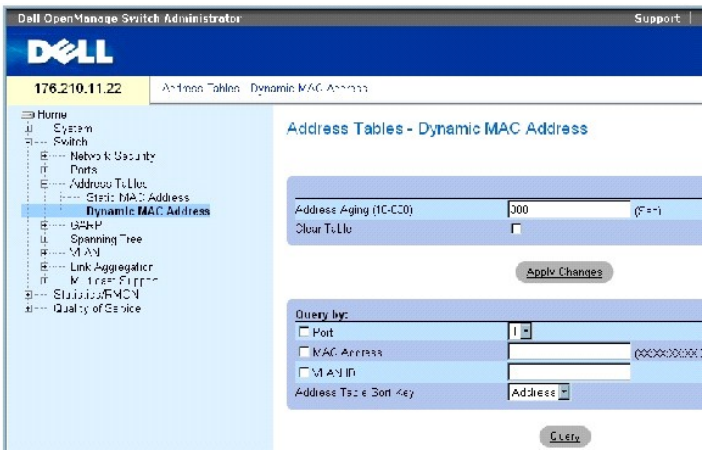
----	----------	----	--------
1	00:60:70:4C:73:FF	1/e8	dynamic
1	00:60:70:8C:73:FF	1/e8	dynamic
200	00:10:0D:48:37:FF	1/e9	static

Просмотр динамических адресов

На странице **Динамический MAC-адрес** содержится информация по запросу в таблице динамических адресов сведений относительно типа интерфейса, MAC-адреса, VLAN и сортировки таблицы. Пакеты, которые пересылаются по адресам, хранящимся в таблице адресов, пересылаются непосредственно на эти порты. На странице **Динамический MAC-адрес** также приводятся сведения о сроке действия динамического MAC-адреса (срок, по истечении которого он удаляется), и перечислены параметры запроса и просмотра списка динамических адресов. В таблице Current Address Table (Таблица текущих адресов) хранятся параметры динамических адресов, по которым пакеты пересылаются непосредственно на порты.

Чтобы открыть страницу **Динамический MAC-адрес**, щелкните Switch (Коммутатор) →Address Tables (Адресные таблицы) → Dynamic**MAC Address (Динамический MAC-адрес)** в панели дерева.

Рисунок 7-20. Динамический MAC-адрес



На странице **Динамический MAC-адрес** есть следующие поля:

Address Aging (Срок хранения адресов)- Время, в течение которого MAC-адрес хранится в таблице Динамический MAC-адрес при отсутствии трафика из источника. Значение по умолчанию: 300 секунд.

Clear Table (Очистить таблицу) - Удаляет данные из таблицы динамических адресов, если это поле отмечено.

Port - Указывает интерфейс, который запрашивается в таблице. Имеется два типа интерфейсов.

MAC Address - MAC-адрес, для которого опрашивается таблица.

VLAN ID - Идентификатор сети VLAN, для которой опрашивается таблица.

Address Table Sort Key (Ключ для сортировки таблицы адресов) - Метод, по которому сортируется таблица динамических адресов. Записи в таблице адресов можно сортировать по адресам, сетям VLAN или интерфейсам.

Переопределение срока хранения

1. Откройте страницу **Динамический MAC-адрес**.
2. Определите поле **Aging Time** (Срок хранения).
3. Нажмите кнопку Apply Changes (Применить изменения).

Срок хранения будет изменен, а устройство обновлено.

Опрос таблицы динамических адресов

1. Откройте страницу **Динамический MAC-адрес**.
2. Определите, по какому параметру нужно выполнить запрос по таблице **Dynamic Address Table**.

Можно вводить запрос по параметрам **Port (Порт)**, **MAC Address (MAC-адрес)** или **VLAN ID**.

3. Нажмите кнопку **Query** (Запрос).

Выполнен запрос Динамический MAC-адрес.

Сортировка таблицы динамических адресов

1. Откройте страницу **Динамический MAC-адрес**.
2. Из раскрывающегося меню **Address Table Sort Key (Параметр сортировки адресной таблицы)** выберите параметр сортировки адресов: адрес, VLAN ID или интерфейс.
3. Нажмите кнопку **Query** (Запрос).

Выполнена сортировка Динамический MAC-адрес.

Опрос и сортировка динамических адресов с помощью команд консоли

В следующей таблице приведены команды консоли для опроса, срока хранения и сортировки динамических адресов на странице Динамический MAC-адрес.

Таблица 7-12. Команды запроса и сортировки

Команды консоли	Описание
bridge aging-time *seconds*	Задает срок хранения для таблиц адресов.
show bridge address-table [**vlan** *vlan*] [**ethernet** *interface* | **port-channel** *port-channel-number*]	Отображает классы динамически созданных записей базы данных, содержащей сведения о пересылке данных через мосты.

Ниже приведен пример команд консоли:

```
console (config)# bridge aging-time 250

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 GARP

Протокол GARP (Generic Attribute Registration Protocol) - это протокол общего назначения, регистрирующий любые возможности связи в сети или сведения о членстве. Протокол GARP определяет набор устройств, заинтересованных в данном атрибуте сети, например VLAN или адрес многоадресной передачи.

При настройке GARP примите во внимание следующее:

- Время отключения должно быть больше или равно трехкратному времени соединения.
- Время полного отключения должно быть больше времени отключения.
- Задайте одно значение таймера GARP для всех устройств, подключенных к уровню Layer 2. Разные показания таймеров GARP, подключенных к уровню Layer 2, приводят к сбоям в работе приложения GARP.

Чтобы открыть страницу **GARP** , нажмите Switch (Коммутатор) → **GARP** в панели дерева.

Определение таймеров GARP

На странице Таймеры GARP имеются поля для включения протокола GARP на устройстве. Чтобы открыть страницу Таймеры GARP, нажмите Switch (Коммутатор) → **GARP** → **GARP Timers (Таймеры GARP)** в панели дерева.

Рисунок 7-21. Таймеры GARP

На странице GARP Timers (Таймеры GARP) есть следующие поля:

Interface (Интерфейс) - Чтобы выбрать порт или LAG для изменения таймеров GARP.

GARP Join Timer (10-2147483640) (Таймер соединения GARP) - Время в миллисекундах, когда передаются данные PDU. По умолчанию используется значение 200.

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 и отменяется при получении сообщения Join (Соединение). Время отключения должно быть больше или равно трехкратному времени соединения. По умолчанию используется значение 600.

GARP Leave Timer (10-2147483640) (Таймер отключения GARP) - Время (в миллисекундах), в течение которого устройство ожидает, прежде чем выйти из состояния GARP. Время полного отключения должно быть больше времени отключения. По умолчанию используется значение 10000.

Определение таймеров GARP

1. Откройте страницу Таймеры GARP.
2. Выберите тип интерфейса.
3. Заполните поля.
4. Нажмите кнопку **Apply Changes (Применить изменения)**.

Параметры GARP будут сохранены для этого устройства.

Копирование параметров в таблицу GARP Timers Table.

1. Откройте страницу Таймеры GARP.
2. Нажмите кнопку **Show All** (Показать все).

Откроется таблица таймеров **GARP Timers Table**.

3. Выберите интерфейс в поле **Copy Parameters from (Копировать параметры из).**
4. Выберите интерфейс либо в раскрывающемся меню **Port (Порт)**, либо **LAG**.

Определения этого интерфейса копируются в выбранные интерфейсы. См. Шаг 6.

5. Отметьте флажком поле **Copy to (Копировать в)** того интерфейса, в который хотите скопировать параметры определения таймера GARP, или нажмите кнопку **Select All (Выбрать все)**, чтобы скопировать параметры во все порты или LAG.
6. Нажмите кнопку **Apply Changes (Применить изменения)**.

Параметры копируются в поле портов или LAG в таблице **GARP Timers Table** , а устройство обновляется.

Определение таймеров GARP с помощью команд консоли

В следующей таблице приведены команды консоли, соответствующие полям для определения таймеров GARP на странице Таймеры GARP.

Таблица 7-13. Команды страницы GARP Timer

Команды консоли	Описание
garp timer {join | leave | leaveall} *timer_value*	Задает значения таймеров GARP для времени соединения, отключения и полного отключения приложений GARP.

Ниже 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) обеспечивает топографию дерева при любой организации мостов. Протокол STP обеспечивает единственный путь между конечными станциями сети, тем самым исключая 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.

Коммутатор поддерживает следующие версии протоколов STP:

- Classic STP (Классический STP) - Обеспечивает единственный путь между конечными станциями сети, а, следовательно, исключает циклы. Более подробную информацию о конфигурации классического протокола STP см. в «**Определение общих параметров STP**».
- Протокол RSTP (Rapid Spanning Tree Protocol) - выявляет и использует топологию сети, таким образом обеспечивая лучшую сходимость для протокола STP без образования циклов пересылки. Если коммутатор настроен на работу по протоколу RSTP, а соседние устройства - по протоколу STP, локальное устройство использует STP.

  Более подробную информацию о конфигурации протокола Rapid STP см. в «**Настройка протокола RSTP**».
- Протокол MSTP (Multiple Spanning Tree Protocol) - Обеспечивает полную связность пакетов, предназначенных для любых сетей VLAN. Протокол MSTP основан на протоколе RSTP. Кроме того, протокол MSTP передает пакеты, предназначенные для различных VLAN в различных полях MST. Поля MST действуют как единый мост, если устройство настроено на работу по протоколу MSTP. Тем не менее, если протокол RSTP активирован на соседнем устройстве, а локальное использует STP, RSTP и MSTP, оба устройства могут взаимодействовать.

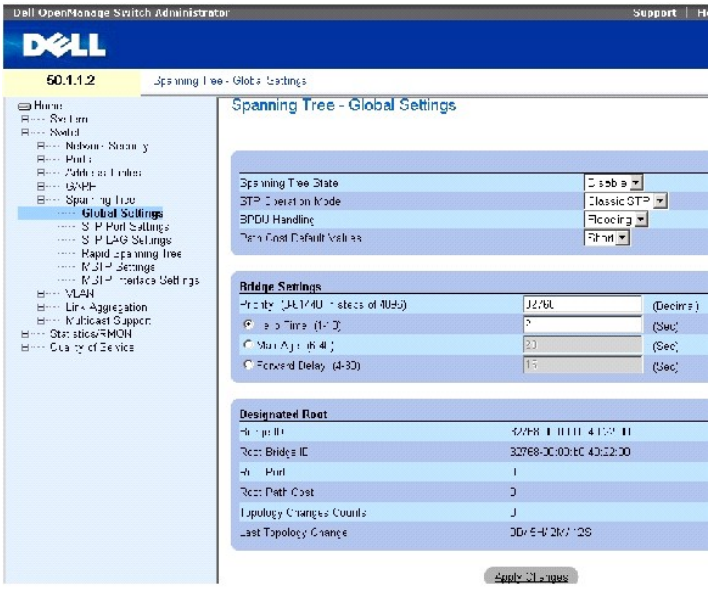
Более подробную информацию о конфигурации протокола Multiple STP см. в «**Настройка протокола MSTP**».

Чтобы открыть страницу **Spanning Tree (Протокол STP)** , нажмите **Switch (Коммутатор)** → **Spanning Tree (Протокол STP)**в панели дерева.

Определение общих параметров STP

На странице Страница Spanning Tree Global Settings имеются параметры для включения протокола STP на устройстве. Чтобы открыть страницу Страница Spanning Tree Global Settings , нажмите **Switch (Коммутатор)** → **Spanning Tree (Протокол STP)** → **Global Settings (Глобальные параметры)** в панели дерева.

Рисунок 7-22. Страница Spanning Tree Global Settings



На странице Страница Spanning Tree Global Settings есть следующие поля:

Spanning Tree State - Включает или выключает протоколы STP, RSTP или MSTP для устройства.

STP Operation Mode (Режим работы STP) - Указывает режим включения протокола STP на устройстве. Возможные значения поля:

Classic STP - Включает протокол CSTP на устройстве. Это значение по умолчанию.

Rapid STP - Включает протокол RSTP на устройстве.

Multiple STP - Включает протокол MSTP на устройстве.

BPDU Handling (Обработка данных BPDU) - Определяет способ обработки пакетов BPDU, когда протокол STP не связан с портом/устройством. Данные BPDU используются для передачи информации протокола STP. Возможные значения поля:

Filtering (Фильтрация) - Выполняет фильтрацию пакетов BPDU, если протокол STP не подключен на интерфейс. Это значение по умолчанию.

Flooding (Наполнение) - Накапливает пакеты BPDU, если протокол STP не подключен на интерфейс.

Path Cost Default Values (Значения стоимости пути по умолчанию) - Определяет метод, используемый для определения стоимости пути для портов STP. Возможные значения поля:

Short (Короткий) - Соответствует диапазону значений от 1 до 65535. Это значение по умолчанию.

Long (Длинный) - Соответствует диапазону значений от 1 до 200 000 000.

Значение по умолчанию может меняться в зависимости от выбранного метода:

Interface (Интерфейс)	Long (Длинный)	Short (Короткий)
LAG	20,000	4
1000 Mbps (МБ/с)	20,000	4
100 Mbps (МБ/с)	200,000	19
10 Mbps (МБ/с)	2,000,000	100

Priority (0-65535) - Значение приоритета для моста. Когда коммутаторы или мосты работают по протоколу STP, каждому из них назначается приоритет. После обмена пакетами BPDU коммутатор с низшим значением приоритета становится корневым мостом. Значение по умолчанию: 32768. Значение приоритета порта увеличивается с шагом, равным 4096: 4096, 8192, 12288 и так далее.

Hello Time (1-10) (Интервал отправки) - Время Hello Time для коммутатора. Это интервал отправки конфигурационных сообщений с корневого моста (в секундах). Значение по умолчанию: 2 секунды.

Max Age (6-40) (Максимальное время) - Время Maximum Age Time для коммутатора. Это максимальное время (в секундах), которое мост ожидает перед отправкой конфигурационного сообщения. Значение по умолчанию для максимального времени: 20 секунд.

Forward Delay (4-30) (Задержка пересылки) - Время задержки пересылки для коммутатора (Forward Delay Time). Это время, которое мост находится в состояниях распознавания (learning) и прослушивания (listening) перед пересылкой пакетов. Значение по умолчанию: 10 секунды.

Bridge ID (Идентификатор моста) - Указывает приоритет моста и MAC-адрес.

Root Bridge ID (Идентификатор корневого моста) - Указывает приоритет корневого моста и MAC-адрес.

Root Port (Корневой порт) - Номер порта, предлагающего путь от данного моста к корневому с наименьшими затратами. Этот параметр важен, если мост не является корневым.

Root Path Cost - Стоимость пути от данного моста до корневого.

Topology Changes Counts (Количество изменений топологии) - Общее количество изменений состояния STP, которые имели место.

Last Topology Change (Последнее изменение топологии) - Время, прошедшее после инициализации или перенастройки моста и последнего изменения топологии. Формат отображения времени: Д/Ч/М/С/, например, 2D/5H/10M/4S.

Определение общих параметров STP

1. Откройте страницу .
2. Выберите в поле **Spanning Tree State** (Состояние Spanning Tree) значение **Enable** (Включить).
3. Выберите режим **STP** в поле **STP Operation Mode (Операционный режим STP)** и определите параметры моста.
4. Нажмите кнопку **Apply Changes (Применить изменения)**.

Протокол STP будет включен на этом устройстве.

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 команды консоли, соответствующие полям для определения общих параметров протокола STP на странице Spanning Tree Global Settings.

Таблица 7-14. Команды для вывода общих параметров STP

Команды консоли	Описание
spanning-tree	Включает функциональные возможности протокола STP.
spanning-tree mode {**stp** | **rstp** | **mstp**}	Конфигурация режима работы протокола STP.
spanning-tree priority	Настраивает приоритет протокола STP.
spanning-tree hello-time *seconds*	Настраивает время Hello Time для моста протокола STP, определяющее, как часто коммутатор выполняет широковещательную передачу сообщений Hello другим коммутаторам.
spanning-tree max-age *seconds*	Настраивает максимальное время для моста протокола STP.
spanning-tree forward- time seconds	Настраивает время пересылки для моста протокола STP, определяющее, как долго порт находится в состоянии прослушивания и распознавания перед включением состояния пересылки.
show spanning-tree [**ethernet** *interface* | **port-channel** *port- channel-number*] [**instance** *instance-id*]	Выводит конфигурацию протокола STP.
show spanning-tree [**detail**] [**active** | **blockedports**] [**instance** *instance-id*]	Выводит на экран подробную информацию об активных и заблокированных портах.
show spanning-tree mst- configuration	Выводит конфигурацию MST протокола STP.

Ниже 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

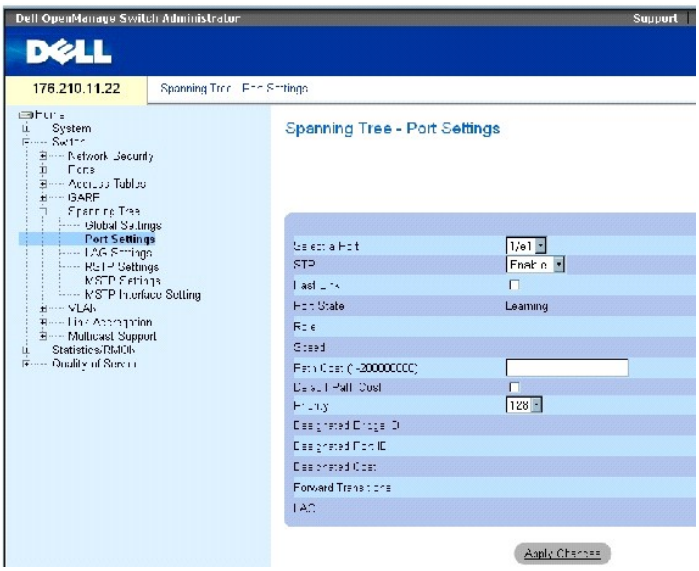
```
console# show spanning-tree active

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

Используйте страницу Spanning Tree Port Settings для назначения свойств STP отдельным портам. Чтобы открыть страницу Spanning Tree Port Settings , нажмите **Switch (Коммутатор)** → **Spanning Tree (Протокол STP)**→ **Port Settings (Параметры порта)** в панели дерева.

Рисунок 7-23. Страница Spanning Tree Global Settings



На Spanning Tree Port Settings (Параметры порта STP) есть следующие поля:

Select a Port (Выбор порта) - Номер порта, для которого требуется изменить параметры STP.

STP - Включает или выключает протокол STP на порте.

Fast Link (Быстрая связь) - Включает режим быстрой связи для порта. Если режим быстрой связи для порта включен, **Port State**автоматически переводится в состояние пересылки **Forwarding** state сразу после появления связи. Режим Fast Link оптимизирует время, которое требуется протоколу STP на сходимость. В больших сетях на нее может потребоваться 30-60 секунд.

Port State - Текущее состояние протокола STP для порта. Если этот параметр включен, он определяет, какое действие пересылки выполняется в ходе трафика. Возможные состояния порта:

Disabled (Выключен) - Протокол STP временно отключен на порте. Порт может пересылать трафик и распознавать новые MAC-адреса.

Blocking (Блокирование) - Порт в данный момент заблокирован и не может использоваться для пересылки трафика или распознавания MAC-адресов. Поле Blocking (Блокирование) отображается, если включен протокол Classic 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)-Роль порта, назначенная алгоритмом STP, который предоставляет пути STP. Возможные значения поля:

Root (Корневой)-Предоставляет путь, требующий минимальных затрат для передачи пакетов на корневой коммутатор.

Designated (Назначенный)-Указывает порт, через который назначенный коммутатор подключается к локальной сети.

Alternate (Альтернативный)-Предоставляет альтернативный путь к корневому коммутатору с корневого интерфейса.

Backup (Резервный)-Предоставляет альтернативный путь к назначенному порту. Резервный метод используется только в том случае, если два порта подсоединены в цепь двухпунктовым соединением. Резервные порты также встречаются, когда в локальной сети имеется два или более соединения, подключенных к общему сегменту.

Disabled (Отключен)-Порт не подключен к протоколу STP.

Speed (Скорость) - Частота, на которой работает порт.

Path Cost (1-200000000) (Стоимость пути) - Вклад порта в стоимость пути к корневому. Стоимость пути может иметь большее или меньшее значение и может пересылать трафик по маршрутизируемому пути или от него.

Default Path Cost - Стандартная стоимость пути. Стоимость длинного пути по умолчанию:

Ethernet - 2,000,000

Fast Ethernet - 200,000

Gigabit Ethernet - 20,000

Стоимость короткого пути по умолчанию:

Ethernet -100

Fast Ethernet -19

Gigabit Ethernet -4

Priority (0-240, in steps of 16) (Приоритет, 0-240 с шагом приращения 16) - Значение приоритета порта. Значение приоритета может быть использовано для регулировки выбора порта, когда мост имеет два порта, соединенных в петлю. Значение приоритета: 0-240. Значение приоритета порта увеличивается с шагом, равным 16.

Designated Bridge ID (Идентификатор назначенного моста) - Приоритет 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. Вероятность того, что порт с низкой стоимостью будет заблокирован, если STP обнаружит петлю, невелика.

Forward Transmission (Переходы к пересылке)- Указывает, 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** (Параметры STP для порта).
2. Выберите порт.
3. Выберите значение **Enabled (Включен)** в поле **STP**.
4. Определите поля **Fast Link**, **Path Cost** и **Priority**.
5. Нажмите кнопку **Apply Changes (Применить изменения)**.

Протокол STP будет включен на этом порте.

Изменение свойств STP для порта

1. Откройте страницу Spanning Tree Port Settings (Параметры STP для порта).
2. Выберите порт.
3. Внесите изменения в соответствующие поля.
4. Нажмите кнопку **Apply Changes (Применить изменения)**.

Параметры STP для порта будут изменены, а устройство обновлено.

Вывод таблицы STP Port Table

1. Откройте страницу Spanning Tree Port Settings (Параметры STP для порта).
2. Нажмите кнопку **Show All** (Показать все).

Откроется страница **STP Port Table** (Таблица портов STP).

Определение параметров порта STP 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 7-15. Команды страницы STP Port Settings

Команды консоли	Описание
spanning-tree disable	Отключает протокол STP на назначенном порте.
spanning-tree cost cost	Настраивает стоимость порта STP для данного порта.
spanning-tree port-priority priority	Настраивает приоритет порта.
show **spanning-tree** [**ethernet** interface | **port-channel** port-channel- number] [**instance** *instance- id*]	Выводит конфигурацию протокола STP.
spanning-tree portfast	Включает режим PortFast.
show spanning-tree [detail] [**active** | **blockedports**] [**instance** *instance-id*]	Выводит на экран подробную информацию об активных и заблокированных портах.
show spanning-tree mst- configuration	Выводит конфигурацию MST протокола STP.

Ниже приведен пример команд консоли:

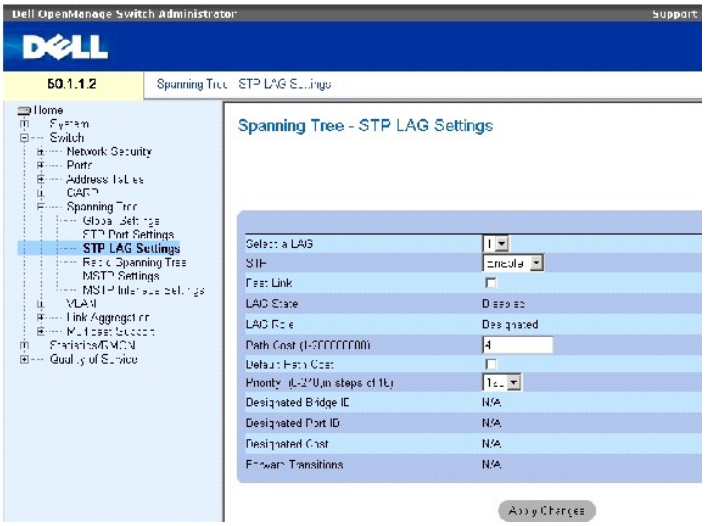
```
console> enable

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: forwarding			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

Используйте страницу **Spanning Tree LAG Settings (Параметры STP для LAG)**, чтобы назначить параметры STP для интегральных портов. Чтобы открыть страницу Spanning Tree LAG Settings, нажмите **Switch (Коммутатор)** → **Spanning Tree (Протокол STP)**→ **LAG Settings (Параметры LAG)** в панели дерева.

Рисунок 7-24. Страница Spanning Tree LAG Settings



На странице **Spanning Tree LAG Parameters** (Параметры STP для LAG) есть следующие поля:

Select a LAG (Выбор LAG) - Номер группы LAG, для которой требуется изменить параметры STP.

STP - Включает или выключает протокол STP в группе LAG.

Fast Link (Быстрая связь) - Включает режим быстрой связи для LAG. Если режим быстрой связи для LAG включен, **LAG State** автоматически переводится в состояние пересылки **Forwarding** сразу после появления связи. Режим Fast Link оптимизирует время, которое требуется протоколу STP на сходимость. В больших сетях на нее может потребоваться 30-60 секунд.

LAG State - Текущее состояние параметров STP для LAG. Если этот параметр включен, он определяет, какое действие пересылки выполняется в ходе трафика. Если мост выявляет неполадки в работе группы LAG, то она переводится в состояние **Broken** (Неполадка). Возможные состояния LAG:

Disabled (Выключен) - Протокол STP временно отключен на LAG. LAG может пересылать трафик и распознавать новые MAC-адреса.

Blocking (Блокирование) - LAG заблокирована и не может использоваться для пересылки трафика или распознавания MAC-адресов.

RSTP Discarding State (Состояние отказа RSTP) - В этом состоянии порт не распознает MAC-адреса и не пересылает кадры.

Это состояние является совмещением блокирования и прослушивания, введенное в STP (802.1.D).

Listening (Прослушивание) - LAG находится в режиме прослушивания и не пересылает трафик, и не распознает MAC-адреса.

Learning (Распознавание) - LAG находится в режиме распознавания и не пересылает трафик, но может распознать новые MAC-адреса.

Forwarding (Передача) - LAG находится в режиме передачи, группа может переслать трафик и распознать новые MAC-адреса.

Broken (Неисправность) - LAG находится в неисправном состоянии, ее нельзя использовать для передачи трафика.

LAG Role (Роль LAG)-Роль LAG, назначенная алгоритмом STP, который предоставляет пути STP. Возможные значения поля:

Root (Корневой)-Предоставляет путь, требующий минимальных затрат для передачи пакетов на корневой коммутатор.

Designated (Назначенный)-Указывает LAG, через которую назначенный коммутатор подключается к локальной сети.

Alternate (Альтернативный)-Предоставляет альтернативную LAG, ведущую к корневому коммутатору с корневого интерфейса.

Backup (Резервный)-Предоставляет альтернативный путь к назначенному порту. Резервный метод используется только в том случае, если два порта подсоединены в цепь двухпунктовым соединением. Резервные порты также встречаются, когда в локальной сети имеется два или более соединения, подключенных к общему сегменту.

Disabled (Отключен)-LAG не подключена к протоколу STP.

Path Cost (1-200000000) (Стоимость пути) - Вклад LAG в стоимость пути к корневому. Стоимость пути может иметь большее или меньшее значение и может пересылать трафик по маршрутизируемому пути или от него. Стоимость пути может иметь значения от 1 до 200000000.

Default Path Cost- Стандартная стоимость пути. Возможные значения стоимости пути LAG по умолчанию :

Long Method for LAG (Метод длинного пути для LAG) - **20,000**

Short Method for LAG (Метод короткого пути для LAG) - 4

Priority (0-240, in steps of 16) (Приоритет, 0-240 с шагом приращения 16) - Значение приоритета LAG. Значение приоритета может быть использовано для регулировки выбора LAG, когда мост имеет порты, соединенные в петлю. Значение приоритета находится в диапазоне 0-240, с шагом приращения равным 16.

Designated Bridge ID (Идентификатор назначенного моста) - Приоритет и MAC-адрес назначенного моста.

Designated Port ID (Идентификатор назначенного порта) - Идентификатор выбранного интерфейса.

Designated Cost (Назначенная стоимость) - Стоимость порта, участвующего в топологии STP. Вероятность того, что порт с низкой стоимостью будет заблокирован, если STP обнаружит петлю, невелика.

Forward Transitions (Переходы к пересылке) - Указывает, сколько раз **LAG меняла свое состояние** с Forwarding (пересылка) на **Blocking (блокирование)**.

Изменение параметров STP для LAG

1. Откройте страницу Spanning Tree**LAG Settings** .
2. Выберите LAG в раскрывающемся меню **Select a LAG (Выбор LAG)**.
3. Внесите необходимые изменения.
4. Нажмите кнопку **Apply Changes (Применить изменения)**.

Параметры STP для группы LAG будут изменены, а устройство обновлено.

Определение параметров LAG STP с помощью команд консоли

В таблице приводятся команды консоли для определения параметров STP для LAG .

Таблица 7-16. Команды страницы STP LAG Settings

Команды консоли	Описание
`spanning-tree`	Включает функциональные возможности протокола STP.
`spanning-tree disable`	Отключает протокол STP для определенной группы LAG.
`spanning-tree cost` *`cost`*	Настраивает стоимость порта STP для данной LAG.
`spanning-tree port-priority` *`priority`*	Настраивает приоритет порта.
`show spanning-tree [`**`ethernet`** `interface |` **`port-channel`** *`port-channel- number`*`] [`**`instance`** *`instance- id`*`]`	Выводит конфигурацию протокола STP.
`show spanning-tree [detail] [active | blockedports] [`**`instance`** *`instance-id`*`]`	Выводит на экран подробную информацию об активных и заблокированных портах.

Ниже приведен пример команд консоли:

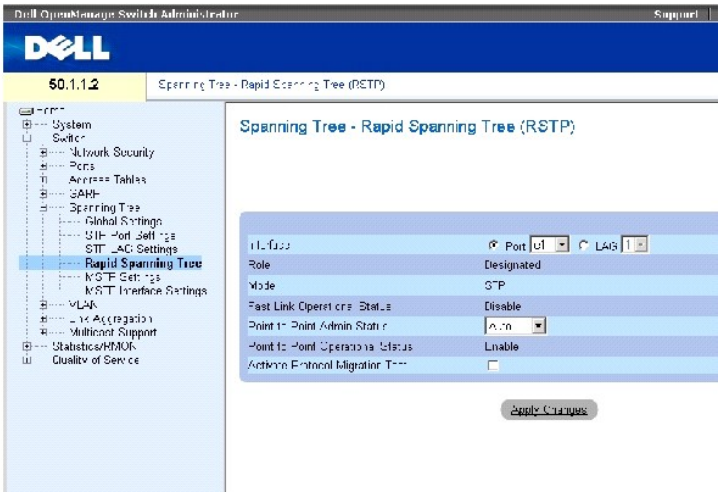
```
console(config)# interface
port-channel 1

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
```

Настройка протокола RSTP

Протокол Classic Spanning Tree позволяет мостам препятствовать возникновению циклов пересылки L2 в общей топологии сети, но на сходимость может уходить 30-60 секунд. В течение этого времени протокол STP определяет возможные замкнутые цепи, а также передает информацию об изменении состояния системы.

Протокол RSTP (Rapid Spanning Tree Protocol) выявляет и использует топологию сети, таким образом обеспечивая лучшую сходимость для протокола STP без образования циклов пересылки. Чтобы открыть страницу Rapid Spanning Tree (RSTP) settings , нажмите **Switch (Коммутатор)** → **Spanning Tree (Протокол STP)**→ **Rapid Spanning Tree (Протокол RSTP)** в панели дерева.

Рисунок 7-25. Страница Rapid Spanning Tree (RSTP) settings



На странице Rapid Spanning Tree (RSTP) есть следующие поля:

Interface (Интерфейс) - Порт или LAG, для которых можно изменить и вывести на экран параметры RSTP.

State (Состояние) - Выключает состояние RSTP на выбранном интерфейсе.

Role (Роль)-Роль порта, назначенная алгоритмом STP, который предоставляет пути STP. Возможные значения поля:

Root (Корневой)-Предоставляет путь, требующий минимальных затрат для передачи пакетов на корневой коммутатор.

Designated (Назначенный)-Указывает LAG, через которую назначенный коммутатор подключается к локальной сети.

Alternate (Альтернативный)-Предоставляет альтернативный путь к корневому коммутатору с корневого интерфейса.

Backup (Резервный)-Предоставляет альтернативный путь к назначенному порту. Резервный метод используется только в том случае, если два порта подсоединены в цепь двухпунктовым соединением. Резервные порты также встречаются, когда в локальной сети имеется два или более соединения, подключенных к общему сегменту.

Disabled (Отключен)-Порт не подключен к протоколу STP.

Mode-Indicates the current Spanning Tree mode. The Spanning Tree mode is selected in the Страница Spanning Tree Global Settings page. The possible field values are:

Classic STP-Indicates that Classic STP is enabled on the device.

Classic STP - Включает протокол CSTP на устройстве.

Classic STP - Включает протокол CSTP на устройстве.

Fast Link Operational Status (Рабочее состояние Fast Link) - Указывает, включена или нет функция быстрой связи для порта или LAG. Если для интерфейса включен режим быстрой связи, то он автоматически переводится в состояние пересылки.

Point-to-Point Admin Status (Администрирование двухточечного соединения) - Позволяет или запрещает устройству установить связь с соединением "точка-точка", или устанавливает эту связь автоматически.

Чтобы установить связь с соединением "точка-точка", исходный протокол двухточечного соединения (PPP) сначала отправляет пакеты протокола контроля соединения (LCP), чтобы настроить и выполнить тест канала передачи данных. После того, как связь установлена, а дополнительные функции настроены по протоколу LCP, исходный протокол двухточечного соединения (PPP) отправляет пакеты на протоколы контроля сети (NCP), чтобы выбрать и настроить один или несколько протоколов сетевого уровня. После того, как все выбранные протоколы сетевого уровня настроены, по связи можно пересылать пакеты со всех протоколов NLP. Связь сохраняет конфигурацию коммуникации до тех пор, пока определенные пакеты протоколов LCP или NCP не закроют ее, или пока не произойдет какое-либо внешнее событие. Это действительный тип связи для порта коммутатора. Он может отличаться от администраторского состояния.

Point-to-Point Operational Status - Рабочее состояние соединения "точка-точка".

Activate Protocol Migrational - Включает отправку пакетов с исходного протокола двухточечного соединения (PPP) на протокол контроля соединения (LCP), чтобы настроить и выполнить тест канала передачи данных.

Определение параметров RSTP

1. Откройте страницу Spanning Tree RSTP Settings (Параметры RSTP).
2. Выберите тип интерфейса.
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**.

Определение параметров Rapid STP с помощью команд консоли

В следующей таблице приведены команды консоли, соответствующие полям для определения ïàðàìåòðîâ RSTP на странице Rapid Spanning Tree (RSTP).

Таблица 7-17. Команды страницы RSTP Settings

Команды консоли	Описание
`spanning-tree link-type {point-to-point | shared}`	Принудительно замещает параметр типа связи, заданный по умолчанию.
`spanning tree mode {stp | rstp | mstp}`	Настраивает протокол STP, работающий в данный момент.
`clear spanning-tree detected-protocols [ethernet interface | port-channel port-channel-number]`	Перезапускает процесс миграции протоколов.
`show spanning-tree [ethernet interface | port-channel port- channel-number]`	Выводит конфигурацию протокола STP.

Ниже приведен пример команд консоли:

```
console(config)# interface ethernet 1/e5
```

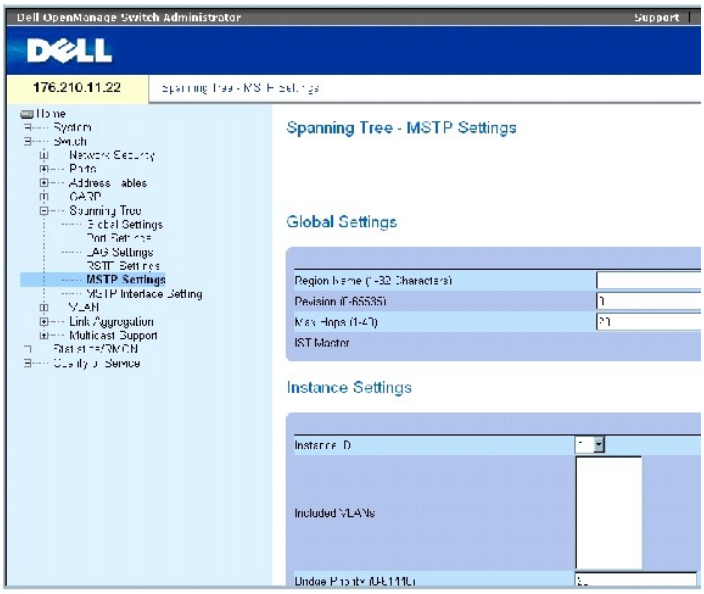
```
console(config-if)# spanning-tree link-type shared

console(config-if)# spanning tree mode rstp
```

Настройка протокола MSTP

Действие протокола MSTP заключается в привязке сетей VLAN на образы протокола STP. MSTP предлагает другой сценарий распределения нагрузки. Например, если порт A заблокирован в одном из образов STP, этот же самый порт переводится в состояние передачи Forwarding State на другом образе STP.

Кроме того, пакеты, назначенные для различных сетей VLAN, передаются по различным каналам в области протокола MSTP (Области MST). Области представляют собой один или несколько мостов MSTP, по которым передаются кадры. Чтобы открыть страницу Параметры MSTP , нажмите Switch (Коммутатор) → Spanning Tree (Протокол STP) → MSTP Settings (Параметры MSTP) в панели дерева.

Рисунок 7-26. Параметры MSTP



На странице Параметры MSTP есть следующие поля:

Region Name (1-32 Characters) (Название области, 1-32 символа) - Пользовательское имя области MSTP.

Revision (Ревизия)(0-65535) - Определяет 16-битный номер, который задает текущую ревизию конфигурации MST. Номер ревизии требуется как параметр конфигурации MST. Возможные значения поля: от 0 до 65535.

Max Hops (1-40) (Количество повторных приемов)- Определяет общее количество повторных приемов в одной области, после которого данные BPDU игнорируются. После того, как данные BPDU начинают игнорироваться, информация порта устаревает. Возможное значение поля: 1-40. Значение по умолчанию: 20 раз.

IST Master - Идентификатор главного устройства протокола STM. Главное устройство IST является копией корня 0.

Instance ID (Идентификатор экземпляра) - Определяет копию MSTP. Значение находится в диапазоне 1-15.

Included VLANs - Показывает сети VLAN, привязанные к выбранному экземпляру. Каждая сеть VLAN соответствует одному экземпляру.

Bridge Priority (0-61440) (Приоритет моста) - Приоритет выбранной копии протокола. Значение поля: 0-61440 с шагом приращения 4096

Designated Root Bridge ID (Назначенный идентификатор корневого моста) - Идентификатор моста, который является корневым для выбранного экземпляра.

Root Port (Корневой порт) - Указывает корневой порт выбранного экземпляра.

Root Port (Корневой порт) - Указывает корневой порт выбранного экземпляра.

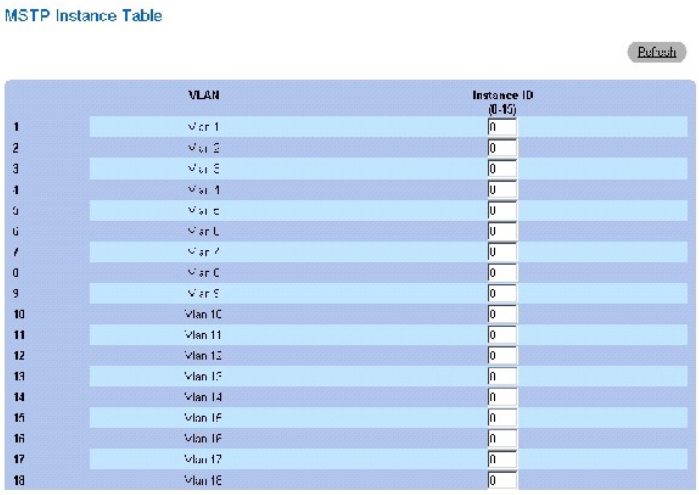
Bridge ID (Идентификатор моста) - Идентификатор моста выбранного экземпляра.

Remaining Hops (Оставшиеся попытки) - Количество оставшихся попыток для передачи данных в приемник.

Отображение таблицы MSTP Instance Table (Таблица копий MSTP)

1. Откройте страницу **Spanning Tree** Параметры MSTP.
2. Щелкните **Show All (Показать все)**, чтобы открыть страницу MSTP Instance Table (Таблица копий MSTP).

Рисунок 7-27. MSTP Instance Table (Таблица копий MSTP)



Определение копий MST с использованием командной строки

В следующей таблице приведены команды консоли, соответствующие полям для определения копий MSTP на странице **Spanning Tree** Параметры MSTP.

Таблица 7-18. Команды страницы MSTP Instances

Команды консоли	Описание
`spanning-tree mst configuration`	Включает режим конфигурации MST.
	Привязывает сети VLAN к копии MST.

instance instance-id {add | remove} vlan vlan-range	
name string	Задает имя конфигурации.
revision value	Задает номер ревизии конфигурации
spanning-tree **mst** instance-id port-priority priority	Задает приоритет порта.
spanning-tree mst instance-id priority priority	Задает приоритет устройства для определенного экземпляра протокола.
spanning-tree mst max- hops hop-count	Определяет количество повторных приемов в области MST, после которого данные BPDU игнорируются, а информация в памяти порта устаревает.
spanning-tree mst instance-id **cost** cost	Задает стоимость пути порта по подсчетам MST
exit	Выход из режима конфигурации области MST и вступление в силу выполненных изменений.
abort	Выход из режима конфигурации области MST, выполненные изменения не применяются.
show {current | pending}	Отображение текущей или ожидающей очереди конфигурации области MST.

Ниже приведен пример команд консоли:

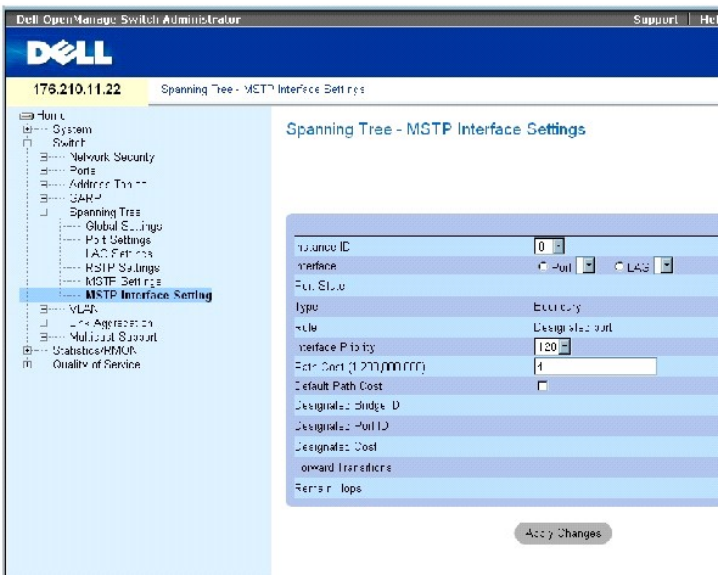
```
console(config)# spanning-tree mst configuration

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

Name: Region1
```

```
Revision: 1

Instance Vlans Mapped

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

0 1-9,31-4094

1 10-20

2 21-30
```

Определение интерфейсных параметров MSTP

На странице Интерфейсные параметры MSTP содержатся параметры, назначающие установки MSTP для определенных интерфейсов. Чтобы открыть страницу Интерфейсные параметры MSTP, нажмите Switch (Коммутатор) → Spanning Tree (Протокол STP) → MSTP Interface Settings (Интерфейсные параметры MSTP) в панели дерева.

Рисунок 7-28. Интерфейсные параметры MSTP



На странице Интерфейсные параметры MSTP есть следующие поля:

Instance ID (Идентификатор копии) - Список копий MSTP, настроенных на устройстве. Возможные значения поля: от 1 до 15.

Interface (Интерфейс) - Назначает порты или LAG для выбранных копий MSTP.

Port State (Состояние порта)- Указывает, включен или выключен порт для определенной копии протокола.

Type (Тип) - Указывает, как MSTP интерпретирует порт - как двухпунктовое соединение или как порт, подключенный к накопителю, а текже определяет, является ли порт внутренним по отношению к области MST или граничным. Главный порт обеспечивает взаимодействие области MSTP и внешнего корневого CIST. Граничный порт соединяет мосты MST с локальной сетью в отклоняющихся областях. Если порт является граничным, также указывается в каком режиме работает устройство на другом конце связи - в RSTP или STP.

Role (Роль)-Роль порта, назначенная алгоритмом STP, который предоставляет пути STP. Возможные значения поля:

Root (Корневой)-Предоставляет путь, требующий минимальных затрат для передачи пакетов на корневой коммутатор.

Designated (Назначенный)-Указывает LAG, через которую назначенный коммутатор подключается к локальной сети.

Alternate (Альтернативный)-Предоставляет альтернативный путь к корневому коммутатору с корневого интерфейса.

Backup (Резервный)-Предоставляет альтернативный путь к назначенному порту. Резервный метод используется только в том случае, если два порта подсоединены в цепь двухпунктовым соединением. Резервные порты также встречаются, когда в локальной сети имеется два или более соединения, подключенных к общему сегменту

Disabled (Отключен)-Порт не подключен к протоколу STP.

Interface Priority (0-240,in steps of 16) (Приоритет интерфейса, 0-240, с приращением 16)- Определяет приоритет интерфейсов для определенных копий протокола. По умолчанию используется значение 128.

Path Cost - Вклад порта в стоимость копии протокола STP. Диапазон допустимых значений: 1-200,000,000.

Default Path Cost (Стоимость пути по умолчанию)- Значение по умолчанию назначено в соответствии с методом, выбранным на странице Страница Spanning Tree Global Settings.

Designated Bridge ID (Идентификатор назначенного моста)- Идентификатор моста, который соединяет совместно используемую локальную сеть с корневым каталогом.

Designated Port ID (Идентификатор назначенного порта)- Идентификатор порта, который соединяет совместно используемую локальную сеть с корневым каталогом.

Designated Cost (Назначенная стоимость) - Стоимость пути от совместно используемой локальной сети до корневого каталога.

Forward Transitions (Переходы к пересылке)- Указывает, сколько раз порт изменял свое состояние на forwarding (пересылка).

Remaining Hops (Оставшиеся попытки) - Количество оставшихся попыток для передачи данных в приемник.

Определение интерфейсных параметров MSTP

1. Откройте страницу Интерфейсные параметры MSTP.
2. Выберите тип интерфейса.
3. Определите поля.
4. Нажмите кнопку **Apply Changes (Применить изменения)**.

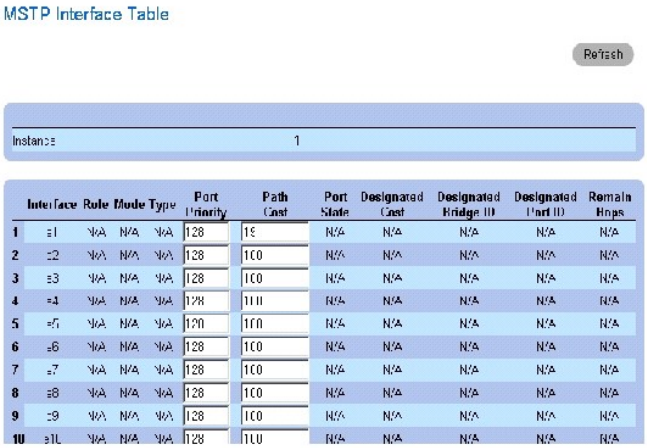
Параметры MSTP будут определены, а устройство обновлено.

Обзор таблицы MSTP Interface Table

1. Откройте страницу Интерфейсные параметры MSTP.
2. Нажмите кнопку Show All (Показать все).

Откроется страница Таблица интерфейсных параметров MSTP.

Рисунок 7-29. Таблица интерфейсных параметров MSTP



Определение интерфейсов MSTP с помощью команд консоли

В следующей таблице приведены команды консоли, соответствующие полям для определения интерфейсов MSTP на странице **Spanning Tree** Интерфейсные параметры MSTP.

Таблица 7-19. Команды страницы MSTP Interface

Команды консоли	Описание
`spanning-tree mst instance-id cost cost`	Задает стоимость пути порта по подсчетам MST
`spanning-tree mst instance-id priority priority`	Задает приоритет устройства для определенного экземпляра ST.
`show spanning-tree mst- configuration`	Выводит конфигурацию MST.

Ниже приведен пример команд консоли:

```
console# show spanning-tree mst-configuration

Gathering information .....

Current MST configuration

Name: 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

Сети VLAN представляют собой логические подгруппы локальной сети (ЛС), созданные программным, а не аппаратным путем. Сети VLAN комбинируют пользовательские станции и сетевые устройства в один домен независимо от того, к какому физическому сегменту LAN они привязаны. Сети VLAN позволяют сделать более эффективным поток сетевого трафика в пределах подгрупп. Сети VLAN, управляемые программно, уменьшают время введения в действие изменений в сети.

Для сетей VLAN не задано минимальное количество портов, они могут быть созданы для блока, для устройства, для стека или любого другого типа соединения, так как сети VLAN создаются программным путем и не обладают физическими атрибутами.

Сети VLAN работают на уровне Layer 2. Поскольку они изолируют трафик внутри себя, для обеспечения трафика между сетями VLAN необходим маршрутизатор уровня Layer 3. Маршрутизаторы уровня Layer 3 идентифицируют сегменты и координируют их с сетями VLAN. Сети 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 VLAN или конечной станцией, или сетевым устройством. Метки VLAN также содержат сведения о приоритете сетей VLAN.

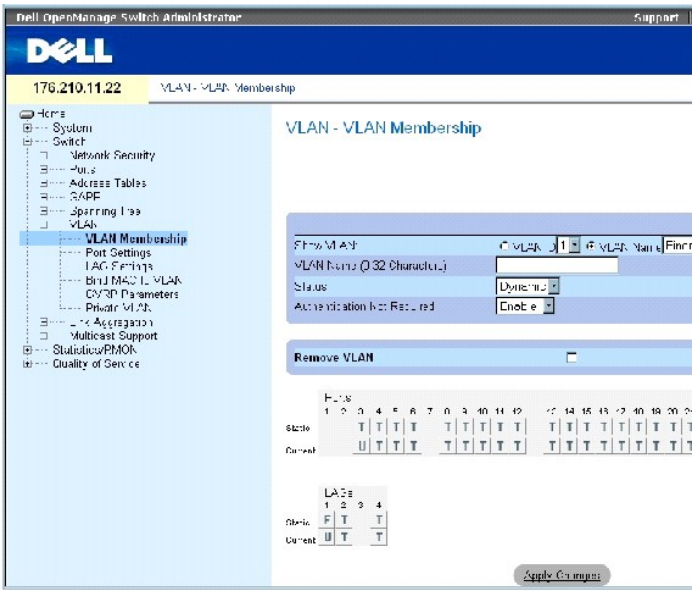
Совместное использование сетей VLAN и протокола GVRP позволяет менеджерам сети определять узлы сети в широковещательные домены. Широковещательный и многоадресный трафики ограничиваются исходной группой.

Чтобы открыть страницу **VLAN**, нажмите **Switch (Коммутатор)** → **VLAN** в панели дерева.

Определение членства в сети VLAN

На странице **Членство в сети VLAN** содержатся поля для определения групп VLAN. Коммутатор поддерживает назначение 4094 идентификаторов VLAN максимум для 256 сетей VLAN. Все порты должны иметь определенный идентификатор PVID. Если не настроено другое значение, используйте значение VLAN PVID по умолчанию. Сеть VLAN ID #1 задана по умолчанию и не может быть удалена из системы. Чтобы открыть страницу **Членство в сети VLAN**, щелкните **Switch (Коммутатор)** → **VLAN**→ **VLAN Membership (Членство в сети VLAN)** в панели дерева.

Рисунок 7-30. Членство в сети VLAN



На странице **Членство в сети VLAN** есть следующие поля:

Show VLAN (Показать VLAN) - Перечисляет и отображает специфическую информацию VLAN при вводе идентификатора VLAN ID или имени VLAN.

VLAN Name (Имя VLAN) (от 0 до 32 символов). Определенное пользователем название VLAN.

Status (Состояние) - Указывает тип VLAN. Возможные значения поля:

Dynamic (Динамическая) - Сеть VLAN создана динамически протоколом GVRP.

Static (Статическая) - Указывает, что сеть VLAN является пользовательской.

Default (По умолчанию) - Сеть VLAN, заданная по умолчанию.

Authentication Not Required (Идентификация не требуется) - Разрешает или запрещает неполномочным пользователям доступ к VLAN.

Remove VLAN (Удалить VLAN) - Удаляет VLAN из таблицы VLAN Membership Table.

Добавление новых сетей VLAN

1. Откройте страницу **Членство в сети VLAN**.
2. Нажмите кнопку **Add** (Добавить).

   Откроется страница **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 членства в сети VLAN

1. Откройте страницу **Членство в сети VLAN**.
2. Выберите VLAN в раскрывающемся списке **Show VLAN**.
3. Внесите необходимые изменения.
4. Нажмите кнопку **Apply Changes (Применить изменения)**.

   Информация о членстве в сети VLAN будет изменена, а устройство обновлено.

Удаление сетей VLAN

1. Откройте страницу **Членство в сети VLAN**.
2. Выберите в поле **Show VLAN** (Отобразить VLAN) сеть VLAN.
3. Установите флажок в поле **Remove VLAN** (Удалить VLAN).
4. Нажмите кнопку **Apply Changes (Применить изменения)**.

   Сеть VLAN будет удалена, а устройство обновлено.

Определение групп членства в сети VLAN с помощью команд консоли

В следующей таблице приведены команды консоли, соответствующие полям для определения групп членства в сети VLAN на странице VLAN Membership (Членство в сети VLAN).

Таблица 7-20. Команды страницы VLAN Membership Group

Команды консоли	Описание
vlan database	Включает режим конфигурации VLAN.
vlan {*vlan-range*}	Создает сеть VLAN.
name *string*	Добавляет имя в сеть VLAN.

Ниже 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
```

Таблица VLAN Port Membership

VLAN Port Membership Table (Таблица портов сети VLAN) - это **таблица назначения портов** в сети VLAN. Порты назначаются в сеть VLAN путем переключения **параметров управления** портом (Port Control). Порты могут иметь следующие значения:

Таблица 7-21. Таблица VLAN Port Membership

Порт	Определение
T	Интерфейс входит в сеть VLAN. Все пакеты, пересылаемые интерфейсом, помечаются. Пакеты содержат информацию о сети VLAN.
U	Интерфейс входит в сеть VLAN. Пакеты, пересылаемые интерфейсом, не помечаются.
F	Интерфейсу запрещено входить в сеть VLAN.
Нет значения	Интерфейс не входит в сеть VLAN. Пакеты, связанные с этим интерфейсом, через него не пересылаются.

В **VLAN Port Membership Table** (Таблице портов сети VLAN) отображаются порты и состояния портов, а также группы LAG.

Назначение портов в группу VLAN

1. Откройте страницу VLAN Membership (Членство в сети VLAN).
2. Щелкните переключатель **VLAN ID** или **VLAN Name** и выберите VLAN из раскрывающегося меню.
3. Выберите порт в таблице **Port Membership Table** и задайте ему значение.
4. Нажмите кнопку **Apply Changes (Применить изменения)**.

Порт будет назначен в группу VLAN, а устройство обновлено.

Удаление сети VLAN

1. Откройте страницу VLAN Membership (Членство в сети VLAN).
2. Щелкните переключатель **VLAN ID** или **VLAN Name** и выберите VLAN из раскрывающегося меню.
3. Установите флажок в поле **Remove VLAN** (Удалить VLAN).
4. Нажмите кнопку **Apply Changes (Применить изменения)**.

Сеть VLAN будет удалена, а устройство обновлено.

Назначение портов в сети VLAN с помощью команд консоли

В следующей таблице описаны команды для назначения портов в группы VLAN .

Таблица 7-22. Команды для назначения порта в группу VLAN

Команды консоли	Описание
switchport general acceptable-frame-types tagged-only	Отбрасывает входящие непомеченные кадры.
switchport forbidden vlan {**add** *vlan-list* | **remove** *vlan-list*}	Запрещает добавление указанных VLAN для порта.
switchport mode {access | trunk | general}	Настраивает режим членства порта в сети VLAN.
switchport access vlan vlan-id	Настраивает идентификатор VLAN, когда интерфейс находится в доступном режиме.
switchport trunk allowed vlan {add vlan-list | remove vlan-list}	Добавляет или удаляет сети VLAN из порта транка.
switchport trunk native vlan vlan-id	Определяет порт в качестве члена конкретной VLAN и указывает идентификатор сети VLAN в качестве идентификатора Port Default VLAN ID (PVID).
switchport general allowed vlan add vlan-list [tagged | untagged]	Добавляет или удаляет сети VLAN для порта в общем режиме.
switchport general pvid vlan-id	Настраивает идентификатор VLAN, когда интерфейс находится в общем режиме.

Ниже 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
```

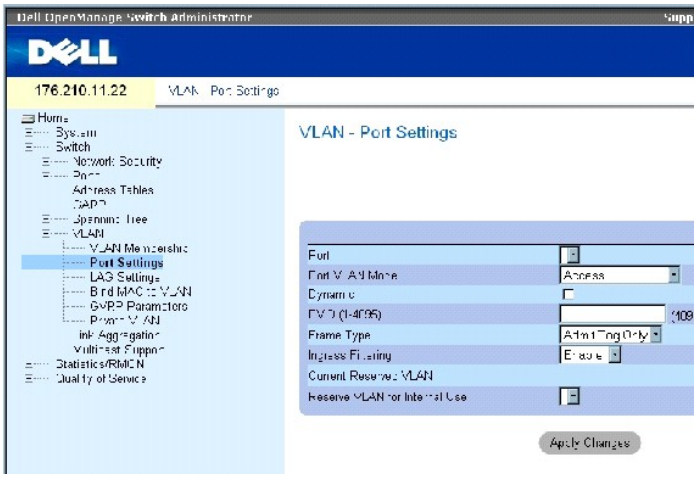
```
console(config)# interface
ethernet 1/e9



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 порта сети VLAN

На странице Параметры VLAN для порта содержатся поля для управления портами, входящими в состав сетиVLAN. Параметр идентификатора сети VLAN для порта по умолчанию (PVID) настраивается на странице Параметры VLAN для порта. Все непомеченные пакеты, поступающие на устройство, маркируются идентификатором PVID портов.

Чтобы открыть страницу Параметры VLAN для порта, щелкните **Switch (Коммутатор)** → **VLAN**→ **Port Settings (Параметры порта)** в панели дерева.

Рисунок 7-31. Параметры VLAN для порта



На странице Параметры VLAN для порта есть следующие поля:

Port - Номер порта, входящего в сеть VLAN.

Port VLAN Mode - Режим работы порта. Возможные значения поля:

General (Общий) - Указывает, что порт принадлежит к сетям VLAN, каждая из которых определена пользователем как помеченная или непомеченная (дуплексный режим 802.1Q).

Access (Доступен) - Указывает, что порт принадлежит к одной непомеченной группе VLAN. Когда порт находится в доступном режиме, типы пакетов, поступающих на порт, не отмечаются. В этом режиме нельзя включить/отключить фильтрацию на входе.

Trunk (Транк) - Порт принадлежит к сетям VLAN, все порты которой помечены (кроме одного порта, который может быть непомеченным).

PV**E** Promiscuous (Универсальный PVE) - Порт входит в состав универсальной сети PVE VLAN.

PVE **Promiscuous (Универсальный PVE)** - Порт входит в состав универсальной сети PVE VLAN.

PVE **Isolated (Изолированный PVE)** - Порт входит в состав изолированной сети PVE VLAN.

Dynamic (Динамический) - Назначает порт в сеть VLAN на основе MAC-адреса хоста-источника, подключенного к порту.

PVID - Назначает идентификатор сети VLAN для непомеченных пакетов. Возможные значения: 1-4095. На практике сети VLAN 4095 называются браковочными VLAN. Пакеты, предназначенные для браковочной VLAN, выбрасываются.

Frame Type (Тип кадра). Тип пакета, принимаемый портом. Возможные значения поля:

Admit Tag Only (Разрешить только помеченные). Порт принимает только помеченные пакеты.

Admit All (Разрешить все) - Указывает, что порт принимает и помеченные, и непомеченные пакеты.

Ingress Filtering (Фильтрация на входе). Включение или выключение фильтрации на входе порта. При фильтрации на входе пакеты, предназначенные для сетей VLAN, определенный порт которых не являются членом сети, выбрасываются.

Current Reserved VLAN (Текущая резервная сеть VLAN) - Сеть VLAN, отмеченная в настоящий момент как резервная.

Reserve VLAN for Internal Use (Резервная сеть VLAN для внутреннего использования) - Сеть VLAN, которую пользователь определил как резервную, если она не используется системой.

Назначение параметров порта

1. Откройте страницу Параметры VLAN для порта.
2. Выберите порт, для которого необходимо назначить параметры из раскрывающегося меню **Port (Порт)**.
3. Заполните остальные поля на странице
4. Нажмите кнопку **Apply Changes (Применить изменения)**.

Параметры VLAN для порта будут определены, а устройство обновлено.

Вывод таблицы портов VLAN

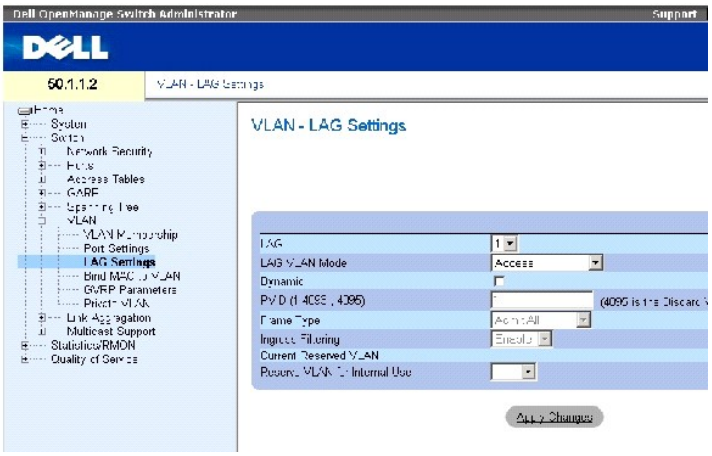
1. Откройте страницу Параметры VLAN для порта.
2. Нажмите кнопку **Show All** (Показать все).

Откроется страница **VLAN Port Table** (Таблица портов VLAN).

Определение параметров групп LAG в сети VLAN

На странице Параметры групп LAG в сетях VLAN приведены параметры для управления группами LAG, входящими в состав сети VLAN. Сети VLAN состоят из отдельных портов или групп LAG. Непомеченные пакеты, поступающие на устройство, маркируются идентификатором группы LAG, который задается по параметруPVID. Чтобы открыть страницу Параметры групп LAG в сетях VLAN, щелкните **Switch (Коммутатор)** → **VLAN**→ **LAG Settings (Параметры LAG)** в панели дерева.

Рисунок 7-32. Параметры групп LAG в сетях VLAN



На странице Параметры групп LAG в сетях VLAN есть следующие поля:

LAG - Номер LAG, входящего в сеть VLAN.

LAG VLAN Mode - Режим работы группы LAG в сети VLAN. Возможные значения поля:

General (Общий) - Указывает, что LAG принадлежит к сетям VLAN, каждая из которых определена пользователем как помеченная или непомеченная (дуплексный режим 802.1Q).

Access (Доступен) - Указывает, что группа LAG принадлежит к одной непомеченной группе VLAN.

Trunk (Транк) - LAG принадлежит к сетям VLAN, все порты которой помечены (кроме одного порта, который может быть непомеченным).

PVE Promiscuous (Универсальный PVE) - LAG входит в состав универсальной сети PVE VLAN.

PVE Community (Сообщество PVE) - LAG входит в состав сети сообщества PVE VLAN.

PVE Isolated (Изолированная PVE) - LAG входит в состав изолированной сети PVE VLAN.

Dynamic (Динамический) - Назначает LAG в сеть VLAN на основе MAC-адреса хоста-источника, подключенного к LAG.

PVID (1-4093 , 4095) - Назначает идентификатор сети VLAN для непомеченных пакетов. Возможные значения поля: 1-4095. На практике сети VLAN 4095 называются браковочными VLAN. Пакеты, предназначенные для браковочной VLAN, выбрасываются.

Frame Type (Тип кадра). Тип пакета, принимаемый группой LAG. Возможные значения поля:

Admit Tag Only (Разрешить только помеченные). LAG принимает только помеченные пакеты.

Admit All (Разрешить все). LAG принимает как помеченные, так и непомеченные пакеты.

Ingress Filtering (Фильтрация на входе). Включение или выключение фильтрации на входе LAG. При фильтрации на входе пакеты, предназначенные для сетей VLAN, определенная группа LAG которых не являются членом сети, выбрасываются.

Current Reserved VLAN (Текущая резервная сеть VLAN) - Сеть VLAN, отмеченная в настоящий момент как резервная.

Reserve VLAN for Internal Use (Резервная сеть VLAN для внутреннего использования) - Сеть VLAN, которая назначается резервной после перезагрузки устройства.

Назначение параметров для групп LAG в сетях VLAN

1. Откройте страницу Параметры групп LAG в сетях VLAN.
2. Выберите группу LAG из раскрывающегося меню **LAG** и заполните поля страницы.
3. Нажмите кнопку **Apply Changes (Применить изменения)**.

Параметры группы LAG сети VLAN будут определены, а устройство обновлено.

Вывод таблицы LAG VLAN

1. Откройте страницу Параметры групп LAG в сетях VLAN.
2. Нажмите кнопку **Show All** (Показать все).

Откроется страница **VLAN LAG Table** (Таблица групп LAG для VLAN).

Назначение групп LAG в сети VLAN с помощью команд консоли

В следующей таблице приведены команды консоли, соответствующие полям для назначения групп LAG в сети VLAN на странице Параметры групп LAG в сетях VLAN.

Таблица 7-23. Команды консоли для назначения LAG в сетях VLAN

Команды консоли	Описание
switchport mode {access | trunk | general}	Настраивает режим членства LAG в сети VLAN.
switchport trunk native vlan *vlan-id*	Определяет порт в качестве члена конкретной VLAN и указывает идентификатор сети VLAN в качестве идентификатора LAG Default VLAN ID (PVID).
switchport general pvid *идентификатор_vlan*	Настраивает идентификатор LAG VLAN ID (PVID), когда интерфейс находится в общем режиме.
switchport general allowed vlan add *vlan-list* [**tagged** | **untagged**]	Добавляет или удаляет сети VLAN из общей группы LAG.
switchport general acceptable-frame-type tagged-only	Отбрасывает входящие непомеченные пакеты.

switchport access vlan dynamic	Привязывает MAC-адрес к сети VLAN.
switchport general ingress-filtering disable	Отключает фильтрацию на входе LAG.

Ниже 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
```

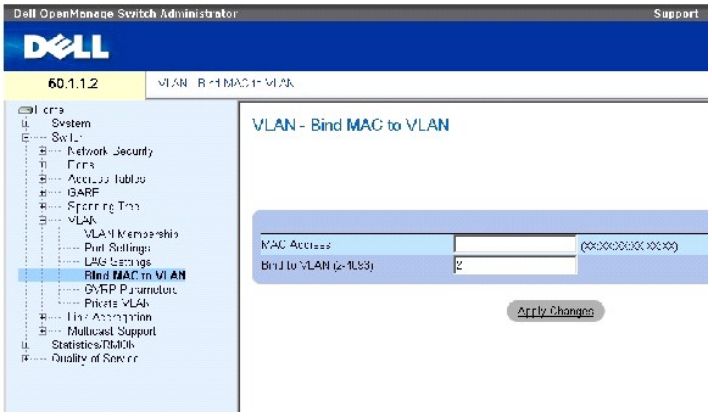
Привязка MAC-адреса к сетям VLAN

Привязка MAC-адресов к сетям VLAN используется для назначения портов для сети VLAN на основе MAC-адресов. После того, как сети VLAN назначен MAC-адрес, и этот адрес распознан при поступлении на порт, считается, что порт вошел в состав VLAN. По истечении срока действия MAC-адреса порт выходит из состава VLAN. Только динамические сети VLAN могут быть привязаны к MAC-адресам.

Чтобы привязать MAC-адреса к сети VLAN, убедитесь, что порты VLAN были добавлены динамически и не являются статическими портами VLAN.

Чтобы открыть страницу **Привязать MAC-адрес к сети VLAN**, щелкните **Switch (Коммутатор) → VLAN→ Bind MAC to VLAN (Привязать MAC-адрес к сети VLAN)** .

Рисунок 7-33. Привязать MAC-адрес к сети VLAN



На странице Привязать MAC-адрес к сети VLAN есть следующие поля:

MAC Address (MAC-адрес) - Указывает MAC-адрес, который привязан к сети VLAN.

Bind to VLAN (2-4093) (Привязка к VLAN) - Указывает сеть VLAN, к которой привязан MAC-адрес.

Отображение таблицы MAC to VLAN table:

1. Откройте страницу Привязать MAC-адрес к сети VLAN.
2. Нажмите кнопку **Show All** (Показать все).

Открывается таблица **MAC to VLAN table (MAC для VLAN)**.

Привязка MAC-адреса к сети VLAN с помощью командной строки:

В следующей таблице приведены команды консоли, предназначенные для привязки MAC-адресов к сетям VLAN.

Таблица 7-24. Привязка MAC-адреса к сети VLAN с помощью командной строки

Команды консоли	Описание

mac-to-vlan mac-address vlan-id	Привязывает MAC-адрес к сети VLAN.
switchport access vlan dynamic	Настраивает частные сети VLAN.
show mac-to-vlan	Отображение базы данных MAC to VLAN:
no mac-to-vlan mac-address	Удаляет привязку MAC-адреса к сети VLAN.

Ниже приведен пример команд консоли:

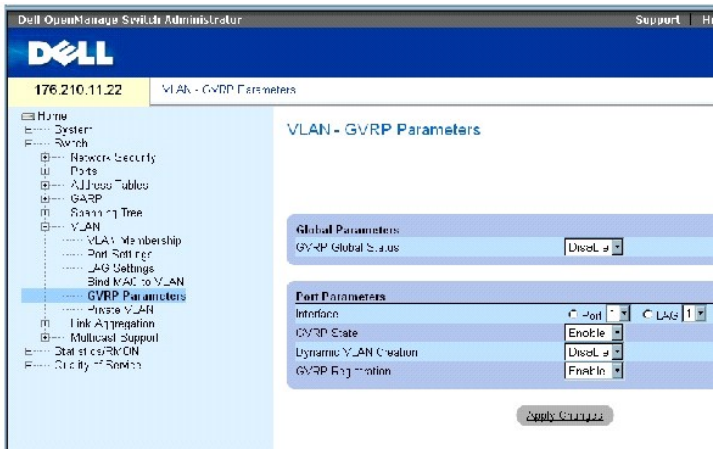
```
console(config-vlan)# mac-to-vlan 0060.704c.73ff 123

console(config-vlan)# exit

console(config)# exit

console# show vlan mac-to-vlan

MAC Address VLAN

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

0060.704c.73ff 123
```

Настройка параметров GVRP

Протокол GVRP (GARP VLAN Registration Protocol) специально предусмотрен для автоматического распределения информации о членстве в сетях VLAN между мостами, способными работать с сетью VLAN. Протокол GVRP позволяет таким мостам автоматически распознавать сети VLAN для назначения портов мостам, не настраивая отдельно каждый мост, и регистрировать членство в сети VLAN.

На странице **Параметры GVRP** выполняется общее включение протокола GVRP. Протокол GVRP можно также включить отдельно для каждого интерфейса. Чтобы открыть страницу **Параметры GVRP**, щелкните **Switch (Коммутатор) → VLAN→ GVRP Parameters (Параметры GVRP)** в панели дерева.

Рисунок 7-34. Параметры GVRP



На странице Параметры GVRP есть следующие поля:

GVRP Global Status (Общее состояние GVRP) - Включает и выключает протокол GVRP на устройстве. По умолчанию протокол GVRP отключен.

Interface (Интерфейс) - Порт или LAG для изменения параметров GVRP.

GVRP State (Состояние GVRP) - Включает или выключает протокол GVRP на интерфейсе.

Dynamic VLAN Creation (Динамическое создание VLAN) - Включает или выключает создание VLAN через протокол GVRP на интерфейсе.

GVRP Registration (Регистрация GVRP) - Включает или выключает регистрацию VLAN через протокол GVRP на интерфейсе.

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 сети VLAN через протокол GVRP

1. Откройте страницу GVRP Global Parameters (Общие параметры GVRP).
2. Выберите значение **Enable** (Включить) в поле **GVRP Global Status** (Общее состояние GVRP).
3. Выберите значение **Enable (Включить)** в поле GVRP State (Состояние GVRP) для необходимого интерфейса.
4. Выберите значение **Enable (Включить)** в поле **GVRP Registration (Регистрация GVRP)**.
5. Нажмите кнопку **Apply Changes (Применить изменения)**.

Регистрация сети VLAN на протоколе GVRP включена, а устройство обновлено.

Настройка протокола GVRP с помощью команд консоли

В следующей таблице приведены команды консоли, соответствующие конфигурации GVRP на странице GVRP Global Parameters (Общие параметры GVRP).

Таблица 7-25. Команды для вывода глобальных параметров GVRP

Команды 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 сети VLAN.
gvrp registration-forbid	Отменяет регистрацию всех динамических сетей VLAN и предотвращает динамическую регистрацию VLAN для порта.
show gvrp configuration [**ethernet** *interface*| **port-channel** *port-channel-number*]	Выводит сведения о конфигурации протокола GVRP, в том числе значения таймеров, разрешен ли протокол GVRP или динамическое создание сети VLAN и какие порты работают по протоколу GVRP.
show gvrp error-statistics [**ethernet** *interface* | **port-channel** *port-channel-number*]	Отображает статистику ошибок протокола GVRP.
show gvrp statistics [**ethernet** *interface* | **port-channel** *port-channel-number*]	Отображает статистику протокола GVRP.
clear gvrp statistics [**ethernet** *interface*| **port-channel** *port-channel-number*]	Сбрасывает всю статистику протокола GVRP.

Ниже 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

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

Настраивает частные сети VLAN

Частные сети VLAN (PVLAN) повышают безопасность сети за счет ограничения коммуникации между портами в сети VLAN. Частные сети VLAN снижают трафик сети на уровне Layer 2. Администраторы сети определяют первичную сеть VLAN. В состав первичной сети VLAN входят изолированные сети и сети VLAN для сообщества. Состояние портов частных сетей VLAN может быть следующим:

- **Promiscuous (Универсальный)** - Универсальные порты могут сообщаться со всеми портами сети PVLAN. Все универсальные пакеты автоматически назначаются как для изолированных VLAN, так и для VLAN сообщества.
- **Isolated (Изолированный)**- Изолированные порты полностью изолированы от других портов, входящих в сеть PVLAN. Но изолированные порты могут сообщаться с универсальными. Кроме того, трафик, который поступает с изолированных портов и на них, блокируется в сети VLAN. Это не распространяется на универсальные порты. Все изолированные порты автоматически назначаются для изолированных сетей VLAN.
- **Community (Сообщество)**- Порты сообщества взаимодействуют с другими портами сообщества, а также с универсальными. Порты сообщества отделены от всех других интерфейсов в других сообществах или от изолированных портов в той же самой сети PVLAN. Все порты сообщества автоматически назначаются для сетей сообщества VLAN и для частных сетей VLAN.

ПРИМЕЧАНИЕ. Порты не могут быть определены как универсальные или изолированные, если они входят в состав сети VLAN.

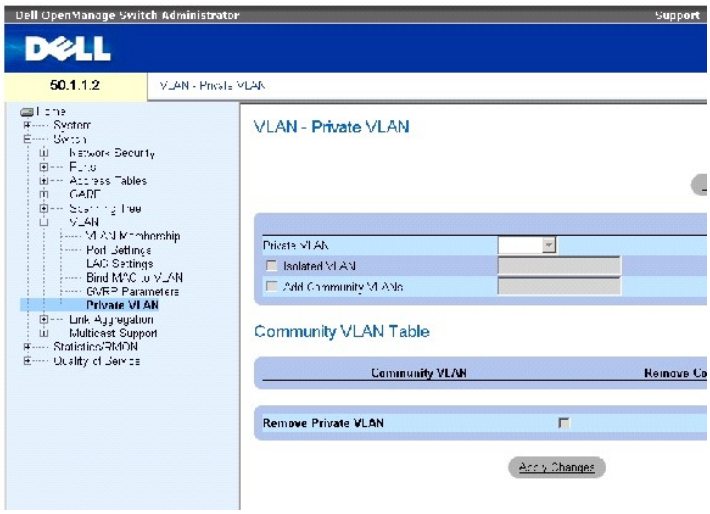
ПРИМЕЧАНИЕ. Предварительно созданные сети VLAN нельзя настроить как изолированные или как сети сообщества.

ПРИМЕЧАНИЕ. Изолированные сети и сети сообществ VLAN, включенные в общий список VLAN.

Если удалить первичную сеть VLAN, вместе с ней будут удалены изолированные сети и сети сообществ VLAN. Кроме того, изолированные сети и сети сообществ VLAN передают только непомеченный трафик.

Чтобы открыть страницу Private VLAN (Частные сети VLAN), щелкните **Switch (Коммутатор)** → **VLAN**→ **Private VLAN (Частная сеть VLAN)** в панели дерева.

Рисунок 7-35. Private VLAN (Частные сети VLAN)



На странице Private VLAN (Частные сети VLAN) есть следующие поля:

Private VLAN (Частная сеть VLAN) - Список пользовательских частых сетей VLAN. Определение частых сетей VLAN дано на странице **Добавить частные сети VLAN**.

Isolated VLAN (Изолированные сети VLAN)- Указывает, какая VLAN назначена на какие изолированные порты.

Add Community VLANs (Добавить VLAN сообществ) - Добавляет сеть VLAN сообществ, для которой назначены порты сообщества.

Community VLAN (VLAN сообщества)- Список сетей VLAN для сообщества.

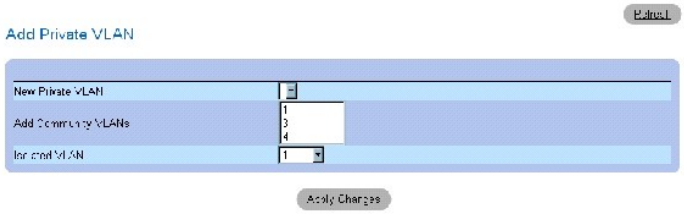
Remove Community (Удалить сообщество) - Удаляет сеть VLAN сообщества.

Remove Private VLAN (Удалить частную VLAN) - Удаляет частную сеть VLAN.

Как добавить частные сети VLAN

1. Откройте страницу **Private VLAN (Частные сети VLAN)**.
2. Нажмите кнопку **Add** (Добавить). Откроется страница **Добавить частные сети VLAN**.

Рисунок 7-36. Добавить частные сети VLAN



На странице Добавить частные сети VLAN есть следующие дополнительные поля:

New Private VLAN (Новые частные VLAN)- Список частных сетей VLAN. Сети VLAN для сообщества добавляются в список частных VLAN.

Add Community VLANs (Добавить VLAN сообщества)- Добавляет VLAN сообщества в список частных VLAN.

Isolated VLAN (Изолированные VLAN) - Добавляет изолированные VLAN в список частных VLAN.

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

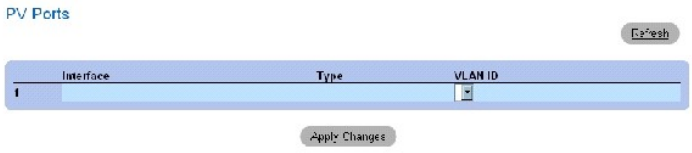
Частная сеть VLAN удалена, а устройство обновлено.

Вывод таблицы PV Ports Table

1. Откройте страницу Private VLAN (Частные сети VLAN).
2. Нажмите кнопку **Show PV Ports** (Показать порты PV).

Откроется страница **Таблица портов PV**.

Рисунок 7-37. Таблица портов PV



Настройка сетей PVLAN с использованием командной строки

В следующей таблице приведены команды консоли, соответствующие конфигурации PVLAN на странице **Private VLAN (Частные сети VLAN)**.

Таблица 7-26. Команды для частных сетей VLAN

Команды консоли	**Описание**
switchport mode private vlan promiscuous	**Добавляет универсальный порт в универсальную сеть VLAN.**
switchport mode private vlan community	**Добавляет порт сообщества в сеть сообщества.**
switchport mode private vlan isolated	**Добавляет изолированный порт в изолированную сеть VLAN.**
private-vlan primary	Определяет первичную сеть VLAN.
private-vlan community {add community-vlan-list | remove community-vlan-list }	Задает или удаляет VLAN сообщества из первичной сети VLAN.

private-vlan isolated	Определяет изолированную VLAN первичной сети
switchport private-vlan *pvlan* **[community** *cvlan***]**	Определяет порты частной VLAN**.**
show vlan private-vlan [primary vlan-id]	Отображает частную первичную сеть VLAN.

Ниже приведен пример команд консоли:

```
console(config)# vlan
database

console(config-vlan)# vlan
2

console(config-vlan)# exit

console(config)# interface
vlan 2

console(config-if)#
private-vlan primary

console(config)# interface
vlan 2

console(config-if)#
private-vlan isolated 10

console(config-if)#
private-vlan community add
20

console# show vlan
private-vlan

console(config-if)# end
```

Объединение портов

Объединение портов (Port Aggregation) оптимизирует использование портов, связывая между собой группу портов, формируя объединенную группу каналов LAG (Link Aggregated Group). Объединение портов увеличивает пропускную способность между устройствами, увеличивает гибкость портов и обеспечивает избыточность каналов.

Коммутатор 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 устанавливают между ними LAG.

При объединении портов необходимо учитывать следующее:

- Все порты в составе LAG должны иметь одинаковый тип носителя.
- Сеть VLAN не настраивается для порта.
- Порт не назначается для другой группы LAG.

- Режим автосогласования не настраивается для порта.
- Порт функционирует в полном дуплексном режиме.
- Все порты в составе LAG работают в одном режиме фильтрации на входе и маркировки.
- Все порты в составе LAG работают в одном режиме обратного давления и управления потоком.
- Все порты в составе LAG имеют одинаковый приоритет.
- Все порты в составе LAG имеют одинаковый тип трансивера.
- Коммутатор поддерживает до 8 групп LAG и до 8 портов на каждой группе LAG.
- Порты могут быть сконфигурированы как LACP, только если они не являются частью предварительно настроенной группы LAG.

Порты, добавленные в состав LAG, теряют свою индивидуальную конфигурацию. Если порт удаляется из LAG, к нему применяется конфигурация исходного порта.

Коммутатор использует функцию хеширования, чтобы определить, какие пакеты и на какой части объединенного канала выполняются. Функция хеширования статически выравнивает загрузку членов объединенного канала. Устройство интерпретирует объединенный канал как единый логический порт.

Определение параметров LACP

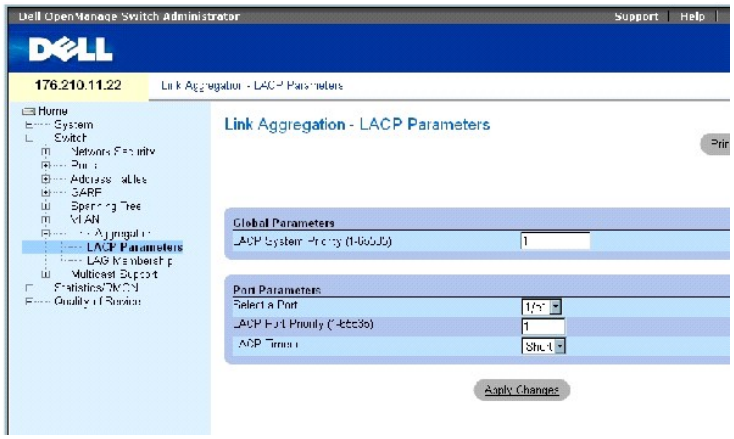
Объединенные порты могут быть связаны в группы портов объединенного канала. Объединенная группа каналов состоит из портов с одинаковой скоростью, работающих в дуплексном режиме.

Порты в группе Link Aggregated group (LAG) могут иметь разные типы носителей, если они работают на одной скорости. Объединенные каналы могут быть назначены вручную или автоматически путем включения протокола LACP (Link Aggregation Control Protocol) на соответствующих каналах.

Определение параметров протокола LACP

Страница **LACP Parameters** (Параметры LACP) содержит поля для настройки групп LAG протокола LACP. Объединенные порты могут быть связаны в группы портов объединенного канала. Каждая группа состоит из портов с одинаковой скоростью. Объединенные каналы могут быть назначены вручную или автоматически путем включения протокола LACP (Link Aggregation Control Protocol) на соответствующих каналах. Чтобы открыть страницу Параметры LACP, щелкните **Switch (Коммутатор)** → **Link Aggregation (Объединение канала)**→ **LACP Parameters (Параметры LACP)** в панели дерева.

Рисунок 7-38. Параметры LACP



На странице Параметры LACP есть следующие поля:

LACP System Priority (Системный приоритет 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 назначаются параметры паузы ожидания и приоритета.

LACP Port Priority (Портовый приоритет LACP)(1-65535) - Значение приоритета LACP для порта.

LACP Timeout - Административная пауза LACP. Возможные значения поля:

Short - Короткая пауза.

Long - Длинная пауза.

Определение общих параметров объединения канала

1. Откройте страницу Параметры LACP.
2. Заполните поле **LACP System Priority (Системный приоритет LACP)** .
3. Нажмите кнопку **Apply Changes (Применить изменения)**.

Параметры определены, а устройство обновлено.

Определение портовых параметров объединения канала

1. Откройте страницу Параметры LACP.
2. Заполните поля в области **Port Parameters (Параметры порта)**.
3. Нажмите кнопку **Apply Changes (Применить изменения)**.

Параметры определены, а устройство обновлено.

Вывод таблицы параметров LACP

1. Откройте страницу Параметры LACP.
2. Нажмите кнопку **Show All** (Показать все).

Откроется таблица параметров **LACP Parameters Table**.

Настройка параметров LACP с помощью команд консоли

В следующей таблице приведены команды консоли, соответствующие конфигурации параметров LACP на странице Параметры LACP.

Таблица 7-27. Команды консоли для параметров LACP

Команды консоли	Описание
lacp system-priority *значение*	Настраивает приоритет системы.
lacp port-priority *значение*	Настраивает приоритет физических портов.
lacp timeout {**long** | **short**}	Задает административную паузу LACP.
show lacp ethernet *interface* [**parameters** | **statistics** | **protocol-state**]	Выводит информацию о протоколе LACP для порта Ethernet.

Ниже 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
```

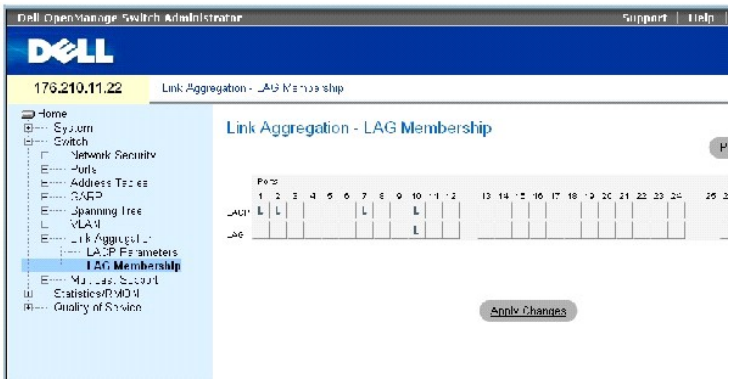
Определение членства в группе LAG

Коммутатор поддерживает до 8 групп LAG на систему и 8 портов на группу LAG независимо от его режима работы - автономного или в стеке.

Если порт добавляется в группу LAG, он получает свойства этой группы LAG. Если порт не может быть настроен со свойствами LAG, он не добавляется в группу. Выдается сообщение об ошибке. Однако, если не удается настроить первый входящий в группу LAG порт по параметрам LAG, порт добавляется в LAG с параметрами настройки по умолчанию. Выдается сообщение об ошибке. Тем не менее, этот порт будет единственным портом с параметрами по умолчанию в составе LAG.

Используйте страницу **Членство в группе LAG**, чтобы назначить порты в LAG. Чтобы открыть страницу **Членство в группе LAG**, щелкните **Switch (Коммутатор)** → **Link Aggregation (Объединение канала)**→ **LAG Membership (Членство в группе LAG)** в панели дерева.

Рисунок 7-39. Членство в группе LAG



На странице **Членство в группе LAG** есть следующие поля:

LACP - Интегрирует порт в LAG с использованием протокола LACP.

LAG. Добавление порта в группу LAG и определение конкретной группы LAG, которой принадлежит порт.

Добавление портов в LAG или LACP

1. Откройте страницу **Членство в группе LAG**.
2. В ряду LAG (второй ряд) переключите кнопку на конкретный номер, чтобы интегрировать или удалить порт для этого номера LAG.
3. В ряду LACP (первый ряд) переключите кнопку под номером порта, чтобы присвоить LACP или статическую сеть LAG.
4. Нажмите кнопку **Apply Changes (Применить изменения)**.

Порт будет добавлен в группу LAG или LACP, а устройство обновлено.

Добавление портов в группы LAG с помощью команд консоли

В следующей таблице приведены команды консоли, соответствующие полям для включения портов в группы LAG на странице **Членство в группе LAG**.

Таблица 7-28. Команды, связанные с членством LAG

Команды консоли	Описание
channel-group *port-channel-number* **mode** {**on** | **auto**}	Связывает порт с каналом порта. Эта команда используется для удаления конфигурации канал-группа из интерфейса.
show interfaces port-channel [*port-channel-number*]	Отображение информации порт-канал.

Ниже приведен пример команд консоли:

```
console(config)# interface
ethernet 1/e11

console(config-if)#
channel-group 1 mode on
```

Поддержка многоадресного трафика

Передача многоадресного трафика позволяет пересылать один пакет по нескольким адресатам. Передача многоадресного трафика уровня L2 основана на коммутаторе L2, который получает один пакет, адресованный нескольким адресатам. Она создает копии пакета и передает их на соответствующие порты.

Registered Multicast traffic (Зарегистрированный многоадресный трафик)- Если трафик адресован для зарегистрированной многоадресной группы, он обрабатывается по записи базы данных многоадресной фильтрации и отправляется на зарегистрированные порты.

Unregistered Multicast traffic (Незарегистрированный многоадресный трафик) - Если трафик адресован для незарегистрированной многоадресной группы, он обрабатывается по специальной записи базы данных многоадресной фильтрации. Настройка по умолчанию: заполнить весь трафик (трафик в незарегистрированной многоадресной группе).

Устройство поддерживает:

- **Forwarding L2 Multicast Packets (Пересылку многоадресных пакетов L2)** - Пересылает многоадресные пакеты уровня Layer 2. Многоадресная фильтрация на уровне Layer 2 включена по умолчанию, а не настраивается пользователем.

ПРИМЕЧАНИЕ. Система поддерживает многоадресную фильтрацию для 256 многоадресных групп.

- **Filtering L2 Multicast Packets (Фильтрацию многоадресных пакетов L2)** - Пересылает многоадресные пакеты уровня 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)**, нажмите **Switch (Коммутатор)** → **Multicast Support (Поддержка многоадресного трафика)**в панели дерева.

Определение общих параметров многоадресного трафика

Переключение Layer 2 пересылает многоадресные пакеты на все соответствующие порты VLAN по умолчанию, обрабатывая пакет как единственный многоадресный. Этот тип пересылки трафика эффективен, но не является оптимальным, так как несоответствующие порты также принимают многоадресные пакеты. Это вызывает общее увеличение сетевого трафика. Фильтры многоадресной пересылки позволяют отправлять пакеты Layer 2 на подмножества порта.

Когда наблюдение на базе IGMP включено в полном объеме, все пакеты IGMP пересылаются на процессор. Процессор анализирует входящие пакеты и определяет:

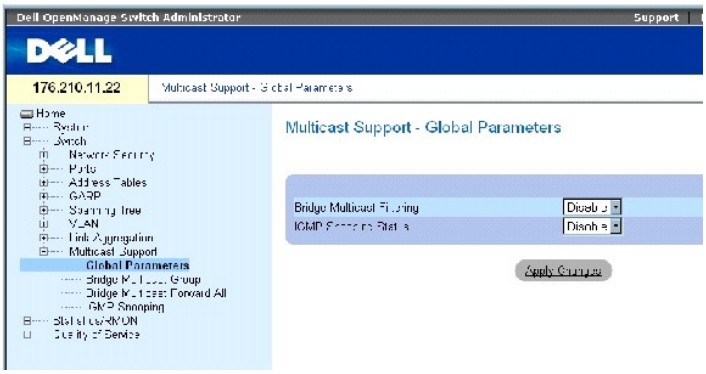
- Какие порты собираются вступить в какие многоадресные группы.
- Какие порты обладают многоадресными маршрутизаторами, генерирующими запросы IGMP.
- Какие протоколы маршрутизации передают пакеты и многоадресный трафик.

Порт, который собирается вступить в определенную многоадресную группу, выдает отчет IGMP, определяющий эту группу. В результате этого создается база данных многоадресной фильтрации.

Чтобы открыть страницу **Multicast Support (Поддержка многоадресного трафика)** , нажмите **Switch (Коммутатор)** → **Multicast Support (Поддержка многоадресного трафика)**в панели дерева.

На странице **Страница Global Parameters** имеются поля для включения отслеживания протокола IGMP на устройстве. Чтобы открыть страницу **Страница Global Parameters**, нажмите **Switch (Коммутатор)** → **Multicast Support (Поддержка многоадресного трафика)** → **Global Parameters (Глобальные параметры)** в панели дерева.

Рисунок 7-40. Страница Global Parameters



На странице **Страница Global Parameters** есть следующие поля:

Bridge Multicast Filtering (Фильтрация многоадресного трафика через мост) - Включает и выключает на устройстве фильтрацию многоадресного трафика через мост. По умолчанию установлено значение Disabled (Отключено).

IGMP Snooping Status (Состояние наблюдение на базе IGMP) - Включает или выключает наблюдение на базе протокола IGMP. По умолчанию установлено значение Disabled (Отключено). Наблюдение на базе IGMP можно включить только, если включен параметр **Страница Global Parameters**.

Включение на устройстве фильтрации многоадресного трафика через мост

1. Откройте страницу **Страница Global Parameters**.
2. Выберите **Enable** (Включено) в поле **Bridge Multicast Filtering** (Фильтрация многоадресного трафика через мост).
3. Нажмите кнопку **Apply Changes (Применить изменения)**.

На устройстве будет включена функция Bridge Multicast *Filtering* (Фильтрация многоадресного трафика через мост).

Включение на устройстве наблюдения на базе IGMP

1. Откройте страницу **Страница Global Parameters**.
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 команды консоли для включения фильтрации многоадресного трафика и наблюдения на базе IGMP на странице **Страница Global Parameters**.

Таблица 7-29. Команды консоли для включения фильтрации многоадресного трафика и наблюдения

Команды консоли	Описание
bridge multicast filtering	Включает фильтрацию многоадресных адресов.
ip igmp snooping	Включает наблюдение на базе протокола IGMP.

Ниже приведен пример команд консоли:

```
console(config)# bridge
```

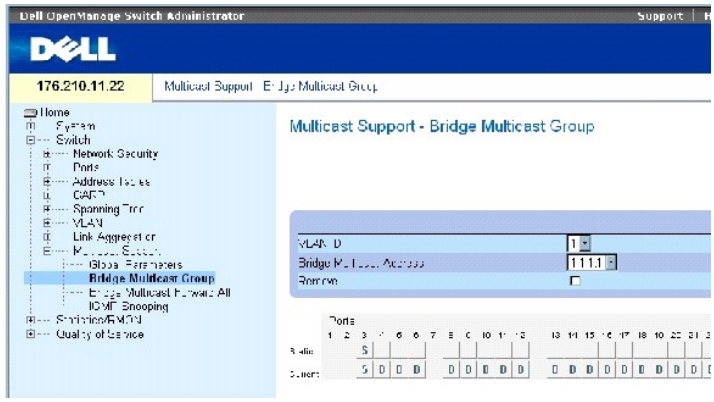
```
multicast filtering

console(config)# ip igmp
snooping
```

Добавление членов мостовой многоадресной группы

На странице **Многоадресная группа мостов** показаны порты и группы LAG, связанные с многоадресной группой в таблицах **Ports** и **LAGs**. Таблицы Port и LAG также отражают схему вхождения порта или LAG в многоадресную группу. Порты могут быть добавлены в существующую группу или в новые многоадресные группы. Страница **Многоадресная группа мостов** позволяет создавать новые многоадресные группы. На странице **Многоадресная группа мостов** также можно присвоить порты определенной многоадресной группе.

Чтобы открыть страницу **Многоадресная группа мостов** , нажмите **Switch (Коммутатор)** → **Multicast Support (Поддержка многоадресного трафика)** → **Bridge Multicast Group (Многоадресная группа мостов)** в панели дерева.

Рисунок 7-41. Многоадресная группа мостов



На странице **Многоадресная группа мостов** есть следующие поля:

VLAN ID (Идентификатор VLAN) - Указывает сеть VLAN и содержит сведения об адресе многоадресной группы.

Bridge Multicast Address - Указывает MAC-/IP-адреса многоадресной группы.

Remove - Если включено, адрес группы удаляется из группы.

Ports (Порты) - Список портов, которые могут быть добавлены в многоадресную передачу.

LAGs - Список LAG, которые могут быть добавлены в многоадресную передачу.

В следующей таблице приведены параметры для управления портом IGMP и членами LAG:

Таблица 7-30. Параметры управления таблицей членов портов / LAG для IGMP

Порт	Определение
D	Порт/группа LAG присоединена к многоадресной группе 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 Row* (Текущий).

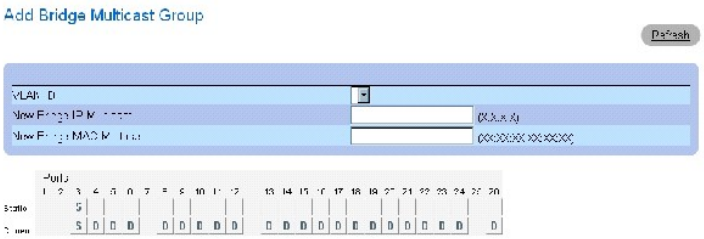
F	Forbidden (Запрещена)
Нет значения	Порт не закреплен за многоадресной группой.

Добавление членов мостовой многоадресной группы

1. Откройте страницу **Многоадресная группа мостов** .
2. Нажмите кнопку **Add** (Добавить).

Откроется страница **Add Bridge Multicast Group**.

Рисунок 7-42. Add Bridge Multicast Group



3. Определите поля **VLAN ID** и **New Bridge Multicast Address (Новый адрес мостовой группы)**.
4. Переключите порт в значение **S**, чтобы присоединить его к выбранной многоадресной группе.
5. Переключите порт в значение **F**, чтобы запретить добавление адресов многоадресной группы на определенный порт.
6. Нажмите кнопку **Apply Changes (Применить изменения)**.

Адрес будет добавлен в многоадресную группу, а устройство обновлено.

Определение портов для получения службы многоадресной пересылки

1. Откройте страницу **Многоадресная группа мостов** .
2. Определите поля **VLAN ID** и **Bridge Multicast Address (Адрес мостовой группы)** .
3. Переключите порт в значение **S**, чтобы присоединить его к выбранной многоадресной группе.
4. Переключите порт в значение **F**, чтобы запретить добавление адресов многоадресной группы на определенный порт.
5. Нажмите кнопку **Apply Changes (Применить изменения)**.

Порт будет назначен в многоадресную группу, а устройство обновлено.

Назначение групп LAG для получения службы многоадресной пересылки

1. Откройте страницу **Многоадресная группа мостов** .
2. Определите поля **VLAN ID** и **Bridge Multicast Address (Адрес мостовой группы)** .
3. Переключите LAG в значение **S**, чтобы присоединить ее к выбранной многоадресной группе.
4. Переключите LAG в значение **F**, чтобы запретить добавление адресов многоадресной группы на заданную LAG.
5. Нажмите кнопку **Apply Changes (Применить изменения)**.

LAG будет назначена в многоадресную группу, а устройство обновлено.

Управление членами службы многоадресной пересылки с помощью команд консоли

В следующей таблице приведены команды консоли, соответствующие полям для управления членами службы многоадресной пересылки на странице **Многоадресная группа мостов** .

Таблица 7-31. Команды службы многоадресной пересылки

Команды консоли	Описание
bridge multicast address {*mac-multicast-address* | *ip-multicast-address*}	Регистрирует адреса для многоадресной передачи на уровне MAC-адресов для таблицы мостов и добавляет в группу статические порты.
bridge multicast forbidden address {*mac-multicast-address* | *ip-multicast-address*}[**add** | **remove**] {**ethernet** *interface-list* | **port-channel** *port-channel-number-list*}	Запрещает добавление определенного адреса многоадресной группы на определенный порт. Используйте эту команду с отрицанием no, чтобы вернуться к параметру по умолчанию.
show bridge multicast address-table [**vlan** *vlan*-id] [**address** {*mac-multicast-address* | *ip-multicast-address*}] [**format ip** | **mac**]	Выводит сведения таблицы MAC-адресов для многоадресной пересылки.

Ниже 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	

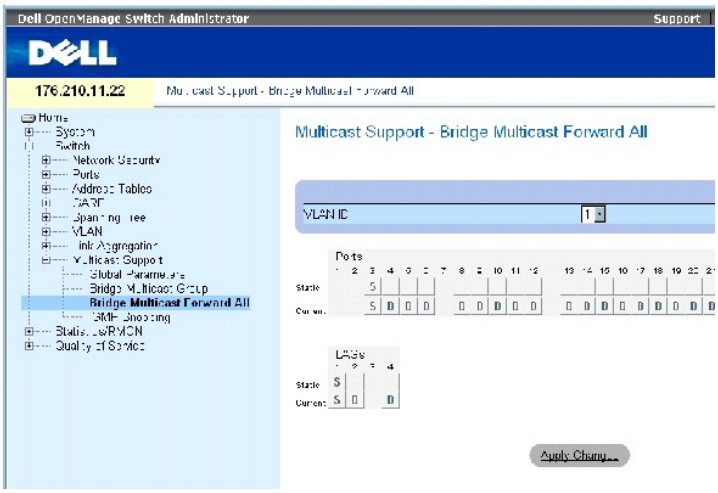
```
console # show bridge multicast address-table format ip

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 передачи всем

На странице **Страница Bridge Multicast Forward All** содержатся поля для привязки портов или LAG к коммутатору, связанному с соседним маршрутизатором или коммутатором для многоадресной пересылки. После того как наблюдение по протоколу IGMP включено, многоадресные пакеты пересылаются соответствующему порту или сети VLAN.

Чтобы открыть страницу **Страница Bridge Multicast Forward All**, нажмите **Switch (Коммутатор)** → **Multicast Support (Поддержка многоадресного трафика)** → **Страница Bridge Multicast Forward All** в панели дерева.

Рисунок 7-43. Страница Bridge Multicast Forward All



На странице Страница Bridge Multicast Forward All есть следующие поля:

VLAN ID - Идентификатор сети VLAN.

Ports (Порты) - Список портов, которые могут быть добавлены в многоадресную передачу.

LAGs - Список LAG, которые могут быть добавлены в многоадресную передачу.

В таблице **Bridge Multicast Forward All Switch / / Port Control Settings Table (Управление маршрутизатором / портом для моста многоадресной пересылки всем)** приведены параметры управления параметрами маршрутизатора и порта.

Managing Bridge Multicast Forward All Switch / Port Control Settings Table (Управление маршрутизатором / портом для моста многоадресной пересылки всем)

В следующей таблице описаны элементы управления, используемые для настройки управления портом.

Таблица 7-32. Bridge Multicast Forward All Switch//Port Control Settings Table (Управление маршрутизатором / портом для моста многоадресной пересылки всем)

Порт	Определение
D	Связывает порт с многоадресным маршрутизатором или коммутатором как динамический порт.
S	Связывает порт с многоадресным маршрутизатором или коммутатором как статический порт.
F	Forbidden (Запрещена)
Нет значения	Порт не закреплен за многоадресным маршрутизатором или коммутатором.

Привязка порта к многоадресному маршрутизатору или коммутатору

1. Откройте страницу **Страница Bridge Multicast Forward All**.
2. Определите поле **VLAN ID** (Идентификатор VLAN).
3. Выберите порт в таблице **Ports** и задайте ему значение.
4. Нажмите кнопку **Apply Changes (Применить изменения)**.

Порт подключен к маршрутизатору или коммутатору многоадресной передачи.

Привязка LAG к многоадресному маршрутизатору или коммутатору

1. Откройте страницу **Страница Bridge Multicast Forward All**.
2. Определите поле **VLAN ID** (Идентификатор VLAN).
3. Выберите порт в таблице **LAGs** и задайте ему значение.
4. Нажмите кнопку **Apply Changes (Применить изменения)**.

LAG подключена к маршрутизатору или коммутатору многоадресной передачи.

Управление группами LAG и портами, связанными с многоадресными маршрутизаторами с помощью команд консоли

В следующей таблице приведены команды консоли для управления группами LAG и портами, подключенными к маршрутизатору многоадресной передачи, на странице **Страница Bridge Multicast Forward All**.

Таблица 7-33. Управление группами LAG и портами, связанными с многоадресными маршрутизаторами с помощью команд консоли

Команды консоли	Описание
show bridge multicast filtering *vlan-id*	Выводит конфигурацию фильтрации многоадресной группы.
bridge multicast forward-all {**add** | **remove**} {**ethernet** *interface-list* | **port-channel** *port-channel-number-list*}	Разрешает пересылку всех многоадресных пакетов для порта. Используйте эту команду с отрицанием no, чтобы вернуться к параметру по умолчанию.

Ниже 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)
```

Отслеживание протокола IGMP

На странице **IGMP Snooping (Отслеживание IGMP)** содержатся поля для включения отслеживания IGMP по сети VLAN, и определения истечения срока действия для пакетов. Чтобы открыть страницу **Отслеживание протокола IGMP**, нажмите **Switch (Коммутатор)** → **Multicast Support (Поддержка многоадресного трафика)** → **IGMP Snooping (Отслеживание IGMP)** в панели дерева.

Рисунок 7-44. Отслеживание протокола IGMP

VLAN ID - Идентификатор сети VLAN.

IGMP Snooping Status (Состояние наблюдение на базе IGMP) - Включает или выключает наблюдение на базе протокола IGMP в сети VLAN.

Auto Learn (Атоматическое распознавание) - Включает или выключает автоматическое распознавание на коммутаторе Ethernet.

Host Timeout (1-2147483647) (Время ожидания хоста) - Время, по истечении которого запись наблюдения по протоколу IGMP устаревает. Значение по умолчанию: 260секунд.

Multicast Router Timeout (1-2147483647) (Время ожидания многоадресного маршрутизатора) - Время, по истечении которого запись многоадресного маршрутизатора устаревает. Значение по умолчанию: 300 секунд.

Leave Time Out (0-2147483647) (Время старения) - Время в секундах после получения сообщения портом и до истечения срока хранения записи. Значение по умолчанию: 10 секунд.

Включение на устройстве наблюдения на базе IGMP

1. Откройте страницу **Отслеживание протокола IGMP**.
2. Выберите идентификатор VLAN ID того устройства, на котором необходимо включить наблюдение на базе IGMP.
3. Выберите **Enable** (Включено) в поле **IGMP Snooping Status** (Состояние наблюдения на базе IGMP).
4. Заполните поля на странице.
5. Нажмите кнопку **Apply Changes (Применить изменения)**.

Наблюдение на базе IGMP будет включено на этом устройстве.

Вывод таблицы наблюдения по протоколу IGMP:

1. Откройте страницу **Отслеживание протокола IGMP**.
2. Нажмите кнопку **Show All** (Показать все).

Откроется страница **IGMP Snooping Table** (Таблица наблюдения по протоколу IGMP).

Настройка наблюдения по протоколу IGMP с помощью команд консоли

В следующей таблице приведены команды консоли, соответствующие полям на странице Отслеживание протокола IGMP.

Таблица 7-34. Команды для отслеживания на базе IGMP

Команды консоли	Описание
ip igmp snooping	Включает наблюдение на базе протокола IGMP.
ip igmp snooping mrouter learn-pim-dvmrp	Включает автоматическое распознавание портов многоадресного маршрутизатора в контексте конкретной сети VLAN.
ip igmp snooping host-time-out time-out	Настраивает время ожидания хоста.
ip igmp snooping mrouter-time-out *time-out*	Настраивает время ожидания маршрутизатора.
ip igmp snooping leave-time-out {*time-out* | **immediate-leave**}	Настраивает время старения хоста.
show ip igmp snooping groups [**vlan** *vlan-id*] [**address** *ip-multicast-address*]	Отображает многоадресные группы по результатам отслеживания IGMP.
show ip igmp snooping interface *vlan-id*	Отображает конфирурацию отслеживания на базе IGMP
show ip igmp snooping mrouter [interface vlan-id]	Выводит сведения о динамически распознаваемых интерфейсах многоадресного маршрутизатора.

Ниже 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)# ip igmp
snooping leave-time-out 60

console(config-if)# end

console# show ip igmp snooping
groups
```

Vlan	IP Address	Querier	Ports

------	-----------------	---------	---------
1	224-239.130|2.2.3	Yes	1/e11, 1/e12
19	224-239.130|2.2.8	Yes	1/e11-13

```
console# show ip igmp snooping
interface 1/e1


IGMP Snooping is globally enabled


IGMP Snooping is enabled on VLAN 1


IGMP host timeout is 300 sec


IGMP Immediate leave is disabled.
IGMP leave timeout is 60 sec


IGMP mrouter timeout is 200 sec


Automatic learning of multicast
router ports is enabled


console# show ip igmp snooping
mrouter
```

VLAN	Ports		
----	------		
1	1/e11		

Назад на страницу Содержание

Назад на страницу Содержание

Просмотр статистики

Системы Dell™ PowerConnect™ 34XX Руководство пользователя

На **страницах статистики** содержится информация по интерфейсу, протоколу GVRP, базе Etherlike, удаленному мониторингу (RMON) и использованию устройств. Чтобы открыть страницу **Statistics (Статистика)**, выберите **Statistics (Статистика)** в панели дерева.

ПРИМЕЧАНИЕ. Режим командной строки не применяется к страницам статистики.

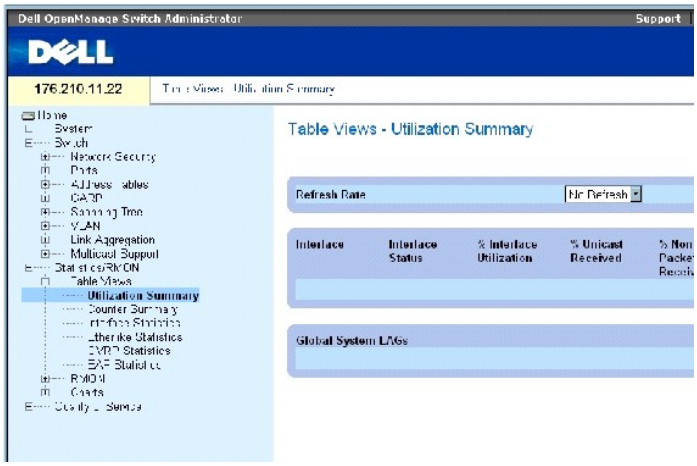
Просмотр таблиц

Страница **Table View** (Просмотр в виде таблиц) содержит ссылки для отображения статистики в виде таблицы. Чтобы открыть страницу, нажмите **Statistics (Статистика→Table (Таблица)** в панели дерева.

Просмотр сводки по использованию

На странице Сводка по использованию приведены статистические данные по использованию интерфейса. Чтобы открыть страницу, нажмите**Statistics (Статистика)→ Table Views (Просмотр в виде таблиц) → Utilization Summary (Сводка по использованию)** в панели дерева.

Рисунок 8-1. Сводка по использованию



ПРИМЕЧАНИЕ. Экран периодически обновляется, чтобы минимизировать влияние на компьютеры с малым объемом памяти. Во время этого процесса на экране могут возникнуть помехи.

На странице Сводка по использованию есть следующие поля:

Refresh Rate - Время, по истечении которого происходит обновление статистики интерфейса.

Interface - Номер интерфейса.

Interface Status - Состояние интерфейса.

% Interface Utilization - Процент использования интерфейса в сети, исходя из интерфейса, работающего в дуплексном режиме. Значение этого поля: от 0 до 200%. Максимальное показание, равное 200% для полной дуплексной связи, свидетельствует о том, что используется 100% пропускной способности всех соединений, пропускающих трафик через интерфейс. Максимальное показание для соединения в полудуплексном режиме равно 100%.

% Unicast Received - Процент адресных пакетов с односторонней передачей, полученных на порт.

% Non Unicast Packets Received - Процент адресных пакетов с передачей, отличной от односторонней, полученных на порт.

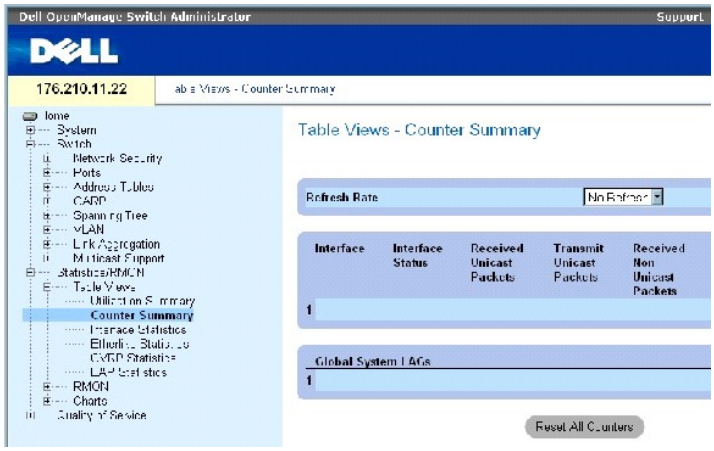
% Error Packets Received - Количество ошибочных пакетов, полученных на порт.

Global System LAGs - Указывает текущее общее использование групп LAG.

Просмотр сводки по счетчикам

На странице **Сводка по счетчикам** содержится статистика по использованию портов в числовом виде (а не в процентном). Чтобы открыть страницу **Сводка по счетчикам**, нажмите **Statistics/RMON (Статистика/RMON)→ Table Views (Просмотр в виде таблиц) → Counter Summary (Сводка по счетчикам)** в панели дерева.

Рисунок 8-2. Сводка по счетчикам



На странице **Сводка по счетчикам** есть следующие поля:

Refresh Rate - Время, по истечении которого происходит обновление статистики интерфейса.

Interface - Номер интерфейса.

Interface Status - Состояние интерфейса.

Received Unicast Packets - Процент адресных пакетов с односторонней передачей, полученных на порт.

Transmit Unicast Packets - Количество адресных пакетов с односторонней передачей, полученных с порта.

Received Non Unicast Packets - Количество адресных пакетов с передачей, отличной от односторонней, полученных на порт.

Transmit NonUnicast Packets - Количество адресных пакетов с передачей, отличной от односторонней, полученных с порта.

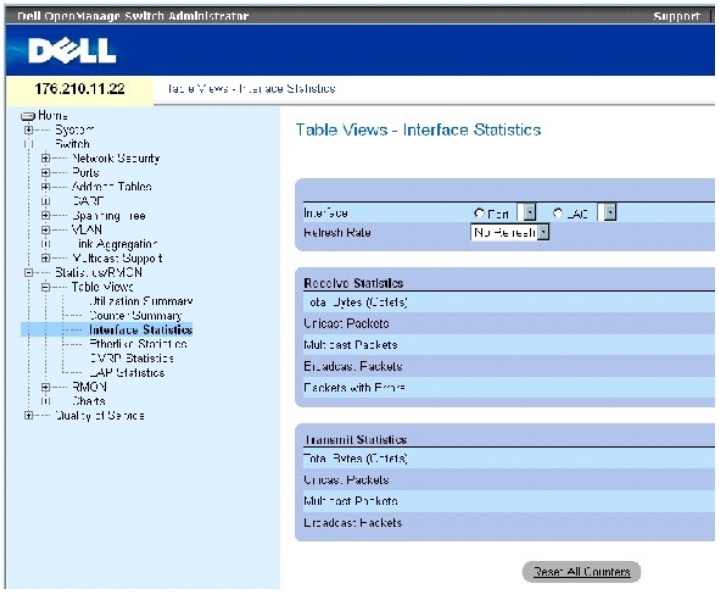
Received Errors - Количество ошибочных пакетов, полученных на порт.

Global System LAGs - Сводка по счетчикам для всей системы групп LAG.

Просмотр статистики интерфейса

На странице **Статистика интерфейса** содержится статистика по полученным и отправленным пакетам. Поля одинаковы как для полученных, так и для отправленных пакетов. Чтобы открыть страницу **Статистика интерфейса** , нажмите **Statistics/RMON (Статистика/RMON)→ Table Views (Просмотр в виде таблиц) → Interface Statistics (Статистика интерфейса)** в панели дерева.

Рисунок 8-3. Статистика интерфейса



На странице **Статистика интерфейса** есть следующие поля:

Interface (Интерфейс). Определяет порт или группу LAG, для которой отображается статистика.

Refresh Rate (Частота обновления). Объем времени перед обновлением статистики.

Получение статистики

Total Bytes (Octets) - Количество байт, полученных на выбранный интерфейс.

Unicast Packets - Количество адресных пакетов, полученных на выбранный интерфейс.

Multicast Packets - Количество многоадресных пакетов, полученных на выбранный интерфейс.

Broadcast Packets - Количество пакетов широковещательной адресации, полученных на выбранный интерфейс.

Передача статистики

Total Bytes (Octets) - Количество байт, отправленных с выбранного интерфейса.

Unicast Packets - Количество адресных пакетов, отправленных с выбранного интерфейса.

Multicast Packets - Количество многоадресных пакетов, отправленных с выбранного интерфейса.

Broadcast Packets - Количество пакетов широковещательной адресации, отправленных с выбранного интерфейса.

Отображение статистики интерфейса

1. Откройте страницу **Статистика интерфейса**.
2. Выберите поле **Interface** (Интерфейс).

На экране появится статистика для выбранного интерфейса.

Сброс статистических счетчиков интерфейса

1. Откройте страницу **Статистика интерфейса**.
2. Нажмите кнопку **Reset All Counters** (Сбросить все счетчики).

Показания статистических счетчиков интерфейса сброшены.

Просмотр статистики интерфейса с помощью команд консоли

В таблице приводятся команды консоли для просмотра статистики интерфейса.

Таблица 8-1. Команды страницы Interface Statistics

Команды консоли	Описание
show interfaces counters [**ethernet** *interface* | **port- channel** *port-channel-number*]	Отображает трафик, видимый на физическом интерфейсе.

Ниже приведен пример команд консоли:

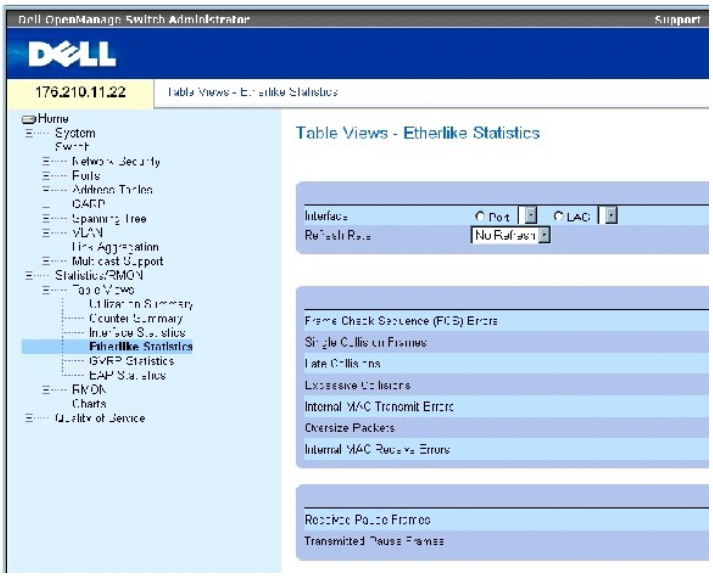
```
console> enable (âêëþ÷èòü)
```

```
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 базы Etherlike

На странице **Статистика базы Etherlike** приведены статистические данные по ошибкам интерфейса. Чтобы открыть страницу**Статистика базы Etherlike** , нажмите **Statistics/RMON (Статистика/RMON)→ Table Views (Просмотр в виде таблиц) → Etherlike Statistics (Статистика базы Etherlike)** в панели дерева.

Рисунок 8-4. Статистика базы Etherlike



На странице **Статистика базы Etherlike** есть следующие поля:

Interface (Интерфейс). Определяет порт или группу LAG, для которой отображается статистика.

Refresh Rate (Частота обновления). Объем времени перед обновлением статистики.

Frame Check Sequence (FCS) Errors - Количество ошибок последовательности проверки кадра, полученных на выбранный интерфейс.

Single Collision Frames - Количество одиночных коллизий в кадрах, полученных на выбранный интерфейс.

Late Collision - Количество поздних коллизий, полученных на выбранный интерфейс.

Oversize Packets - Количество пакетов с размером, превышающим максимально возможный, полученных на выбранный интерфейс.

Internal MAC Transmit Errors - Количество внутренних ошибок управления доступом к среде передачи (Internal MAC Transmit), полученных на выбранный интерфейс.

Received Pause Frames - Количество кадров паузы, полученных на выбранный интерфейс.

Transmitted Pause Frames - Количество кадров паузы, отправленных с выбранного интерфейса.

Отображение статистики базы Etherlike на интерфейсе

1. Откройте страницу Статистика базы Etherlike.
2. Выберите поле **Interface** (Интерфейс).

Сборс статистики базы Etherlike

1. Откройте страницу Статистика базы Etherlike.
2. Нажмите кнопку **Reset All Counters** (Сбросить все счетчики).

Счетчики Статистика базы Etherlike переустановлены.

Просмотр статистики Etherlike с помощью команд консоли

В таблице приводятся команды консоли для просмотра статистики etherlike.

Таблица 8-2. Команды страницы Etherlike Statistics

Команды консоли	Описание
show interfaces counters [**ethernet** *interface* | **port**- **channel** port-channel-number]	Отображает трафик, видимый на физическом интерфейсе.

Ниже приведен пример команд консоли:

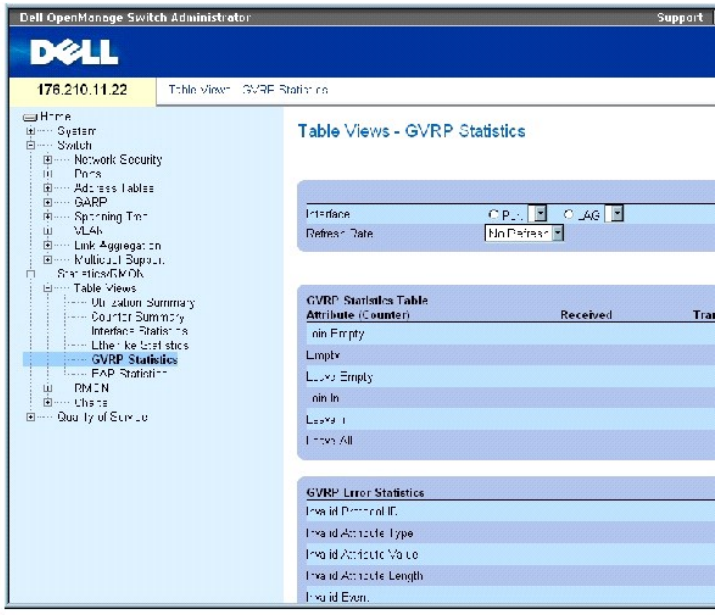
```
Console# show interfaces counters ethernet 1/1

Port    IN Octets   InUcastPkts  InMcastPkts  InBcastPkts
----    ---------   -----------  -----------  -----------
1/e1    183892      1289         987          8

Port    OUT         OutUcastPkts OutMcastPkts OutBcastPkts
        Octets
----    ---------   ------------ ------------ ------------
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 GVRP

На **Статистика GVRP** содержится статистика для протокола GVRP. Чтобы открыть страницу, нажмите **Statistics/RMON (Статистика/RMON)→ Table Views (Просмотр в виде таблиц) → GVRP Statistics (Статистика GVRP)** в панели дерева.

Рисунок 8-5. Статистика GVRP



На странице **Статистика GVRP** есть следующие поля:

Interface (Интерфейс). Определяет порт или группу LAG, для которой отображается статистика.

Refresh Rate (Частота обновления). Объем времени перед обновлением статистики.

Join Empty - Отображает статистику Join Empty протокола GVRP для устройства.

Leave Empty - Отображает статистику Leave Empty протокола GVRP для устройства.

Empty - Отображает количество пустых полей в статистике GVRP.

Join In - Отображает статистику Join In протокола GVRP для устройства.

Leave In - Отображает статистику Leave in протокола GVRP для устройства.

Leave All - Отображает статистику Leave all протокола GVRP для устройства.

Invalid Protocol ID - Отображает статистику Invalid Protocol ID протокола GVRP для устройства.

Invalid Attribute Type - Отображает статистику Invalid Attribute Type протокола GVRP для устройства.

Invalid Attribute Type - Отображает статистику Invalid Attribute Type протокола GVRP для устройства.

Invalid Attribute Length - Отображает статистику Invalid Attribute Length протокола GVRP для устройства.

Invalid Event - Отображает статистику Invalid Event протокола GVRP для устройства.

Отображение статистики GVRP для порта

1. Откройте страницу **Статистика GVRP**.
2. Выберите поле **Interface** (Интерфейс).

На экране появится статистика GVRP для выбранного интерфейса.

Сброс статистики GVRP

1. Откройте страницу **Статистика GVRP**.
2. Нажмите кнопку **Reset All Counters** (Сбросить все счетчики).

Показания статистических счетчиков GVRP сброшены.

Просмотр статистики протокола GVRP с помощью команд консоли

В таблице приводятся команды консоли для просмотра статистики GVRP.

Таблица 8-3. Команды страницы GVRP Statistics

Команды консоли	Описание
show gvrp statistics [**ethernet** *interface* | **port-channel** *port- channel-number*]	Отображает статистические данные GVRP.
show gvrp error- statistics [**ethernet** *interface* | **port-channel** *port-channel-number*]	Отображает статистику ошибок протокола GVRP.

Ниже 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 0

1/e2 0 0 0 0 0 0 0

1/e3 0 0 0 0 0 0 0

1/e4 0 0 0 0 0 0 0
```

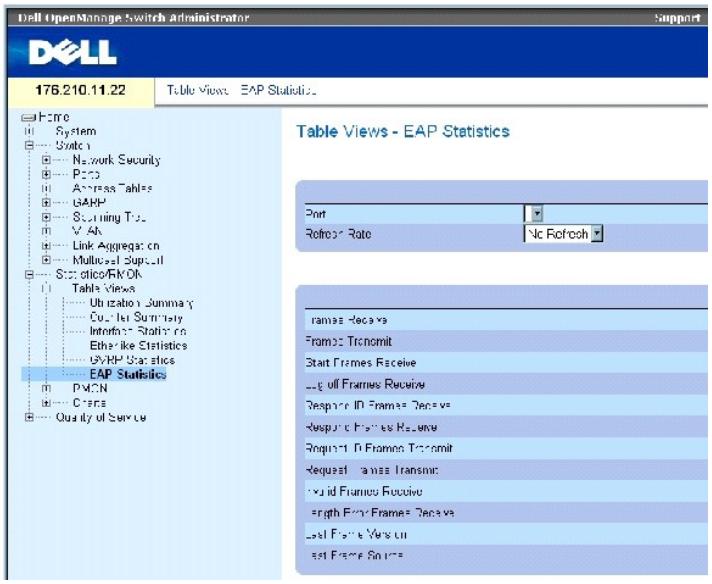
```
sLE : Leave Empty Sent

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

На странице **Статистика EAP** содержится информация по пакетам EAP, полученным на определенный порт. Более подробную информацию о EAP см. в разделе **Конфигурация идентификации на основе портов**. Чтобы открыть страницу **Статистика EAP** , нажмите Statistics/RMON (Статистика/RMON)→ Table Views (Просмотр в виде таблиц) → EAP Statistics (Статистика EAP) в панели дерева.

Рисунок 8-6. Статистика EAP



На странице **Статистика EAP** есть следующие поля:

Port (Порт) - Порт, с которого запрашивается статистика.

Refresh Rate- (Частота обновления)- Объем времени перед обновлением статистики.

Frames Receive (Полученные кадры) - Указывает количество действительных кадров EAPOL, полученных на порт.

Frames Transmit (Отправленные кадры) - Указывает количество действительных кадров EAPOL, отправленных с порта.

Start Frames Receive (Полученные стартовые кадры) - Указывает количество действительных стартовых кадров EAPOL, полученных на порт.

Log off Frames Receive (Полученные выходные кадры) - Указывает количество действительных выходных кадров EAPOL, полученных на порт.

Respond ID Frames Receive (Полученные кадры Respond ID) - Указывает количество действительных Resp/Id кадров EAP, полученных на порт.

Respond Frames Receive (Полученные кадры Respond) - Указывает количество действительных кадров Response EAP, полученных на порт.

Request ID Frames Transmit (Отправленные кадры Request ID) - Указывает количество действительных Req/Idкадров EAP, отправленных с порта.

RequestFrames Transmit (Отправленные кадры Request) - Указывает количество действительных кадров Request EAP, отправленных с порта.

Invalid Frames Receive (Полученные недействительные кадры) - Указывает количество нераспознанных кадров EAPOL, полученных на порт.

Length Error Frames Receive (Полученные кадры ошибочной длины) Указывает количество кадров EAPOL с ошибкой длины Packet Body Length, полученных на порт.

Last Frame Version (Версия последнего кадра) - Указывает номер версии протокола, привязанного к последнему полученному кадру EAPOL.

Last Frame Source (Источник последнего кадра) - Указывает MAC-адрес источника, привязанного к последнему полученному кадру EAPOL.

Вывод статистики EAP для порта

1. Как открыть страницу **Статистика EAP**.
2. Выберите поле **Interface** (Интерфейс).

Отображается статистика EAP.

Как сбросить показатели статистики EAP

1. Как открыть страницу **Статистика EAP**.
2. Нажмите кнопку **Reset All Counters** (Сбросить все счетчики).

Показания статистических счетчиков EAP сброшены.

Просмотр статистики EAP с помощью команд консоли

В таблице приводятся команды консоли для просмотра статистики EAP.

Таблица 8-4. Команды страницы EAP Statistics

Команды консоли	Описание
show dot1x statistics	Отображает статистические данные 802.1X для определенного интерфейса.

Ниже 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
```

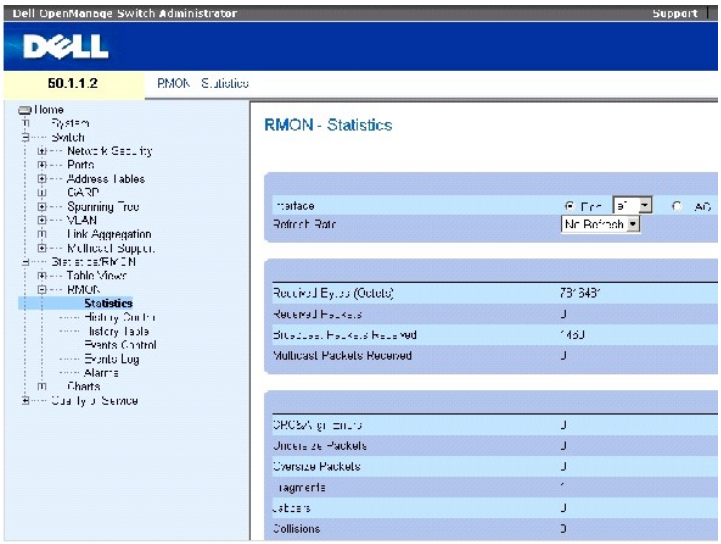
Просмотр статистики RMON

Страница RMON (Удаленный мониторинг) позволяет администраторам сети осуществлять дистанционный доступ к информации по сетевому трафику. Чтобы открыть страницу **RMON (Удаленный мониторинг)**, выберите **Statistics / RMON (Статистика / RMON)→RMON** в панели дерева.

Просмотр статистики группы удаленного мониторинга RMON

Воспользуйтесь информацией со страницы Статистика удаленного мониторинга (RMON) , включающую в себя сведения по использованию устройства и возникающих на нем ошибок. Чтобы открыть страницу Статистика удаленного мониторинга (RMON) , нажмите **Statistics / RMON (Статистика / RMON) → RMON→ Statistics (Статистика)** в панели дерева.

Рисунок 8-7. Статистика удаленного мониторинга (RMON)



На странице Статистика удаленного мониторинга (RMON) есть следующие поля:

Interface (Интерфейс). Определяет порт или группу LAG, для которой отображается статистика.

Refresh Rate (Частота обновления). Объем времени перед обновлением статистики.

Received Bytes (Octets) -Количество байт, полученных на выбранный интерфейс.

Received Packets - Количество пакетов, полученных на выбранный интерфейс.

Broadcast Packets Received (Принято широковещательных пакетов). Количество неиспорченных широковещательных пакетов, полученных на интерфейс с момента последней очистки счетчиков. В это количество не включаются многоадресные пакеты.

Multicast Received Packets (Принято многоадресных пакетов). Количество неиспорченных многоадресных пакетов, полученных на интерфейс с момента последней очистки счетчиков.

CRC & Align Errors (Ошибки CRC и выравнивания). Количество ошибок CRC и выравнивания, произошедших в интерфейсе после последней перезагрузки системы.

Undersize Packets (Маленькие пакеты). Количество пакетов размером меньше номинального (меньше 64 октетов), полученных на интерфейс с момента последней очистки счетчиков.

Oversize Packets (Большие пакеты). Количество пакетов размером больше номинального (свыше 1 518 октетов), полученных на интерфейс с момента последней очистки счетчиков.

Fragments (Фрагменты). Количество фрагментов (пакетов, содержащих менее 64 октетов, исключая кадрирующие биты, но включая октеты FCS), полученных на интерфейс с момента последней очистки счетчиков.

Jabbers (Сбойные пакеты). Количество сбойных пакетов размером более 1518 октетов, полученных на интерфейс с момента последней очистки счетчиков.

Collisions (Коллизии). Количество коллизий, полученных на интерфейс с момента последней очистки счетчиков.

Frames of *xx* Bytes (Кадры размером xx). Количество кадров размером *xx* байт, полученных на интерфейс с момента последней очистки счетчиков.

Просмотр статистики интерфейса

1. Откройте страницу Статистика удаленного мониторинга (RMON).
2. Выберите тип и номер интерфейса в поле **Interface**.

Отображается статистика интерфейса.

Просмотр статистики RMON с помощью команд консоли

В таблице приводятся команды консоли для просмотра статистики RMON.

Таблица 8-5. Команды страницы RMON Statistics

Команды консоли	Описание
show rmon statistics {**ethernet** *interface* | **port-channel** *port-channel- number*}	Отображает статистику удаленного мониторинга.

Ниже приведен пример команд консоли:

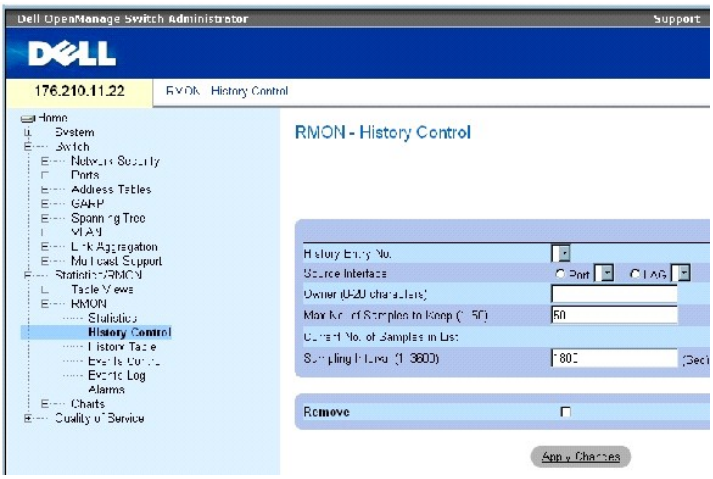
```
console# show rmon statistics ethernet 1/e1

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 1518 Octets: 389
```

Просмотр статистики управления журналом RMON

На странице **Управление журналом RMON** содержится информация по выборкам данных удаленного мониторинга, полученных с портов. Например, такие данные могут включать определения интерфейса или интервалы между опросами. Чтобы открыть страницу **Управление журналом RMON** , нажмите **Statistics/RMON (Статистика/RMON)** → **RMON**→ **History Control (Управление журналом)** в панели дерева.

Рисунок 8-8. Управление журналом RMON



На странице Управление журналом RMON есть следующие поля:

History Entry No. (Номер записи в журнале) - Номер записи на странице **History Control (Управление журналом)**.

Source Interface (Исходный интерфейс) - Указывает порт или группу LAG , из которого были получены выборки протокола.

Owner (0-20 characters) (владелец, 0-20 символов) - Указывает станцию удаленного мониторинга или пользователя, запросившего информацию по RMON.

Max Number of Samples to Keep (1-50) (Максимальное количество сохраняемых выборок) - Указывает, какое количество выборок необходимо сохранить. По умолчанию используется значение 50.

Current No. of Samples in List (Количество выборок в списке)- Указывает количество имеющихся выборок.

Sampling InterKval (1-3600) -Указывает временной интервал в секундах, во время которого выборки получаются с порта. Возможные значения: 1-3600 сек. По умолчанию используется значение 1800 сек (30 мин).

Remove (Удалить) - Если это поле отмечено, удаляется запись из **History Control Table (таблицы управления журналом).**

Добавление записи журнала

1. Откройте страницу **Управление журналом RMON**.
2. Нажмите кнопку **Add** (Добавить).

   Откроется страница **Add History Entry** (Добавить запись журнала).
3. Заполните поля в диалоговом окне.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Запись добавляется в таблицу **History Control Table (Таблица управления журналом)**.

Изменение записи журнала

1. Откройте страницу **Управление журналом RMON**.
2. Выберите запись в поле **History Entry No.**
3. Внесите необходимые изменения.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Запись будет изменена, а устройство обновлено.

Удаление записи таблицы управления журналом

1. Откройте страницу **Управление журналом RMON**.
2. Выберите запись в поле **History Entry No.**.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

   Запись удалена, а устройство обновлено.

Просмотр управления журналом удаленного мониторинга с помощью команд консоли

В этом разделе приводятся команды консоли для просмотра управления журналом удаленного мониторинга.

Таблица 8-6. Команды страницы RMON History

Команды консоли	Описание
rmon collection history index [**owner** *ownername* | **buckets** *bucket-number*] [**interval** *seconds*]	Включает и настраивает удаленный мониторинг на интерфейсе
show rmon collection history [**ethernet** *interface* | **port-channel** *port-channel-number*]	Отображает статистику журнала RMON.

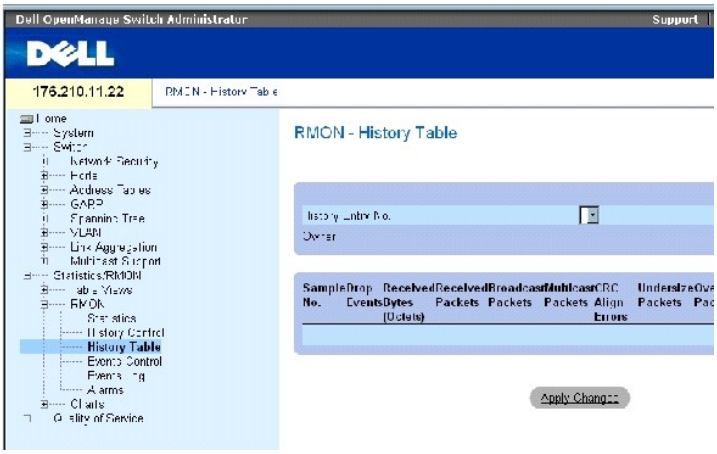
Ниже приведен пример команд консоли:

```
console(config)# interface ethernet 1/e8


console(config-if)# rmon collection history 1 interval
2400
```

Просмотр журнала удаленного мониторинга

На странице **Таблица RMON History** содержатся статистические сетевые выборки по специальному интерфейсу удаленного мониторинга. Каждая запись таблицы представляет собой все значения счетчиков, скомпилированные в течение однократной выборки. Чтобы открыть страницу **Таблица RMON History**, нажмите **Statistics/RMON (Статистика/RMON)** → **RMON**→ **History Table (Таблица журнала)** в панели дерева.

Рисунок 8-9. Таблица RMON History



На странице **Таблица RMON History** есть следующие поля:

ПРИМЕЧАНИЕ. В таблице RMON History показаны не все поля.

History Entry No. (Номер записи в журнале) - Номер записи на странице **History Control (Управление журналом)**.

Owner - Указывает станцию удаленного мониторинга или пользователя, запросившего информацию по RMON.

Sample No. - Указывает определенную выборку, которую отражает информация в таблице.

Drop Events - Указывает количество пакетов, удаленных из-за нехватки сетевых ресурсов в течение интервала выборки. Так как указать точное количество удаленных пакетов невозможно, указывается, сколько раз были обнаружены удаленные пакеты.

Received Bytes (Octets) - Количество октетов данных, включая поврежденные пакеты, полученные по сети.

Received Packets - Количество пакетов, полученных во время интервала выборки.

Broadcast Packets - Количество корректных широковещательных пакетов, полученных во время интервала выборки.

Multicast Packets - Количество корректных многоадресных пакетов, полученных во время интервала выборки.

CRC Align Errors - Количество пакетов, полученных во время сеанса выборки, с длиной в 64-1518 октета. Пакеты имеют неверную контрольную последовательность кадров (FCS) с целым числом октетов или неверную FCS с нецелым числом.

Undersized Packets - Количество пакетов, полученных во время сеанса выборки, с длиной меньше 64 октетов.

Oversize Packets - Количество пакетов, полученных во время сеанса выборки, с длиной более 1 518 октетов.

Fragments - Количество пакетов, полученных во время сеанса выборки, с длиной меньше 64 октетов и содержащих контрольную последовательность кадра.

Jabbers - Количество сбойных пакетов, полученных во время сеанса выборки, с длиной меньше 1 518 октетов и содержащих контрольную последовательность кадра.

Collisions - Оценивает общее количество коллизий пакетов, имевших место во время сеанса выборки. Коллизии обнаруживаются, когда порты повторителя засекают одновременную передачу с двух или более станций.

Utilization - Оценивает физическое использование сети интерфейса во время сеанса выборки. Значение отображается в виде сотых процента.

Просмотр статистики для определенной записи журнала

1. Откройте страницу **Таблица RMON History**.
2. Выберите запись в поле **History Entry No.** .

Статистика для записи будет отображена в таблице RMON History.

Просмотр управления журналом удаленного мониторинга с помощью команд консоли

В таблице приводятся команды консоли для просмотра журнала RMON.

Таблица 8-7. Команды страницы RMON History Control

Команды консоли	Описание
show rmon history index {throughput | errors | other} [period seconds]	Отображает журнал статистики удаленного мониторинга (RMON Ethernet Statistics).

Далее приведен пример команды для отображения статистики RMON ethernet statistics по пропускной способности на index 1:

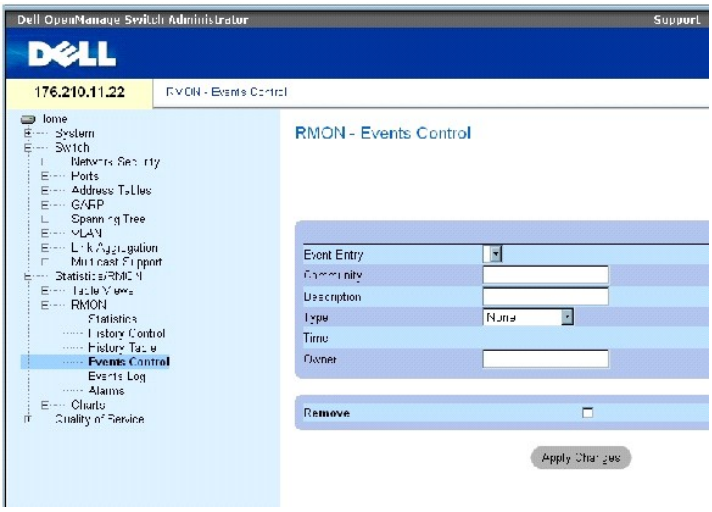
```
console> enable

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

Для определения событий удаленного мониторинга используйте страницу **Управление событиями RMON**. Чтобы открыть страницу**Управление событиями RMON** , нажмите **Statistics / RMON (Статистика / RMON)** → **RMON**→ **Events Control (Управление событиями)** в панели дерева.

Рисунок 8-10. Управление событиями RMON



На странице **Управление событиями RMON** есть следующие поля:

Event Entry - Указывает событие.

Community - Определяет сообщество, которому принадлежит событие.

Description - Описание события, определенного пользователем.

Type - Тип события. Возможные значения поля:

Log - Указывает тип события как запись в журнале.

Trap - Указывает тип события как прерывание.

Log and Trap - Указывает тип события и как запись в журнале, и как прерывание.

None - Событие отсутствует.

Time - Время события.

Owner - Устройство или пользователь, который определил событие.

Remove - Удаляет событие из таблицы событийRMON Events Table.

Добавление события удаленного мониторинга

1. Откройте страницу **Управление событиями RMON**.
2. Нажмите кнопку **Add** (Добавить).

   Откроется страница **Add an Event Entry** (Добавить запись о событии).
3. Введите данные в диалоговое окно и нажмите кнопку **Apply Changes (Применить изменения)**.

   Запись таблицы **Event Table** будет добавлена, а устройство обновлено.

Изменение события удаленного мониторинга

1. Откройте страницу **Управление событиями RMON**.
2. Выберите запись в **Event Table** (Таблица событий).
3. Измените данные в полях диалогового окна и нажмите кнопку **Apply Changes (Применить изменения)**.

   Запись таблицы **Event Table** будет изменена, а устройство обновлено.

Удаление события удаленного мониторинга

1. Откройте страницу **Управление событиями RMON**.
2. Нажмите кнопку **Show All** (Показать все).

Откроется страница **RMON Events Table** (Таблица событий RMON).

3. Отметьте флажком поле **Remove (Удалить)** для тех событий, которые необходимо удалить, и нажмите кнопку **Apply Changes (Применить изменения)**.

Запись удалена, а устройство обновлено.

ПРИМЕЧАНИЕ. Одну запись можно удалить со страницы **RMON Events Control** с помощью флажка в поле **Remove (Удалить)**.

Определение событий устройства с помощью командной строки

В таблице приводятся команды консоли для определения событий устройства.

Таблица 8-8. Команды страницы Device Event Definition

Команды консоли	Описание
rmon event *index type* [**community** *text*] [**description** *text*] [**owner name**]	Конфигурация событий RMON
show rmon events	Отображает таблицу событий удаленного мониторинга.

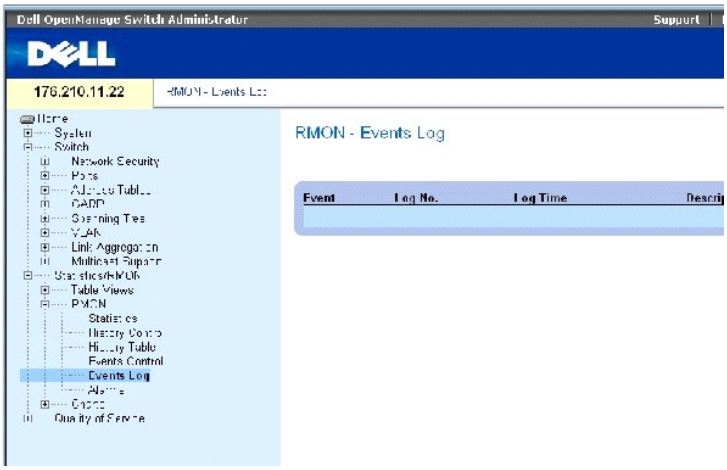
Ниже приведен пример команд консоли:

```
console(config)# rmon event 1 log
console(config)# exit
console# show rmon events
Index  Description  Type  Community  Owner  Last Time Sent
-----  -----------  ----  ---------  -------  ----------
1  Errors  Log  CLI  Jan 18 2002 23:58:17
2  High Broadcast  Log-Trap  router  Manager  Jan 18 2002 23:59:48
```

Просмотр журнала событий RMON

На странице **Журнал событий RMON** имеется список событий удаленного мониторинга. Чтобы открыть страницу**Журнал событий RMON**, нажмите **Statistics / RMON (Статистика / RMON)** → **RMON**→ **Events Log (Журнал событий)** в панели дерева.

Рисунок 8-11. Журнал событий RMON



На странице **Журнал событий RMON** есть следующие поля:

Event - Номер записи событий RMON в журнале.

Log No.-Номер журнала.

Log Time - Время записи события в журнал.

Description - Описание записи в журнале.

Определение событий устройства с помощью командной строки

В таблице приводятся команды консоли для определения событий устройства.

Таблица 8-9. Команды страницы Device Event Definition

Команды консоли	Описание
show rmon log [*ñîáûòèå*]	Отображает журнальную таблицу событий удаленного мониторинга.

Ниже приведен пример команд консоли:

```
console(config)# rmon event 1 log

Console> show rmon log

Maximum table size: 500

Event Description Time
```

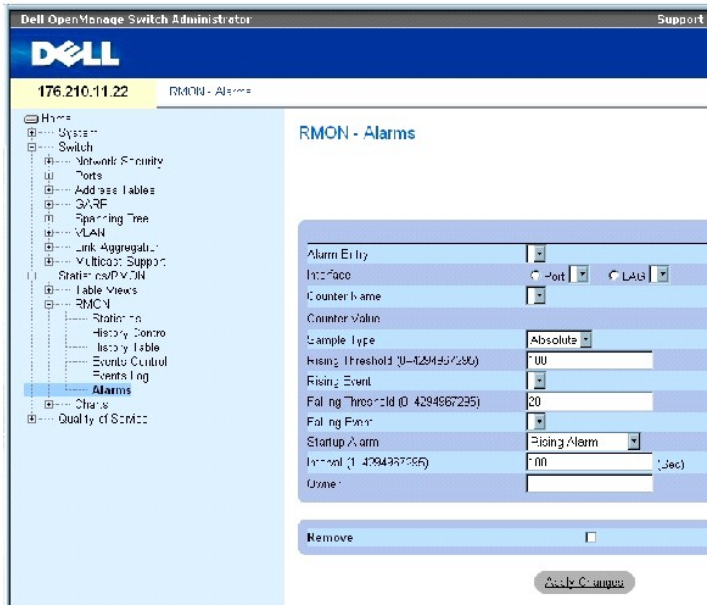
```
----- ---------- ----- --------------


1 Errors Jan 18 2002 23:58:17


2 High Broadcast Jan 18 2002 23:59:48
```

Определение тревог RMON устройства

Для установки сетевых тревог используйте страницу Тревоги RMON. Сетевая тревога происходит при обнаружении проблемы или события в сети. Повышение и понижение пороговых величин приводит к событиям. Более подробную информацию об индикаторах см. в разделе Просмотр журнала событий RMON.

Чтобы открыть страницу Тревоги RMON , нажмите **Statistics/RMON (Статистика/RMON)** → **RMON**→ **Alarms (Тревоги)** в панели дерева.

Рисунок 8-12. Тревоги RMON



На странице **Тревоги RMON** есть следующие поля:

Alarm Entry - Указывает определенную тревогу.

Interface — Тип интерфейса, для которого выводится статистика RMON.

Counter Name (Имя счетчика) - Выбранная переменная MIB.

Counter Value - Значение выбранной переменной MIB.

Sample Type - Определяет метод выборки для выбранной переменной и сравнивает значение с пороговыми величинами. Возможные значения поля:

Delta - Вычитает последнее значение выборки из текущего значения. Разница значений сравнивается с пороговой величиной.

Absolute - Сравнивает значения с пороговыми величинами в конце интервала выборки.

Rising Threshold (0-4294967295) - Значение счетчика превышения, активизирующее тревогу нарушения верхней пороговой величины. Верхняя пороговая величина графически представлена в верхней части столбчатых диаграмм. Каждая отображаемая переменная обозначена цветом. Значение по умолчанию: 100 секунд.

Rising Event - Механизм, в который поступают тревоги, в том числе регистрация, прерывание, или оба. Если выбран LOG, механизм сохранения не сохраняется ни на устройстве, ни в системе управления. Однако если не происходит перезагрузки устройства, он остается в таблице LOG устройства. Если выбрано значение trap, создается прерывание SNMP, о котором докладывается в механизме прерываний. Можно сохранить trap с помощью этого же механизма.

Falling Threshold (0-4294967295) - Значение счетчика понижения, активизирующее тревогу нарушения нижней пороговой величины. Нижняя пороговая величина графически представлена в верхней части столбчатых диаграмм. Каждая отображаемая переменная обозначена цветом. Значение по умолчанию: 20.

Startup Alarm - Переключатель, активизирующий тревогу. Повышение определяется нарушением пороговой величины от нижнего значения к верхнему.

Interval (1-4294967295) **(сек)** - Интервал тревоги. Значение по умолчанию: 100 секунд.

Owner - Указывает устройство или пользователя, который определил тревогу.

Remove (Удалить) - Если включено, тревога RMON удаляется.

Добавление записи в таблицу тревог

1. Откройте страницу **Тревоги RMON**.
2. Нажмите кнопку **Add** (Добавить).

Откроется страница **Add an Alarm Entry** (Добавить запись о тревоге).

Рисунок 8-13. Страница Add an Alarm Entry

3. Выберите тип интерфейса.
4. Заполните поля.
5. Нажмите кнопку **Apply Changes** (Применить изменения).

Тревога удаленного мониторинга будет добавлена, а устройство обновлено.

Изменение записи в таблице тревог

1. Откройте страницу **Тревоги RMON**.
2. Выберите запись в раскрывающемся списке **Alarm Entry** (Запись о тревоге).
3. Внесите изменения в соответствующие поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Запись будет изменена, а устройство обновлено.

Вывод таблицы тревог

1. Откройте страницу **Тревоги RMON**.
2. Нажмите кнопку **Show All** (Показать все).

Откроется страница **Alarms Table** (Таблица тревог).

Удаление записи в таблице тревог

1. Откройте страницу **Тревоги RMON**.
2. Выберите запись в раскрывающемся списке **Alarm Entry** (Запись о тревоге).
3. Установите флажок **Remove** (Удалить).
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Запись удалена, а устройство обновлено.

Определение тревог устройства с помощью командной строки

В таблице приводятся команды консоли для определения тревог устройства.

Таблица 8-10. Команды страницы Device Alarm

Команды консоли	Описание
rmon alarm *index MIB_Object_ID interval rthreshold fthreshold revent fevent* [**type** *type*] [**startup** *direction*] [**owner** *name*]	Настраивает условия тревоги RMON.
show rmon alarm-table	Отображает сводную таблицу тревог.
show rmon alarm	Отображает конфигурацию тревог RMON.

Ниже 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
```

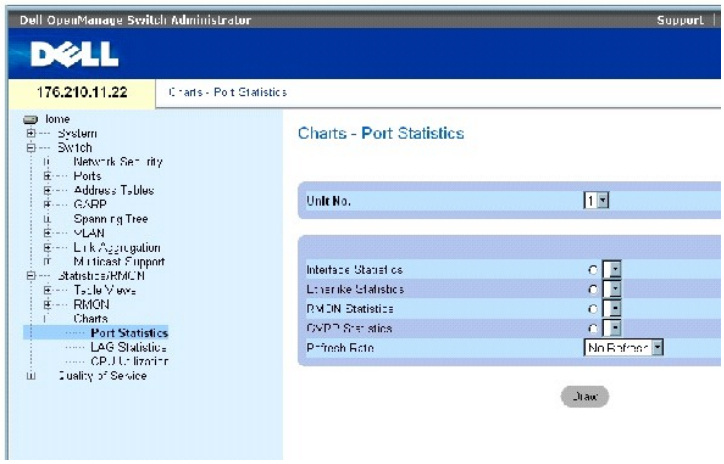
Просмотр диаграмм

На странице **Charts** (Диаграммы) содержатся ссылки для отображения статистики в виде диаграммы. Чтобы открыть страницу, нажмите Statistics (Статистика→ Charts (Диаграммы) в панели дерева.

Просмотр статистики портов

На странице **Статистика портов** отображается статистика для элементов порта в виде диаграммы. Чтобы открыть страницу**Статистика портов** , нажмите **Statistics/RMON (Статистика/RMON) → Charts (Диаграммы→ Port Statistics (Статистика портов)** в панели дерева.

Рисунок 8-14. Статистика портов



На странице **Статистика портов** есть следующие поля:

Unit No. (Номер устройства). - Номер стекового устройства, для которого выводится статистическая информация.

Interface Statistics (Статистика интерфейса) - Отображение статистики интерфейса.

Etherlike Statistics (Статистика Etherlike) - Отображение статистики Etherlike.

RMON Statistics (Статистика RMON) - Отображение статистики RMON.

GVRP Statistics (Статистика GVRP) - Отображение статистики GVRP.

Refresh Rate (Частота обновления). Объем времени перед обновлением статистики.

Отображение статистики порта

1. Откройте страницу **Статистика портов** .
2. Выберите тип статистики, которую хотите открыть.
3. Выберите нужную частоту обновления из раскрывающегося меню **Refresh Rate**.
4. Нажмите кнопку **Draw** (Рисовать).

На экране появится диаграмма для выбранной статистики.

Просмотр статистики порта с помощью команд консоли

В таблице приводятся команды консоли для просмотра статистики порта.

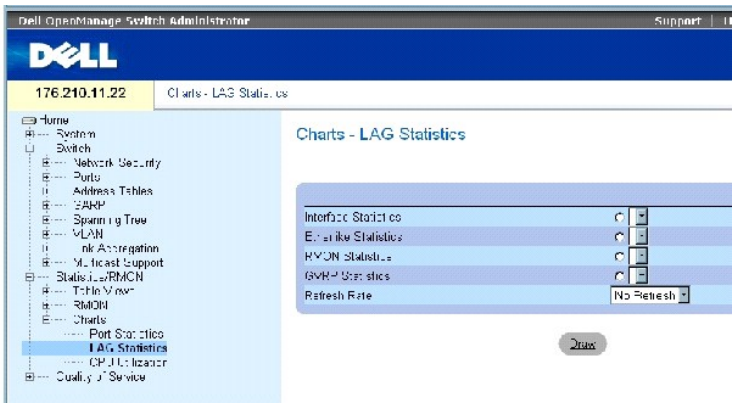
Таблица 8-11. Команды страницы Port Statistic

Команды консоли	Описание
show interfaces counters [**ethernet** *interface* | **port- channel** *port-channel-number*]	Отображает трафик, видимый на физическом интерфейсе.
show rmon statistics {**ethernet** *interface* | **port-channel** *port- channel-number*}	Отображает статистику удаленного мониторинга.
show gvrp statistics {**ethernet** *interface* | **port-channel** *port- channel-number*}	Отображает статистику протокола GVRP.
show gvrp-error statistics {**ethernet** *interface* | **port- channel** *port-channel-number*}	Отображает статистику ошибок протокола GVRP.

Просмотр статистики группы LAG

На странице **Статистика LAG** отображается статистика для LAG в виде диаграммы. Чтобы открыть страницу **Статистика LAG**, нажмите **Statistics / RMON (Статистика / RMON) → Charts (Диаграммы)→ LAG Statistics (Статистика LAG)** в панели дерева.

Рисунок 8-15. Статистика LAG



На странице Статистика LAG есть следующие поля:

Interface Statistics (Статистика интерфейса) - Отображение статистики интерфейса.

Etherlike Statistics (Статистика Etherlike) - Отображение статистики Etherlike.

RMON Statistics (Статистика RMON) - Отображение статистики RMON.

GVRP Statistics (Статистика GVRP) - Отображение статистики GVRP.

Refresh Rate (Частота обновления). Объем времени перед обновлением статистики.

Отображение статистики LAG

1. Откройте страницу **Статистика LAG**.
2. Выберите тип статистики, которую хотите открыть.
3. Выберите нужную частоту обновления из раскрывающегося меню **Refresh Rate**.
4. Нажмите кнопку **Draw** (Рисовать).

На экране появится диаграмма для выбранной статистики.

Просмотр статистики LAG с помощью команд консоли

В таблице приводятся команды консоли для просмотра статистики LAG.

Таблица 8-12. Команды страницы LAG Statistic

Команды консоли	Описание
show interfaces counters [**ethernet** *interface* | **port- channel** *port-channel-number*]	Отображает трафик, видимый на физическом интерфейсе.
show rmon statistics {**ethernet** *interface* | **port-channel** *port- channel-number*}	Отображает статистику удаленного мониторинга.
show gvrp statistics {**ethernet** *interface* | **port-channel** *port- channel-number*}	Отображает статистику протокола GVRP.

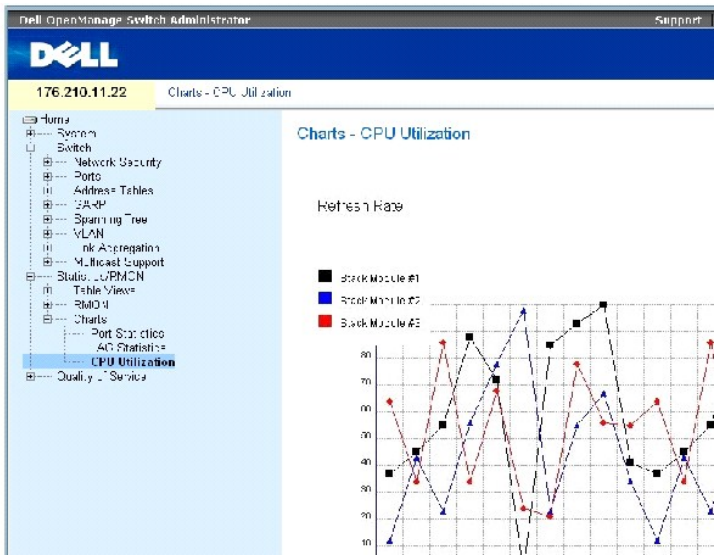
show gvrp-error statistics {**ethernet** *interface* | **port- channel** *port-channel-number*}	Отображает статистику ошибок протокола GVRP.

Обзор использования ЦПУ

На странице **Использование ЦПУ** содержится информация об использовании системного ЦПУ и проценте ресурсов ЦПУ, потребляемым каждым из компонентов стека. Каждому компоненту стека назначается свой цвет на диаграмме.

Чтобы открыть страницу **Использование ЦПУ**, нажмите **Statistics / RMON (Статистика / RMON)** → **Charts (Диаграммы)** → **CPU Utilization (Использование ЦПУ)** в панели дерева.

Рисунок 8-16. Использование ЦПУ



На странице **Использование ЦПУ** приводится следующая информация:

Refresh Rate (Частота обновления). Объем времени перед обновлением статистики.

Назад на страницу Содержание

Назад на страницу Содержание

Настройка качества обслуживания

Системы Dell™ PowerConnect™ 34XX Руководство пользователя

В этом разделе говорится об определении и настройке параметров качества обслуживания Quality of Service (QoS). Чтобы открыть страницу Quality of Service (Качество обслуживания), щелкните Quality of Service (Качество обслуживания)в панели дерева.

Обзор качества обслуживания QoS

Показатель Quality of Service (QoS) позволяет обеспечить качество обслуживания и очередь приоритетов внутри сети.

Пример реализации, в которой требуется качество обслуживания, включает определенные типы трафика, такие как звук, видео и данные реального времени, которые можно разместить в очереди с высоким приоритетом, а остальной трафик можно разместить в очереди с более низким приоритетом. Это позволяет ускорить прохождение первоочередного трафика.

Показатель QoS характеризуется следующим.

- Классификация - описывает, какие поля пакета соответствуют указанным значениям. Все пакеты, соответствующие пользовательским спецификациям, классифицируются вместе.
- Действие - определяет управление трафиком, при котором пересылаемые пакеты классифицируются по информации пакета и значениям таких полей пакета, как приоритет VLAN (VPT) и DSCP (DiffServ Code Point).

Классификационная информация VPT

Метки приоритета VLAN используются для классификации пакетов посредством привязки их к одной из очередей выхода. Метки приоритета VLAN для назначений в очередь определяются пользователем. В приведенной ниже таблице содержится информация о параметрах VPT по умолчанию для очереди.

Таблица 9-1. Значения по умолчанию для таблицы привязки CoS к очереди

Значение CoS	Значения очереди пересылки
0	q1 (низший приоритет)
1	q1 (низший приоритет)
2	q1 (низший приоритет)
3	q1 (низший приоритет)
4	q2
5	q2
6	q3
7	q3

ПРИМЕЧАНИЕ. В стековой конфигурации очередь 4 используется для пересылки стекового трафика. Следовательно, назначение дополнительного трафика для очереди 4 может помешать пересылке трафика.

Пакеты, поступающие непомеченными, назначаются в соответствии со значением VPT по умолчанию, которое определяется для каждого порта. Заданное значение VPT используется для привязки пакета к очереди выхода.

Значения DSCP можно поставить в соответствие очереди приоритетов. В приведенной ниже таблице содержится информация об используемом по умолчанию соответствии DSCP и таблицы привязки к очереди.

Таблица 9-2. Значения по умолчанию для таблицы привязки DSCP к очереди

Значение DSCP	Значения очереди пересылки
0-15	q1 (низший приоритет)
16-39	q2
40-63	q3

Привязка DSCP активизируется индивидуально для каждой системы.

Службы CoS

После постановки пакетов в определенную очередь выхода, можно назначить службы CoS этой очереди (очередям). Очереди выхода настраиваются с помощью схемы планирования одним из следующих способов.

- Strict Priority (Строгий приоритет) - Гарантирует, что чувствительные ко времени приложения всегда передаются. Строгий приоритет позволяет проводить по сети важнейший и наиболее срочный трафик быстрее трафика приложений, менее требовательных ко времени доставки данных. Например, при использовании параметра «Strict Priority» трафик голосовой информации по IP пересылается раньше трафика FTP или электронной почты (SMTP).
- Weighted Round Robin (Взвешенное круговое обслуживание). Гарантирует, что одно приложение не займет всю полосу пропускания коммутатора. Взвешенное круговое обслуживание (WRR) позволяет пересылать целые очереди в соответствии с циклическим алгоритмом. Все очереди могут участвовать во взвешенном круговом обслуживании с ожиданием очередей с высоким приоритетом. Очереди с высоким приоритетом обслуживаются быстрее, чем очереди WRR. Если поток трафика минимальный, а очереди с высоким приоритетом не занимают всю ширину полосы пропускания, отведенную для порта, очереди WRR могут быть пропущены по одной с ними полосе. При этом должно выполняться условие, что полоса пропускания распределена в соответствии с весовым коэффициентом. При выборе WRR очередям присваиваются следующие весовые коэффициенты: 1, 2, 4, 8.

Определение общих параметров QoS

На странице **QoS Parameters (Параметры QoS)** имеются ссылки на страницы, на которых задаются общие параметры качества обслуживания.

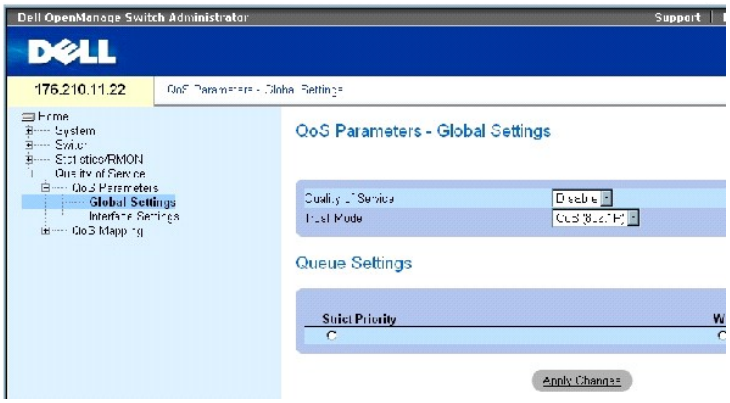
Настройка общих параметров QoS

На страницеThe **Общие параметры** содержится поле для включения или выключения параметров QoS. На ней также имеется поле для выбора доверенного режима (Trust mode). Доверенный режим определяет очередь выхода на основании встроенных полей пакета.

Кроме того, на странице **Общие параметры** можно определить приоритет очереди как Strict Priority (SP, строгий приоритет) или Weighted Round Robin (WRR, взвешенное круговое обслуживание).

Чтобы открыть страницу **Общие параметры** ,нажмите Quality of Service (Качество обслуживания)→QoS Parameters (Параметры QoS)→ Global Settings (Общие параметры) в панели дерева.

Рисунок 9-1. Общие параметры



На странице **Общие параметры** есть следующие поля:

- QoS Settings (Параметры QoS)
- Queue Settings (Параметры очереди)

QoS Settings (Параметры QoS)

Quality of Service (Качество обслуживания) - Включение или отключение управления сетевым трафиком с использованием QoS.

Trust Mode (Доверенный режим) - Определяет, какие поля пакета использовать для классификации пакетов, поступающих на коммутатор. Если не задано ни одно правило, трафик, содержащий встроенное поле пакета (CoS или DSCP), распределяется согласно выбранному доверенному режиму. Трафик, не содержащий встроенных полей, назначается в очередь с наибольшей возможной скоростью доставки (q2). Возможные следующие значения поля "Trust Mode" (Доверенный режим):

CoS (802.1p). Привязка к очереди выхода определяется меткой приоритета VLAN (VPT) по стандарту IEEE802.1p или значением VPT по умолчанию, назначенным порту. Значение по умолчанию: IEEE802.1p.

DSCP. Привязка к очереди выхода определяется согласно полю DSCP.

ПРИМЕЧАНИЕ. Интерфейсные параметры доверенного режима имеют более высокий приоритет, чем глобальный параметр доверенного режима.

Queue Settings (Параметры очереди)

Strict Priority (Строгий приоритет) - Указывает очереди со строгим приоритетом, если они определены.

WRR (Взвешенное круговое обслуживание)- Указывает очереди со взвешенным круговым обслуживанием, если они определены.

Включение QoS:

1. Откройте страницу **Общие параметры**.
2. Выберите в поле **Quality of Service** (Качество обслуживания) значение **Enable** (Включено).
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Функция Class of Service (Класс обслуживания) на этом устройстве будет включена.

Включение доверенного режима:

1. Откройте страницу **Общие параметры**.
2. Определите поле **Trust Mode** (Доверенный режим).
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Доверенный режим будет включен на устройстве.

Включение доверенного режима командами консоли

В следующей таблице приведены команды консоли, соответствующие полям на странице **Общие параметры**.

Таблица 9-3. Команды страницы QoS Settings

Команды консоли	Описание
qos trust [**cos** | **dscp**]	Настраивает систему на работу в доверенном режиме.
no qos trust	Выключает доверенное состояние системы.

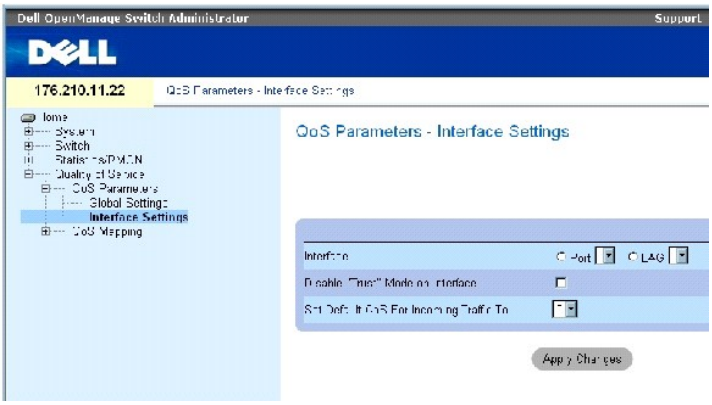
Ниже приведен пример команд консоли:

```
console(config)# qos trust
dscp
```

Определение интерфейсных параметров QoS

На странице **Параметры интерфейса** имеются поля для деактивации доверенного режима и присвоения значения CoS по умолчанию для входящих непомеченных пакетов. Чтобы открыть страницу **Параметры интерфейса**, нажмите Quality of Service (Качество обслуживания) →QoS Parameters (Параметры QoS→ Interface Settings (Параметры интерфейса) в панели дерева.

Рисунок 9-2. Параметры интерфейса



На странице **Параметры интерфейса** есть следующие поля:

Interface (Интерфейс). Заданный порт или группа LAG для настройки.

Disable "Trust" Mode on Interface (Отключить доверенный режим для интерфейса). Отключение доверенного режима для указанного интерфейса. Этот

параметр переопределяет глобальную настройку доверенного режима в коммутаторе.

Set Default CoS For Incoming Traffic To (Задать CoS по умолчанию для входящего трафика). Определяет используемое по умолчанию значение метки CoS для непомеченных пакетов. Метки CoS могут иметь значения от 0 до 7. Значение по умолчанию - 0.

Назначение параметров QoS для интерфейса:

1. Откройте страницу **Параметры интерфейса**.
2. Выберите поле **Interface** (Интерфейс).
3. Определите поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Параметры QoS будут назначены для интерфейса.

Отображение параметров QoS/CoS:

1. Откройте страницу **Параметры интерфейса**.
2. Нажмите кнопку **Show All** (Показать все).

Выводится таблица интерфейса Interface Table.

Назначение интерфейсов QoS командами консоли

В следующей таблице приведены команды консоли, соответствующие полям на странице **Параметры интерфейса**.

Таблица 9-4. Команды страницы QoS Interface

Команды консоли	Описание
qos trust	Включение доверенного режима.
no qos trust	Отключает доверенное состояние для каждого порта.

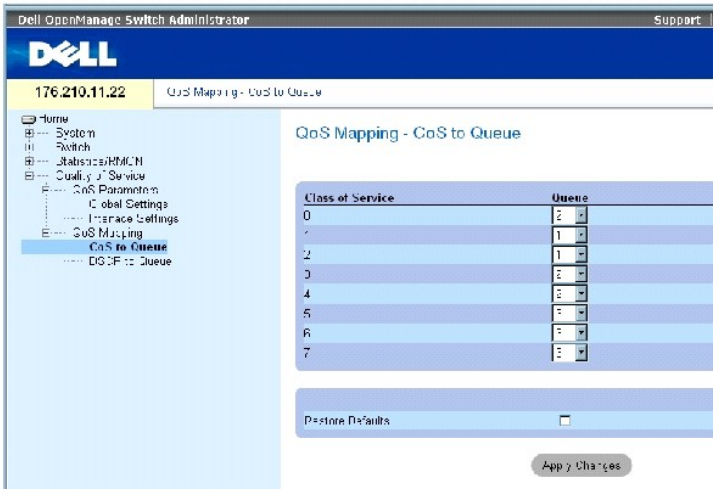
Ниже приведен пример команд консоли:

```
console(config)# interface
ethernet 1/e15

console(config-if)# qos
trust
```

Привязка значений CoS к очередям

Страница **Привязка CoS к очереди** содержит поля, позволяющие классифицировать параметры CoS для очередей трафика. Чтобы открыть страницу **Привязка CoS к очереди** , нажмите Quality of Service (Качество обслуживания) → QoS Mapping (Привязка QoS) → CoS to Queue (CoS к очереди) в панели дерева.

Рисунок 9-3. Привязка CoS к очереди



На странице **Привязка CoS к очереди** есть следующие поля:

Class of Service (Класс обслуживания). Определяет значения метки приоритета CoS (0 - наименьшее, 7 - наибольшее).

Queue (Очередь). Очередь, с которой сопоставляется приоритет CoS. Поддерживаются четыре очереди приоритета трафика.

Restore Defaults (Восстановить значения по умолчанию). Восстановление предустановленных значений по умолчанию коммутатора для привязки значений CoS к очереди выхода.

Привязка значения CoS к очереди

1. Откройте страницу **Привязка CoS к очереди**.
2. Выберите запись CoS.
3. Определите номер очереди в поле **Queue** (Очередь).
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Устанавливается соответствие значения CoS и очереди выхода и выполняется обновление в коммутаторе.

Привязка значений CoS к очередям командами консоли

В следующей таблице приведены команды консоли, соответствующие полям на странице **Привязка CoS к очереди**.

Таблица 9-5. Команды страницы CoS to Queue Settings

Команды консоли	Описание
wrr-queue cos-map queue-id cos0.cos7	Связывает значения CoS для выделения приоритетных очередей.

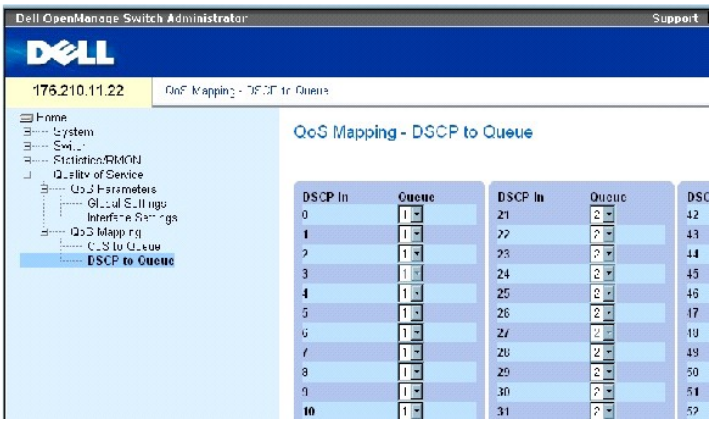
Ниже приведен пример команд консоли:

```
console(config)# wrr-queue
cos-map 4 7
```

Привязка значений DSCP к очередям

На странице **Привязка DSCP к очереди** содержатся поля, позволяющие определить очередь выхода для определенных полей DSCP. Чтобы открыть страницу **Привязка DSCP к очереди**, нажмите Quality of Service (Качество обслуживания) → QoS Mapping (Привязка QoS)→ DSCP to Queue (DSCP к очереди) в панели дерева.

Рисунок 9-4. Привязка DSCP к очереди



На странице **Привязка DSCP к очереди** есть следующие поля:

DSCP In (DSCP на входе). Значения поля DSCP во входящем пакете.

Queue (Очередь). Очередь, в которую направляются пакеты с заданным значением DSCP. Допустимые значения поля: 1-4 (1 - наименьшее, 4 - наибольшее).

Привязка значения DSCP и назначение очереди приоритета

1. Откройте страницу **Привязка DSCP к очереди**.
2. Выберите значение в столбце **DSCP In**.
3. Определите поле **Queue** (Очередь).
4. Нажмите кнопку **Apply Changes** (Применить изменения).

DSCP перезаписывается, а выбранному значению ставится в соответствие очередь выхода.

Привязка значений DSCP командами консоли

В следующей таблице приведены команды консоли, соответствующие полям на странице **Привязка DSCP к очереди**.

Таблица 9-6. Команды страницы DSCP Value to Queue

Команды консоли	Описание
qos map dscp-queue dscp-list **to** queue-id	Изменяет привязку DSCP к очереди.

Ниже приведен пример команд консоли:

```
console(config)# qos map
dscp-queue 33 40 41 to 1
```

Назад на страницу Содержание

Назад на страницу Содержание

Системы Dell™ PowerConnect™ 34XX Руководство пользователя

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

ЗАМЕЧАНИЕ. ПРЕДУПРЕЖДЕНИЕ указывает на возможность повреждения оборудования или потери данных и объясняет, как этого избежать.

ПРЕДУПРЕЖДЕНИЕ. ПРЕДОСТЕРЕЖЕНИЕ указывает на потенциальную опасность повреждения, получения легких травм или угрозу для жизни.

Март 2005

Назад на страницу Содержание

Назад на страницу Содержание

Информация о взаимодействии фунций устройства

Системы Dell™ PowerConnect™ 34XX Руководство пользователя

В приведенной ниже таблице содержится информация о взаимодействии фунций

Возможность	Примечания
802.1x Unauthenticated VLAN (Неидентифицированные сети VLAN 802.1x)	Неидентифицированные сети VLAN 802.1x взаимодействуют в ограниченной степени с: • Гостевыми сетями VLAN 802.1x • Частными сетями VLAN • Изолированными сетями VLAN • Сетями VLAN для сообщества • Специальными сетями VLAN
802.1x Unauthenticated VLAN Port (Порт неидентифицированной сети VLAN 802.1x)	Порты неидентифицированной сети VLAN 802.1x взаимодействуют в ограниченной степени с: • Изолированными портами • Портами сообщества • Универсальными портами • Портами сетей VLAN на базе MAC-адреса • фильтрацией на входе
ACL (Списки контроля доступа)	ACL взаимодействуют в ограниченной степени со: • Списками ACL на основе MAC-адреса • Специальными сетями VLAN
Auto-negotiation (Автоматическое согласование)	Зависимости или ограничения отсутствуют.
Back Pressure Suppor (Поддержка обратного давления)	
Bridge Multicast Filtering (Фильтрация многоадресного трафика через мост)	Зависимости или ограничения отсутствуют.
Cable Tests (Тестирование кабелей)	Зависимости или ограничения отсутствуют.
Community ports (Порты сообществ)	Порты сообществ взаимодействуют в ограниченной степени с заблокированными портами.
Community VLAN (Сети VLAN сообщества)	Сети VLAN сообщества взаимодействуют в ограниченной степени с: • Статическими MAC-адресами • ACL • GVRP • Отслеживанием IGMP • Специальными сетями VLAN
DNS	Ограничения отсутствуют.
Duplex Mode (Дуплексный режим)	
Flow Control (Управление потоком)	Зависимости или ограничения отсутствуют.
GARP	Зависимости или

	ограничения отсутствуют.
Guest VLANs (Гостевые сети VLAN)	Гостевые сети VLAN не работают совместно с: • Частными сетями VLAN • Изолированными сетями VLAN • Сетями VLAN сообщества • Сетями VLAN на базе MAC-адреса • Специальными сетями VLAN
GVRP	Зависимости или ограничения отсутствуют.
IGMP Snooping (Отслеживание IGMP)	Зависимости или ограничения отсутствуют.
Ingress Filtering (Фильтрация на входе)	Зависимости или ограничения отсутствуют.
Isolated Port (Изолированный порт)	Изолированные порты не работают совместно с: • Портами сообщества • Универсальными портами • Заблокированными портами • GVRP • Списками ACL на основе MAC-адреса • Фильтрацией на входе
Isolated VLAN (Изолированные сети VLAN)	Изолированные сети VLAN не работают совместно с: • Сетями VLAN сообщества • Статическими MAC-адресами • ACL • GVRP • Отслеживанием IGMP • Специальными сетями VLAN
LAG Statistics (Статистика LAG)	Зависимости или ограничения отсутствуют.
Link Aggregation (Объединение канала)	Зависимости или ограничения отсутствуют. Однако, имеются некоторые правила конфигурации объединенных каналов. Подробности см. в разделе "Определение параметров LAG".
Locked Ports (Заблокированные порты)	Заблокированные порты взаимодействуют в ограниченной степени с: • Списками ACL на основе MAC-адреса • Фильтрацией на входе
Logging (Протоколирование)	Зависимости или ограничения отсутствуют.
MAC Address Support (Поддержка MAC-адреса)	Зависимости или ограничения отсутствуют.
MDI/MDIX Decection (Обнаружение MDI/MDIX)	Зависимости или ограничения отсутствуют.
Multicast Filtering (Фильтрация многоадресного трафика)	Зависимости или ограничения отсутствуют.
Multiple Hosts (Множественные хосты)	Множественные хосты по стандарту 802.1X Standard не работают совместно с: • Изолированным портом • Портом сети VLAN на базе MAC-адреса
Multiple Spanning Tree (Протокол MST)	Протокол MST не работает совместно с: • Изолированным портом

	• Фильтрацией на входе
Port Based Authentication (Идентификация на основе портов)	Идентификация на основе портов взаимодействует в ограниченной степени с: • 802.1 Single • Изолированным портом • Заблокированными портами • Сетями VLAN на базе MAC-адреса • Входными портами
Port Mirroring (Дублирование портов)	Зависимости или ограничения отсутствуют. Однако, имеются некоторые правила конфигурации Storm Control. Подробности см. в разделе "Определение сеансов с зеркалированием портов".
Port Statistics (Статистика портов)	Зависимости или ограничения отсутствуют.
Private VLAN (Частные сети VLAN)	Частные сети VLAN не работают совместно с: • Изолированными портами • Портами сообщества • GVRP • Отслеживанием IGMP • Специальными сетями VLAN
Private VLAN (Частные сети VLAN)	Частные сети VLAN взаимодействуют в ограниченной степени с: • Изолированными сетями VLAN • GVRP • Отслеживанием IGMP • Специальными сетями VLAN
Promiscuous Ports (Универсальные порты)	Универсальные порты не работают совместно с: • Заблокированными портами • GVRP • Портами сети VLAN на базе MAC-адреса
Quality of Service (Качество обслуживания)	Зависимости или ограничения отсутствуют.
RMON Statistics (Статистика удаленного мониторинга)	Зависимости или ограничения отсутствуют.
SNMP Authentication Notifications (Уведомления идентификации SNMP)	Зависимости или ограничения отсутствуют.
SNMP Notifications (Извещения SNMP)	Зависимости или ограничения отсутствуют.
SNTP Authentication (Идентификация SNTP)	Зависимости или ограничения отсутствуют.
Spanning Tree (STP)	Зависимости или ограничения отсутствуют.
Special VLAN (Специальные сети VLAN)	Зависимости или ограничения отсутствуют.
Static MAC (Статический MAC-адрес)	Зависимости или ограничения отсутствуют.
Storm Control (Контроль "лавины")	Зависимости или ограничения отсутствуют.
System Logs (Системные журналы)	Зависимости или ограничения отсутствуют.
System Time Synchronization (Синхронизация системного времени)	Зависимости или ограничения отсутствуют.
Unauthenticated VLAN Ports (Порты неидентифицированных сетей VLAN)	Порты неидентифицированной сети взаимодействуют в ограниченной степени с:

	• Изолированными портами • Портами сообщества • Универсальными портами • GVRP • Портами сетей VLAN на базе MAC-адреса • Фильтрацией на входе

Назад на страницу Содержание

Назад на страницу Содержание

Глоссарий

Системы Dell™ PowerConnect™ 34XX Руководство пользователя

В глоссарии приведены основные технические термины по данной тематике.

A | B | C | D | E | F | G | H | I | J | L | M | N | O | P | Q | R | S | T | U | V | W

A

Access mode (Режим доступа)

Метод, с помощью которого пользователь получает доступ в систему.

Access Profiles (Профили доступа)

Позволяет сетевым менеджерам определять профили и правила для доступа к коммутатору. Доступ к управлению для указанной группы пользователей может быть ограничен по следующим критериям:

- Интерфейсы на входе
- Исходный IP-адрес или IP-подсети

Aggregated VLAN (Объединенные сети VLAN)

Объединяет несколько сетей VLAN в единую сеть VLAN. Объединенные сети VLAN позволяют маршрутизаторам отвечать на запросы ARP по узлам, расположенным на разных подсетях VLAN, которые входят в состав одной супер-сети VLAN. Маршрутизаторы отзываются по MAC-адресам.

ARP

Address Resolution Protocol (Протокол разрешения адресов). Протокол, преобразующий IP-адреса в физические.

ASIC

Application Specific Integrated Circuit (Интегральная схема программного обеспечения). Заказная микросхема, предназначенная для определенного программного обеспечения.

Asset Tag (Дескриптор ресурса)

Задает пользовательскую ссылку на коммутатор.

Authentication Profiles (Профили идентификации)

Своды правил, которые дают возможность идентифицировать пользователей и программы.

Auto-negotiation (Автоматическое согласование)

Позволяет устанавливать следующие функции для портов Ethernet 10/100 Мбит/с и 10/100/1000 Мбит/с:

- Дуплексный и полудуплексный режим.
- Управление потоком
- Скорость

B

Back Pressure (Обратное давление)

Механизм, использование которого в полудуплексном режиме позволяет порту не принимать сообщение.

Backplane (Объединительная плата)

Главная информационная шина в коммутаторе.

Backup Configuration Files (Резервные файлы конфигурации)

Содержат резервную копию конфигурации коммутатора. Резервный файл конфигурации изменяется, когда в него копируется файл рабочей конфигурации или файл для запуска.

Bandwidth (Пропускная способность)

Пропускная способность определяет, какой объем данных можно передать за фиксированный интервал времени. Для вычисления пропускной способности цифровых коммутационных модулей используются биты в секунду (бит/с) или байты в секунду.

Bandwidth Assignments (Назначения пропускной способности)

Объем пропускной способности, назначенный приложению, пользователю или интерфейсу.

Baud (Скорость передачи)

Количество сигнальных элементов, передаваемых за секунду.

Best Effort (Максимально возможная скорость доставки)

Трафик поступает в очередь с низшим приоритетом и доставка пакетов не гарантирована.

Boot Version (Версия загрузчика)

Версия загрузчика.

BootP (Протокол Boot)

Протокол начальной самозагрузки. Позволяет рабочей станции распознавать свой IP-адрес, IP-адрес сервера BootP в сети или файл конфигурации, включаемый в загрузку коммутационного модуля.

BPDU

Bridge Protocol Data Unit (Единица протокола преобразования данных). Предоставляет информацию преобразования данных в формате сообщений. Единицы протокола преобразования данных (BPDU) передаются на коммутатор вместе с конфигурацией связующего дерева. Пакеты BPDU содержат информацию о портах, адресах, правах доступа и затраты на передачу данных.

Bridge (Мост)

Устройство, которое связывает две сети. Мосты являются предметом оборудования, но они не зависят от протокола. Мосты функционируют на канальных уровнях 1 и 2.

Broadcast Domain (Широковещательный домен)

Наборы устройств, которые получают широковещательные кадры, отправленные с любого коммутационного модуля из назначенного набора. Маршрутизаторы связывают широковещательные домены, поскольку маршрутизаторы не пересылают широковещательные кадры.

Broadcasting (Широковещательная передача)

Метод передачи пакетов на все порты сети.

Broadcast Storm (Широковещательная "лавина")

Чрезмерное количество широковещательных сообщений, одновременно передаваемых по сети с одного порта. Ответы на пересылаемые сообщения отправляются в сеть, перегружая ее ресурсы или вызывая простой сети.

Более подробную информацию о широковещательных лавинах см. в разделе ""Определение параметров LAG"".

C

CDB

База данных конфигурации. Файл, содержащий информацию о конфигурации устройства.

Класс обслуживания (Class of Service)

Класс обслуживания (CoS). Класс обслуживания представляет собой схему приоритетов 802.1p. CoS позволяет включать в маркировку пакетов сведения о приоритете. В заголовки пакетов на уровне 2 добавляется значение CoS от 0 до 7, где 0 - наименьший приоритет, 7 - наибольший.

Передача одного или более пакетов с перекрытием, при котором происходит коллизия. Отправленные данные не могут быть использованы, и сеанс начинается заново.

CLI

Command Line Interface (Режим командной строки). Набор командных строк, который используется для конфигурации системы. Более подробную информацию по использованию CLI см. в разделе Using the CLI (Использование интерфейса командной строки).

Communities (Сообщества)

Определенные группы пользователей, которые имеют одинаковые права доступа к системе.

CPU (ЦПУ)

Центральный процессор. Компонент компьютера, который обрабатывает информацию. ЦПУ состоит из блока управления и арифметико-логического устройства (АЛУ).

D

DHCP Client (Клиент DHCP)

Устройство, использующее протокол DHCP для получения параметров конфигурации, например, сетевого адреса.

DSCP

Код дифференцированной услуги(DSCP). DSCP позволяет включать в маркировку IP-пакетов сведения о приоритете QoS.

Domain (Домен)

Группа коммутационных модулей и компьютеров в сети, связанных между собой общими правилами и процедурами.

DRAC/MC

DRAC/MC. Предоставляет единое управление для компонентов системы коммутационных серверов Dell.

Duplex Mode (Дуплексный режим)

Обеспечивает одновременную передачу и прием данных. Существуют два типа дуплексного режима:

- **Полный дуплексный режим**. Обеспечивает бисинхронную передачу, например, как в телефонии. Данные могут одновременно передаваться в обе стороны.

- **Полудуплексный режим**. Обеспечивает асинхронную передачу, например, как в портативной рации. Данные могут одновременно передаваться только в одну сторону.

E

Egress Ports (Выходные порты)

Порты, с которых передается сетевой трафик.

End System (Оконечная система)

Оконечное пользовательское устройство в сети.

Ethernet

Используется стандарт Ethernet IEEE 802.3. Ethernet является наиболее распространенным стандартом для локальных сетей. Ethernet поддерживает передачу данных на скорости 10, 100 и 1000 Мбит/с.

EWS

Встроенный веб-сервер. Предоставляет возможность управления устройством через стандартный веб-браузер. Встроенные веб-серверы используются в дополнение или вместо интерфейса командной строки или станции управления сетью.

F

FFT

Таблица быстрой передачи. Предоставляет информацию о передающих маршрутизаторах. Если на устройство поступает пакет по известному маршруту, этот пакет передается по маршруту, указанном в таблице FFT. При отсутствии известного маршрута ЦПУ передает пакет и обновляет данные таблицы FFT.

FIFO

Первый на вход, первый на выход. Процесс очередности, при котором первый пакет в очереди является первым на выходе.

Flapping (Колебание)

Колебание имеет место, когда состояние интерфейса постоянно изменяется. Например, порт STP постоянно меняет режимы работы: слушание, обнаружение, передача. Возможный результат: потеря трафика.

Flow Control (Управление потоком)

Позволяет устройствам с низкой скоростью передачи данных взаимодействовать с высокоскоростными устройствами, удерживая устройства с высокой скоростью передачи данных от отправки пакетов.

Fragment (Фрагмент)

Пакет Ethernet размером менее 576 бит.

Frame (Кадр)

Пакет, содержащий заголовок и концевик, необходимые для передачи в физической среде.

G

GARP

Протокол регистрации атрибутов. Регистрирует станции-клиенты в многоадресном домене.

Gigabit Ethernet

Стандарт Gigabit Ethernet обеспечивает передачу данных на скорости 1000 Мбит/с и совместим с существующими стандартами Ethernet 10/100 Мбит/с.

GVRP

Регистрационный протокол GARP в сетях VLAN. Регистрирует станции-клиенты в сетях VLAN.

H

HOL

Начало очереди. Пакеты добавляются в очередь. Пакеты, находящиеся в начале очереди, пересылаются раньше, чем пакеты, находящиеся в конце очереди.

Host (Хост)

Компьютер, выполняющий роль источника данных или услуг по отношению к другим компьютерам.

HTTP

Hypertext Transfer Protocol (протокол передачи гипертекста).Обеспечивает передачу документов HTML между серверами и клиентами через Интернет.

I

IC

Интегральная схема. Интегральные схемы представляют собой электронные устройства, состоящие из полупроводниковых материалов.

ICMP

Internet Control Message Protocol (протокол управляющих сообщений в Интернете). Позволяет шлюзу или принимающему хосту взаимодействовать с передающим хостом, например, для сообщения об ошибке выполнения.

IEEE

Institute of Electrical and Electronics Engineers (Общество инженеров по электротехнике и радиоэлектронике). Техническая организация, разрабатывающая стандарты в области связи и сетевых технологий.

IEEE 802.1d

Используется в протоколе STP. Стандарт IEEE 802.1d поддерживает установку перемычки MAC, чтобы избежать возникновления шлейфов в сети.

IEEE 802.1p

Стандарт, устанавливающий приоритет сетевого трафика на подуровне управления передачей данных/доступом к среде (MAC).

IEEE 802.1Q

Стандарт, описывающий порядок функционирования мостов VLAN и позволяющий определять, использовать и администрировать сети VLAN в инфраструктуре локальной сети, оснащенной мостами.

Image File (Файл-образ)

Системные образы сохраняются в двух FLASH-файлах, называемых образами (Image 1 and Image 2). Активный образ хранит активную копию, а остальные - вторичную копию.

Ingress Port (Входной порт)

Порт, который принимает сетевой трафик.

IP

Internet Protocol (протокол Интернет). Определяет формат пакетов и метод их адресации. Протокол IP назначает пакетам адреса и пересылает эти пакеты на требуемый порт.

IP Address (IP-адрес)

Адрес протокола Интернета. Уникальный адрес, назначенный сетевому устройству, связывающему две или более локальных или глобальных сетей.

J

Jumbo Frames (Большие кадры)

Позволяют использовать для передачи равного объема данных меньшее количество кадров. При передаче больших кадров требуется меньше служебных данных, сокращается время обработки и количество прерываний.

L

LAG

Link Aggregated Group (Объединенная группа каналов). Группа, объединяющая порты или сети VLAN в один виртуальный порт или одну сеть VLAN.

Подробнее об определении групп LAG см. в разделе **Defining LAG Membership (Определение членства в группе LAG)**.

LAN

Local Area Networks (Локальные сети) Сеть, находящаяся внутри комнаты, здания, комплекса зданий или другой ограниченной географической области.

Layer 2 (Уровень Layer 2)

Уровень управления передачей данных или уровень MAC. Содержит физический адрес клиентской или серверной станции. Обработка уровня Layer 2 выполняется быстрее, чем уровня Layer 3, поскольку объем обрабатываемой информации меньше.

Layer 4 (Уровень Layer 4)

Устанавливает соединение и гарантирует, что все данные достигнут своего назначения. Пакеты, проверяемые на уровне Layer 4, анализируются и передаются исходя из их назначения.

Load Balancing (Распределение нагрузки)

Равномерное распределение данных или пакетов обработки по доступным сетевым ресурсам. Напрмер, распределение нагрузки может произойти в равной степени по всем серверам или пакет может быть переправлен на следующий доступный сервер.

M

MAC Address (MAC-адрес)

Адрес протокола управления доступом к передающей среде (Media Access Control - MAC). MAC-адрес определяет адрес оборудования каждого узла в сети.

Распознавание MAC-адреса (MAC Address Learning)

Распознавание MAC-адреса выполняет обучающийся мост, в котором записан MAC-адрес источника пакетов. Пакеты, отправленные на этот адрес, пересылаются только на интерфейс моста, содержащего этот адрес. Пакеты, отправленные на неизвестные адреса, пересылаются на интерфейсы каждого моста. Функция распознавания MAC-адреса позволяет уменьшить трафик в присоединенные локальные сети.

MAC Layer (Уровень MAC)

Подуровень уровня управления передачей данных.

Mask (Маска)

Фильтр, включающий или исключающий определенные значения, например, фрагменты IP-адреса.

Например, если устройство 2 подключено на первой минуте десятиминутного цикла, а устройство 1 - на пятой того же самого цикла, считается, что они подключены одновременно.

MD5

Message Digest 5Алгоритм 128-битного шифрования. Алгоритм MD5 является вариантом MD4, который предоставляет более высокий уровень защиты. Метод MD5 проверяет целостность условий коммуникации и идентифицирует базу связи.

MDI

Media Dependent Interface (интерфейс, зависящий от среды передачи). Кабель, используемый для конечных станций.

MDIX

Media Dependent Interface with Crossover (интерфейс, зависящий от среды передачи, с перекрещиванием). Кабель, используемый для концентраторов и коммутаторов.

MIB

Management Information Base (База данных управления). Базы данных управления содержат информацию, описывающую специфические аспекты компонентов сети.

Multicast (Многоадресная передача)

Передача копий одного пакета на несколько портов.

N

NMS

Network Management System (Система управления сетью). Интерфейс, предоставляющий возможность управлять системой.

Node (Узел)

Конечная точка соединения в сети или место соединения нескольких линий в сети. Узлы включают:

- Процессоры
- Контроллеры
- Рабочие станции

O

OID

Object Identifier (Идентификатор объекта). Используется протоколом SNMP для идентификации управляемых объектов. В примере управления сетью SNMP по схеме Администратор - агент каждый управляемый объект должен иметь свой идентификатор.

P

Packets (Пакеты)

Блоки информации, передаваемые в системах с пакетной коммутацией.

PDU

Protocol Data Unit (Протокольная единица обмена). Единица обмена, заданная в пределах одного уровня, которая включает управляющую информацию протокола и пользовательские данные уровня.

PING

Packet Internet Groper (отправитель пакетов Интернета). Утилита, позволяющая проверить доступность IP-адреса. На IP-адрес передается пакет и ожидается ответ.

Port (Порт)

С помощью физических портов осуществляется подключение компонентов, что обеспечивает взаимодействие процессоров с периферийными устройствами.

Port Mirroring (Дублирование портов)

Контролирует и дублирует сетевой трафик путем пересылки копий входящих и исходящих пакетов с одного порта на другой (дублирующий).

Более подробную информацию о дублировании портов см. в разделе **Defining Port Mirroring Sessions (Определение сеансов с зеркалированием портов)**.

Port Speed (Скорость порта)

Скорость передачи данных через порт. Поддерживаются следующие скорости портов:

- Ethernet, 10 Мбит/с.
- Fast Ethernet, 100 Мбит/с.
- Gigabit Ethernet, 1000 Мбит/с.

Protocol (Протокол)

Набор правил, регламентирующий обмен информацией между коммутационными модулями по сети.

Q

QoS

Quality of Service (качество обслуживания). Показатель QoS позволяет менеджерам сети определять состав сетевого трафика и порядок пересылки в соответствии с приоритетами, типом приложений, а также исходным и целевым адресами.

Query (Запрос)

Извлекает информацию из базы данных и предоставляет ее для использования.

R

RADIUS

Удаленная служба идентификации наборного доступа пользователя. Метод идентификации системных пользователей и отслеживания времени соединения.

RMON

Remote Monitoring (Удаленный мониторинг). Позволяет собирать информацию о сети на отдельной рабочей станции.

Router (Маршрутизатор)

Устройство, которое подключается к различным сетям. Маршрутизаторы пересылают пакеты между двумя или более сетями. Маршрутизаторы работают на уровне Layer 3.

RSTP

Rapid Spanning Tree Protocol (Протокол связующего дерева). Выявляет и использует топологию сети, таким образом обеспечивая лучшую сходимость для протокола STP без образования циклов пересылки.

Running Configuration file (Файл рабочей конфигурации)

Содержит все команды файла для запуска, а также все команды, введенные во время последнего сеанса. После отключения или перезагрузки устройства все команды, сохраненные в файле рабочей конфигурации, теряются.

S

Segmentation (Сегментация)

Разделяет сети LAN на отдельные сегменты для установки перемычки. Сегментация устраняет ограничения по пропускной способности в сетях LAN.

Server (Сервер)

Центральный компьютер, предоставляющий услуги другим компьютерам, объединенным в сеть. К услугам относятся возможности хранения файлов и доступа к приложениям.

SNMP

Simple Network Management Protocol (Простой протокол сетевого управления). Используется для управления локальными сетями. Программы, ориентированные на протокол SNMP, взаимодействуют с сетевым коммутатором посредством встроенных агентов SNMP. Агенты SNMP собирают информацию о работе сети и состоянии коммутатора, а затем отправляют эту информацию на рабочую станцию.

SNTP

Простой протокол сетевого управления. Протокол SNTP гарантирует синхронизацию времени на таймере сети с точностью до миллисекунд.

SoC

System on a Chip (Система на микропроцессоре). Специализированная интегральная схема, которая содержит всю систему. Например, приложение telecom SoC может включать в себя микропроцессор, процессор цифровых сигналов, ОЗУ и ПЗУ.

Spanning Tree Protocol (Протокол связующего дерева).

Предотвращает появление циклов в трафике сети. Протокол STP обеспечивает топографию дерева при любой организации мостов. Протокол STP обеспечивает единственный путь между конечными станциями сети, тем самым исключая циклы.

SSH

Защищенная оболочка. Предоставляет доступ к другому компьютеру в сети, позволяет выполнять команды на удаленном компьютере и перемещать файлы с одного компьютера на другой. Защищенная оболочка предоставляет надежные методы идентификации и коммуникации через незащищенные каналы.

Startup Configuration (Конфигурация при запуске)

Сохраняет точную конфигурацию коммутатора при отключении или перезагрузке коммутационного модуля.

Subnet (Подсеть)

Сегмент сети. Подсети состоят из сетевых компонентов с одинаковыми фрагментами адреса. В сетях TCP/IP подсети объединяют коммутационные модули одинаковыми префиксами. Например, все коммутационные модули с префиксом 157.100.100.100 относятся к одной подсети.

Subnet Mask (Маска подсети)

Целиком или полностью маскирует IP-адреса компонентов подсети.

Switch (Коммутатор)

Устройство, фильтрующее и пересылающее пакеты между сегментами локальной сети. Коммутаторы поддерживают все протоколы пакетной передачи.

T

TCP/IP

Transmissions Control Protocol (протокол управления передачей). Обеспечивает взаимодействие и обмен потоками данных между двумя хостами. Протокол TCP гарантирует доставку пакетов, а также передачу и прием пакетов в том порядке, в каком они были отправлены.

Telnet

Протокол эмуляции терминала. Предоставляет доступ к системе для пользователей и дает возможность использовать ресурсы удаленных сетей.

TFTP

Trivial File Transfer Protocol (Тривиальный протокол передачи файлов). Передает файлы с помощью протокола UDP без использования функций защиты.

Trap (Прерывание)

Сообщение, отправляемое с сервера SNMP, которое уведомляет о том, что в системе произошло событие.

Trunking (Создание транков)

Объединение канала. Оптимизирует использование портов, связывая между собой группу портов и формируя объединенный транк (объединенный канал).

U

UDP

User Data Protocol (Протокол пользовательских данных). Передает пакеты, но не дает гарантию их доставки.

Unicast (Однонаправленная передача)

Форма маршрутизации, при которой один пакет передается одному пользователю.

V

VLAN

Virtual Local Area Network (Виртуальная локальная сеть). Логические подгруппы локальной сети (ЛС), созданные программным, а не аппаратным путем.

W

WAN

Wide Area Networks (Глобальная вычислительная сеть). Сеть, покрывающая обширную географическую область.

Wildcard Mask (Маска ввода)

Указывает, какие биты IP-адреса используются, а какие игнорируются. Маска ввода коммутационного модуля 255.255.255.255 показывает, что все биты не важны. Маска ввода 0.0.0.0 показывает, что все биты важны.

Например, если приемник имеет IP-адрес 149.36.184.198 и применяется маска ввода 255.36.184.00, то первые два бита IP-адреса игнорируются, а используются последние два бита.

Назад на страницу Содержание