

Системы Dell™ PowerConnect™ 6024/6024F

[Введение](#)

[Описание аппаратного обеспечения](#)

[Кабели, порты и расположение контактов](#)

[Использование Dell OpenManage Switch Administrator](#)

[Настройка коммутатора](#)

[Информация о настройке системы](#)

[Информация о настройке коммутатора](#)

[Настройка маршрутизации](#)

[Просмотр статистики](#)

[Настройка качества обслуживания](#)

[Получение справки](#)

Примечания, уведомления и предупреждения



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



ВНИМАНИЕ. Указывает на опасность повреждения оборудования или потери данных и объясняет, как этого избежать.



ПРЕДУПРЕЖДЕНИЕ. Указывает на возможность материального ущерба, травмы или смерти.

Информация, включенная в состав данного документа, может быть изменена без уведомления.
© Dell Inc., 2005. Все права защищены.

Воспроизведение материалов данного руководства в любой форме без письменного разрешения корпорации Dell Inc. строго запрещено.

Торговые марки, упомянутые в данном документе: *Dell, Dell OpenManage, логотип DELL, Inspiron, Dell Precision, Dimension, OptiPlex, PowerConnect, PowerApp, PowerVault, Axim, DellNet* и *Latitude* являются товарными знаками корпорации Dell Inc. *Microsoft* и *Windows* являются охраняемыми товарными знаками корпорации Майкрософт.

Другие торговые марки и фирменные названия упомянуты в данной документации в качестве ссылки как на предприятия, имеющие эти марки и названия, так и на их продукцию. Dell Inc. заявляет об отказе от всех прав собственности на любые товарные знаки и названия, кроме своих собственных.

Январь 2005 г.

[Назад на страницу Содержание](#)

Кабели, порты и расположение контактов

Системы Dell™ PowerConnect™ 6024/6024F

- [Контактные разъемы для интерфейса 10/100/1000 Ethernet](#)
- [Контактные разъемы для интерфейсов SFP](#)
- [Подключение кабеля последовательного порта](#)
- [Подключение к источнику питания переменного тока](#)

В этом разделе описаны физические интерфейсы и кабельные соединения коммутатора.

Станции подсоединяются к портам коммутатора через порты физического интерфейса на передней панели. Для каждой станции устанавливается соответствующий режим (дуплекс, полудуплекс и авто).

Контактные разъемы для интерфейса 10/100/1000 Ethernet

Переключаемый порт можно подключать к станциям в стандартном режиме станции RJ-45 Ethernet с помощью кабелей прямого подключения. Передающие устройства соединены друг с другом с помощью перекрестных кабелей.

На [рис. 3-1](#) показаны порты RJ-45, а в [таблице 3-1](#) описано назначение контактов разъема RJ-45.

Рис. 3-1. Разъем RJ-45

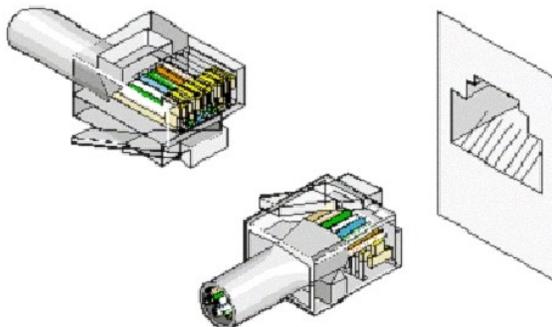


Таблица 3-1. Назначение контактов разъема RJ-45 для 10/100/1000 Base T

Контакт	Назначение
1	TxRx 1+
2	TxRx 1-
3	TxRx 2+
4	TxRx 2-
5	TxRx3+
6	TxRx 3-
7	TxRx 4+
8	TxRx 4-

Контактные разъемы для интерфейсов SFP

На [рис. 3-2](#) показан разъем SFP, а в [таблице 3-2](#) показано назначение контактов для дополнительного разъема SFP.

Рис. 3-2. Разъем SFP

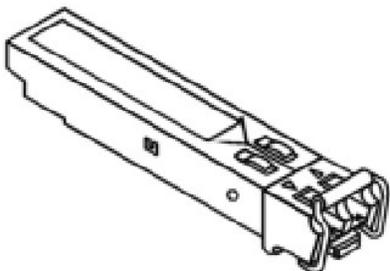


Таблица 3-2. Назначение контактов интерфейса SFP

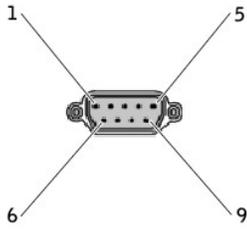
Контакт	Назначение
1	Заземление передатчика (общее с заземлением приемника).
2	Сбой передатчика.
3	Отключение передатчика: выход лазера отключается на высоком уровне или в разомкнутом состоянии.
4	Определение модуля 2; строка данных для идентификатора последовательного порта.
5	Определение модуля 1; строка синхронизации для идентификатора последовательного порта.
6	Определение модуля 0; заземлен внутри модуля.
7	Выбор скорости; подключение не требуется.
8	Индикация потери сигнала; логический 0 означает нормальную работу.
9	Заземление приемника (общее с заземлением передатчика).
10	Заземление приемника (общее с заземлением передатчика).
11	Заземление приемника (общее с заземлением передатчика).
12	Инвертированный выход данных приемника; пара АС.
13	Неинвертированный выход данных приемника; пара АС.
14	Заземление приемника (общее с заземлением передатчика).
15	Источник питания приемника.
16	Питание передатчика.
17	Заземление передатчика (общее с заземлением приемника).
18	Неинвертированный вход данных передатчика.
19	Инвертированный вход данных передатчика.
20	Заземление передатчика (общее с заземлением приемника).

Подключение кабеля последовательного порта

Чтобы подключить коммутатор к терминалу для начальной установки и настройки, можно использовать последовательные кабели (нуль-модемные). (Можно также использовать программу эмуляции терминала, запущенную на ПК.) Последовательный кабель коммутатора представляет собой кроссовый кабель DB-9 с гнездом (см. [рис. 3-3](#)).

На [рис. 3-3](#) показан последовательный кабель, а в [таблице 3-3](#) показано назначение контактов разъема последовательного порта.

Рис. 3-3. Разъем последовательного порта



В [таблице 3-3](#) показано назначение контактов разъема последовательного порта.

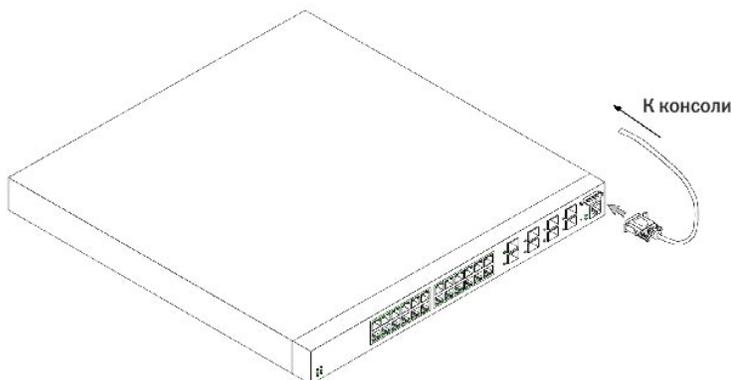
Таблица 3-3. Назначение контактов разъема последовательного порта

Сигнал	Контакт	Сигнал порта консоли управления
Не используется	1	Не используется
TXD	2	TXD
RXD	3	RXD
Не используется	4	RXD
GND	5	GND
Не используется	6	Не используется
CTS	7	CTS
RTS	8	RTS
Не используется	9	Не используется

Подключение коммутатора к терминалу

1. Подключите нуль-модемный (последовательный) кабель к разъему терминала (консоли) ASCII DTE RS-232.
2. Подключите интерфейсный кабель к разъему последовательного порта коммутатора (см. [рис. 3-4](#)).

Рис. 3-4. Подключение к последовательному порту коммутатора



Подключение к источнику питания переменного тока

1. Используя стандартный кабель питания длиной 1,5 м (5 футов) с заземляющим контактом, подсоедините кабель питания к главному разъему

электропитания на задней панели (см. [рис. 3-5](#)).

2. Подсоедините кабель питания к заземленной электрической розетке.

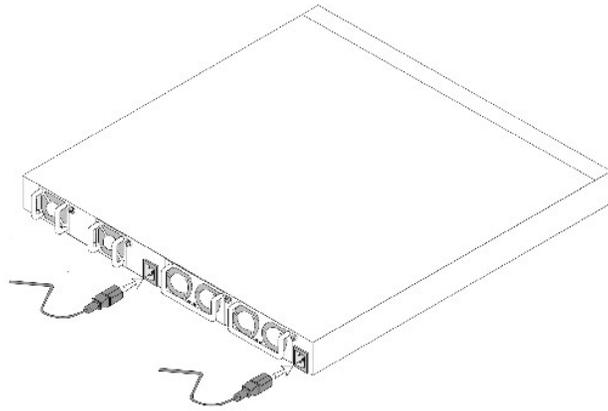
ПРИМЕЧАНИЕ. Рекомендуется подключить второй кабель питания к другому источнику электропитания.

3. По состоянию индикаторов на передней и задней панелях проверьте, правильно ли подключено и работает устройство.

Полное описание индикаторов см. в разделе «[Описание аппаратного обеспечения](#)».

4. Повторите процедуру для второго источника питания.

Рис. 3-5. Подключение источника питания к коммутатору



[Назад на страницу Содержание](#)

Информация о настройке системы

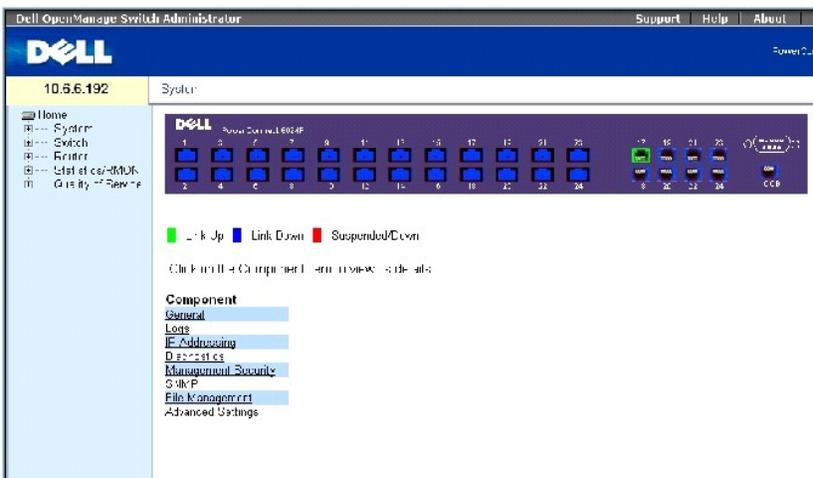
Системы Dell™ PowerConnect™ 6024/6024F

- [Открытие страницы System \(Система\)](#)
- [Определение общих сведений об устройстве](#)
- [Настройка параметров SNMP](#)
- [Настройка портов управления вне диапазона \(OOB\)](#)
- [Управление журналами](#)
- [Определение IP-адресации](#)
- [Запуск диагностики кабелей](#)
- [Управление безопасностью устройств](#)
- [Определение параметров SNMP](#)
- [Управление файлами](#)
- [Определение расширенных параметров](#)

Открытие страницы System (Система)

Чтобы открыть страницу [System](#) (Система), выберите System (Система) на панели дерева (см. [рис. 6-1](#)).

Рис. 6-1. Страница System (Система)



Определение общих сведений об устройстве

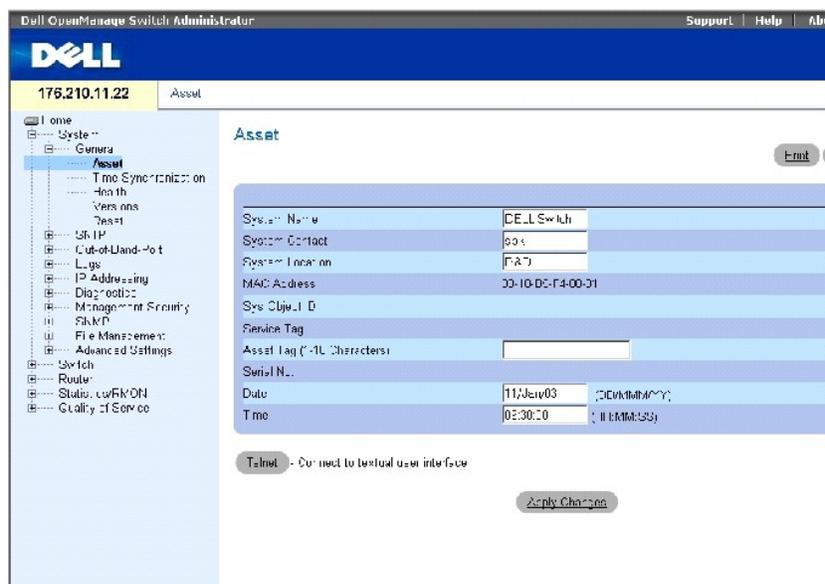
Страница General (Общее) содержит ссылки на страницы, с помощью которых администраторы сети могут настраивать параметры устройства.

Настройка сведений об устройстве

Страница Asset (Ресурсы) содержит параметры для настройки и просмотра общих сведений об устройстве, включая имя системы, ее местонахождение и контактную информацию, системный MAC-адрес для коммутатора и порта управления вне диапазона, системный идентификатор объекта, дату, время, а также время работы системы.

Чтобы отобразить страницу [Asset](#) (Ресурсы), выберите System (Система)→ General (Общие)→ Asset (Ресурсы) на панели дерева.

Рис. 6-2. Страница Asset (Ресурсы)



Страница [Asset](#) (Ресурсы) содержит следующие поля.

System Name (Имя системы) - имя системы, назначенное пользователем.

System Contact (Контактное лицо системы) - имя контактного лица.

System Location (Местонахождение системы) - место запуска системы.

MAC Address (MAC-адрес) - MAC-адрес коммутатора.

Sys Object ID (Идентификатор объекта системы) - идентификатор объекта (OID) информационной базы управления (MIB).

Service Tag (Метка производителя) - справочный номер, используемый при обслуживании устройства.

Asset Tag (Дескриптор ресурса) - ссылка на устройство, задаваемая пользователем. Возможные значения параметра: от 1 до 16.

Serial No. (Серийный номер) - серийный номер устройства.

Date (DD/MM/YY) (Дата (ДД/ММ/ГГ)) - текущая системная дата. Формат даты: месяц, день, год; например: 11/Jan/02 означает 11 января 2002.

Time (HH/MM/SS) (Время (ЧЧ:ММ:СС)) - текущее системное время. Формат времени: час, минуты, секунды; например: 20:12:03 означает 8:12:03 вечера.

Определение сведений о системе

1. Откройте страницу [Asset](#) (Ресурсы).
2. Определите следующие поля. **System Name** (Имя системы), **System Contact** (Контактное лицо системы), **System Location** (Местоположение системы) и **Asset Tag** (Дескриптор ресурса).
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Системные параметры будут определены, а устройство обновлено.

Запуск сеанса Telnet

1. Откройте страницу [Asset](#) (Ресурсы).

 **ПРИМЕЧАНИЕ.** Соответствующие параметры telnet устанавливаются до запуска сеанса telnet. Дополнительную информацию см. в разделе «[Настройка первоначального пароля Telnet](#)».

2. Щелкните Telnet.

Настройка сведений об устройстве с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для просмотра полей, отображенных на странице [Asset](#) (Ресурсы).

Таблица 6-1. Команды консоли для настройки ресурсов

Команда консоли	Описание
<code>hostname имя_хоста</code>	Указывает или изменяет имя хоста устройства.
<code>snmp-server contact текст</code>	Задаёт контактное лицо для системы.
<code>snmp-server location текст</code>	Определяет сведения о местонахождении устройства.
<code>show clock</code>	Отображает системное время и дату.
<code>asset-tag метка</code>	Определяет дескриптор ресурса для устройства.
<code>show system-id</code>	Отображает данные идентификации системы, включая метку производителя, дескриптор ресурса и серийный номер.
<code>show system</code>	Отображает информацию о системе.

Далее приведен пример команд консоли.

```
Console (config)# hostname dell
```

```
Console (config)# snmp-server contact Dell_Tech_Supp
```

```
Console (config)# snmp-server location New_Yorks
```

```
Console(config)# exit
```

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

Console# **show clock**

15:29:03 Jun 17 2002

Определение параметров системного времени

Страница [Time Synchronization](#) (Синхронизация по времени) содержит поля для синхронизации системного времени и часов локального оборудования или внешних часов SNTP.

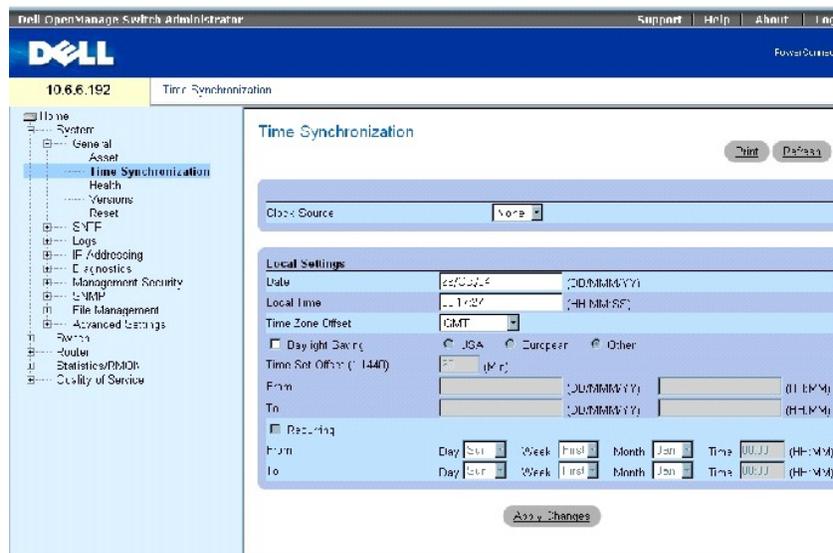
В случае сбоя внешних часов SNTP, с которыми синхронизировано системное время, в качестве источника времени системных часов автоматически начинаются использоваться часы локального оборудования.

Можно настроить автоматический перевод системных часов на летнее время.

Дополнительную информацию о протоколе SNTP см. в разделе «[Настройка параметров SNTP](#)».

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

Рис. 6-3. Страница Time Synchronization (Синхронизация по времени)



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

Clock Source (Источник синхронизации) - источник, используемый для установки системных часов. Возможные значения:

None (Нет) - указывает, что системное время синхронизировано с часами локального оборудования.

SNTP - указывает, что системное время синхронизировано с часами SNTP-сервера. Дополнительную информацию см. в разделе [«Настройка параметров SNTP»](#).

Date (Дата) - определяет системную дату. Формат поля: ДД:ММ:ГГ.

Local Time (Локальное время) - определяет системное время. Формат поля: ЧЧ:ММ:СС.

Time Zone Offset (Смещение часового пояса) - разница в часах между временем по Гринвичу (GMT) и местным временем.

Можно запрограммировать автоматический перевод системных часов на летнее время в определенный период времени в конкретном году или на повторяющийся период времени. Чтобы указать период времени в конкретном году, используйте параметры в области Daylight Savings (Летнее время), а чтобы указать повторяющийся период времени, используйте параметры в области Recurring (Повторение).

Daylight Savings (Летнее время) - установите этот флажок, чтобы включить переход на летнее время на устройстве на основе его географического положения. Возможные значения:

USA (США) - устройство переключается на летнее время в 2 часа ночи в первое воскресенье апреля и переключается на стандартное время в 2 часа ночи в последнее воскресенье октября.

European (Европейское) - устройство переключается на летнее время в 1:00 ночи в последнее воскресенье марта и переключается на стандартное время в 1:00 ночи в последнее воскресенье октября. Этот параметр применяется для стран членов Европейского Союза и других стран Европы, использующих стандарты Европейского Союза.

Other (Другое) - переход устройства на летнее время происходит в период времени, определенный пользователем.

Time Set Offset (1-1440) (Смещение установки времени) - для стран, кроме США и стран Европы, разницу между стандартным временем и летним временем можно установить в минутах. Время по умолчанию - 60 минут.

From/To (С/по) - для стран, кроме США и стран Европы, определяет дату и время начала/окончания периода летнего времени. Формат даты ДД/ММ/ГГ, а формат времени ЧЧ:ММ.

Recurring (Повторение) - установите этот флажок, чтобы включить на устройстве переход на летнее время в один и тот же период времени. Возможные значения:

From/To (С/по) - определяет день/неделю/месяц и время начала/окончания периода летнего времени. Формат времени ЧЧ:ММ.

Выбор источника синхронизации

1. Откройте [Time Synchronization](#) (Синхронизация по времени).
2. Определите значение поля Clock Source (Источник синхронизации).
3. Нажмите кнопку Apply Changes (Применить изменения).

Будет выбран источник синхронизации, а устройство обновлено.

Определение параметров локальных часов

1. Откройте страницу [Time Synchronization](#) (Синхронизация по времени).
2. Определите поля в области Local Settings (Локальные настройки).
3. Нажмите кнопку Apply Changes (Применить изменения).

Будут применены настройки локальных часов, а устройство обновлено.

Определение летнего времени

1. Откройте страницу [Time Synchronization](#) (Синхронизация по времени).
2. Определите поля в области **Daylight Saving** (Летнее время) или **Recurring** (Повторение).
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Будут применены настройки летнего времени, а устройство обновлено.

Определение параметров часов с помощью команд консоли

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

Таблица 6-2. Команды консоли для синхронизации по времени

Команда консоли	Описание
<code>clock source {sntp}</code>	Синхронизирует системное время с часами SNTP-сервера.
<code>no clock source</code>	Устанавливает системное время по часам устройства.
<code>clock timezone разница_в_часах [minutes разница_в_минутах][zone сокращение]</code>	Устанавливает часовой пояс для отображения.
<code>no clock timezone</code>	Устанавливает время в соответствии с универсальным скоординированным временем (UTC).
<code>clock summer-time recurring {usa eu {день недели месяц чч:мм день недели месяц чч:мм}} [offset разница] [zone сокращение]</code>	Настраивает автоматический переход системы на летнее время в соответствии со стандартами, принятыми в США, или европейскими стандартами или с учетом повторяющегося периода времени, установленного пользователем.
<code>clock summer-time date дата_месяц_год чч:мм дата_месяц_год чч:мм [offset разница] [zone сокращение]</code>	Настраивает автоматический переход системы на летнее время в период времени, установленный пользователем.
<code>no clock summer-time</code>	Отключает переход системы на летнее время.
<code>show clock</code>	Отображает системное время и дату.
<code>show clock [detail]</code>	Отображает системное время, дату, часовой пояс и настройку перехода на летнее время.

Далее приведен пример команд консоли

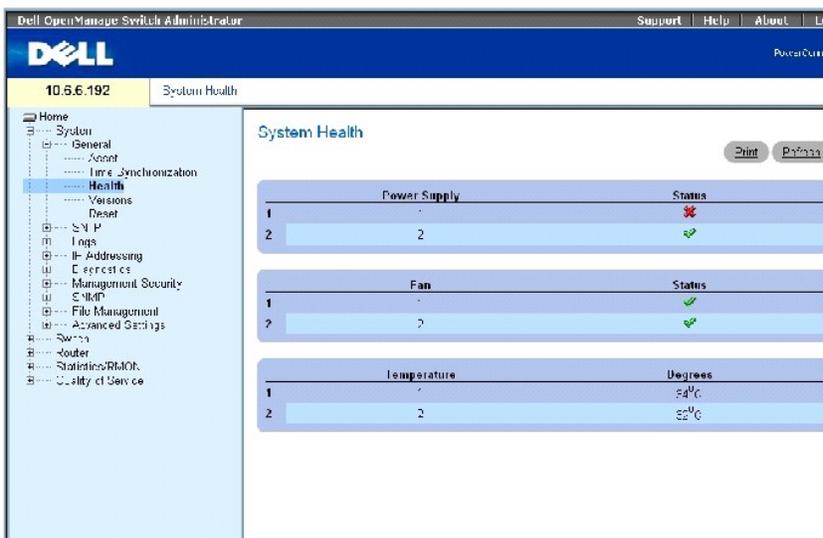
```
Console(config)# clock timezone -6 zone CST
```

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

Настройка отображения сведений о состоянии системы

Страница [System Health](#) (Состояние системы) отображает информацию о физическом состоянии устройства, включая информацию о питании коммутатора и системе вентиляции. Чтобы отобразить страницу [System Health](#) (Состояние системы), выберите System (Система)→ General (Общие)→ Health (Состояние) на панели дерева.

Рис. 6-4. Страница System Health (Состояние системы)



Страница [System Health](#) (Состояние системы) содержит следующие поля.

Power Supply (Источник питания) - состояние источника питания.

✔ - источник питания работает правильно.

✖ - источник питания работает неправильно.

Not Present (Отсутствует) - источник питания не установлен.

Fan (Вентилятор) - указывает состояние вентилятора. Коммутатор PowerConnect 6024/6024F имеет два вентилятора.

✔ - вентилятор работает правильно.

✖ - вентилятор работает неправильно.

Not Present (Отсутствует) - вентилятор не установлен.

Temperature (Температура) - текущая температура работающего устройства.

Просмотр сведений о состоянии системы с помощью команд консоли

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

Таблица 6-3. Команды консоли для просмотра состояния системы

Команда консоли	Описание
show system	Отображает информацию о системе.

Далее приведен пример команд консоли

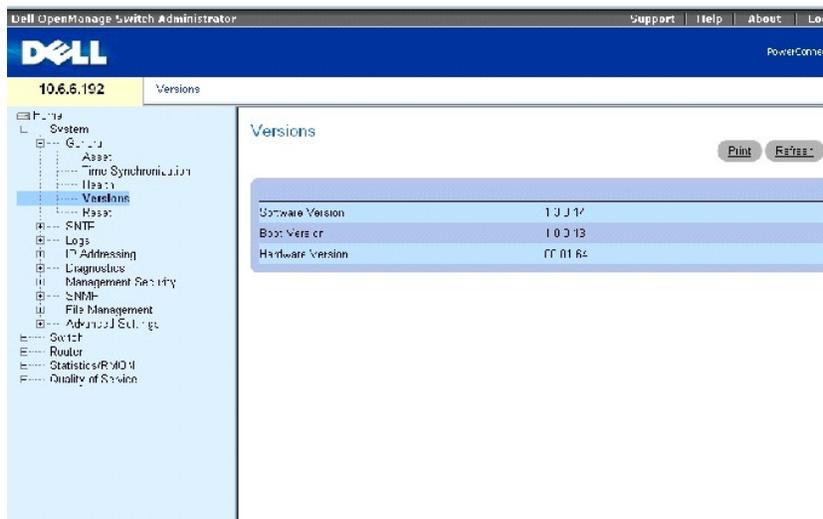
Console# show system	
System Description:	Ethernet Routing Switch
System Up Time (days, hour:min:sec):	0,00:32:04
System Contact:	
System Name:	
System Location:	
System MAC Address:	00:0d:56:2f:45:30
OOB MAC Address:	00:00:00:00:00:18
System Object ID:	1.3.6.1.4.1.674.10895.3000
Type:	Коммутатор PowerConnect 6024
Main Power Supply Status:	OK
Redundant Power Supply Status:	OK
Fan 1 Status:	OK
Fan 2 Status:	OK

Temperature (Celsius):	45
Temperature Sensor Status:	OK

Информация о версии

Страница [Versions](#) (Версии) содержит сведения об используемом оборудовании и версиях программного обеспечения. Чтобы отобразить страницу [Versions](#) (Версии), выберите System (Система) → General (Общие) → Versions (Версии) на панели дерева (см. [рис. 6-5](#)).

Рис. 6-5. Страница Versions (Версии)



Страница [Versions](#) (Версии) содержит следующие поля.

Software Version (Версия программы) - текущая версия программного обеспечения, запущенного на устройстве.

Boot Version (Версия загрузчика) - текущая версия загрузчика, используемого на устройстве.

Hardware Version (Версия аппаратного обеспечения) - текущая версия аппаратного обеспечения устройства.

Отображение версий устройств с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для просмотра полей, отображаемых на странице [Versions](#) (Версии).

Таблица 6-4. Команды консоли для отображения версий

Команда консоли	Описание
<code>show version</code>	Отображает сведения о версии системы.

Далее приведен пример команд консоли.

```
Console# show version
```

```
SW version 1.0.0.67 ( date 26-Jun-2003 time 18:15:42 )
```

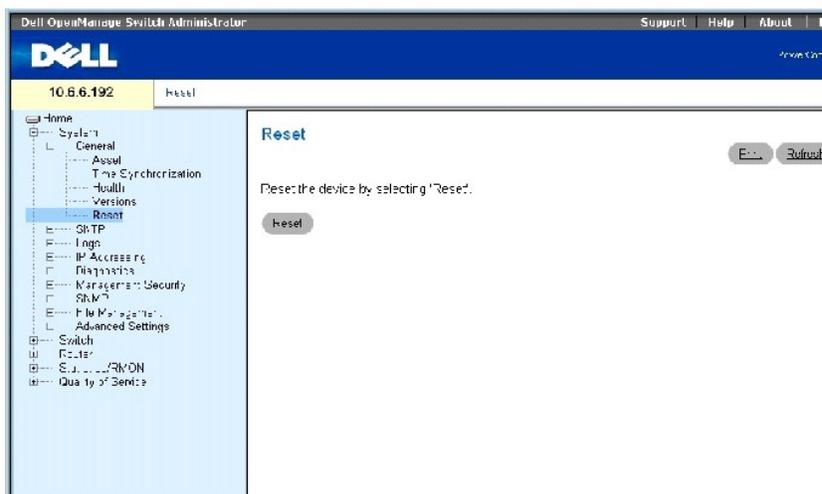
```
Boot version 1.0.0.11 ( date 12-Jun-2003 time 15:55:01 )
```

```
HW version 00.01.64
```

Восстановление заводских параметров устройства

Для восстановления заводских параметров устройства можно использовать страницу [Reset](#) (Сброс). Чтобы открыть страницу [Reset](#) (Сброс), выберите System (Система) → General (Общие) → Reset (Сброс) на панели дерева (см. [рис. 6-6](#)).

Рис. 6-6. Страница Reset (Сброс)



ПРИМЕЧАНИЕ. Чтобы не потерять текущую конфигурацию устройства, прежде чем перенастраивать устройство, сохраните все изменения в файле Running Configuration (Рабочая конфигурация). Дополнительную информацию о сохранении файлов конфигурации см. в разделе «[Управление файлами](#)».

Восстановление заводских параметров устройства

1. Откройте страницу [Reset](#) (Сброс).
2. Нажмите кнопку Reset (Сброс).
3. Когда появится диалоговое окно подтверждения, нажмите ОК.

Будут восстановлены заводские настройки устройства. После этого пользователь должен ввести имя пользователя и пароль.

Восстановление заводских параметров устройства с помощью команд консоли

1. Если еще не активирован режим консоли Privileged User EXEC, введите `enable` (включить).
2. Если необходимо сохранить изменения в настройках устройства, введите команду `copy running-config startup-config`.
3. Введите команду `reload` (перезагрузить).

4. Если необходимо продолжить, нажмите **y**.
-

Настройка параметров SNTP

Данное устройство поддерживает протокол SNTP (Simple Network Time Protocol). Протокол SNTP гарантирует точность синхронизации времени такта сетевого устройства до миллисекунды. Синхронизация по времени выполняется сетевым сервером SNTP. Это устройство работает только как клиент SNTP и не предоставляет службу синхронизации времени для других систем.

Источники времени устанавливаются по уровням. Уровни определяют точность источника времени. Чем выше уровень (где нуль - это самый высокий уровень), тем более точный источник времени. Устройство получает время с уровня 1 и выше.

Далее приведен пример уровней.

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

Получаемые от сервера SNTP данные оцениваются на основе уровня времени и типа сервера.

Оценка и определение значений времени SNTP выполняется по следующим уровням времени.

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

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

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

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

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

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

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

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

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

Страница SNTP содержит ссылки на страницы, с помощью которых администраторы сети могут настраивать параметры SNTP. Чтобы открыть страницу SNTP, выберите System → SNTP на панели дерева.

Определение общих параметров SNTP

Страница [SNTP Global Settings](#) (Общие параметры SNTP) содержит информацию для определения параметров SNTP.

Чтобы открыть страницу [SNTP Global Settings](#) (Общие параметры SNTP), выберите System (Система) → SNTP → Global Settings (Общие параметры) на панели дерева.

Рис. 6-7. Страница SNTP Global Settings (Общие параметры SNTP)



Страница [SNTP Global Settings](#) (Общие параметры SNTP) содержит следующие поля.

Poll Interval (60-86400) (Интервал опроса) - определяет интервал (в секундах), с которым сервер SNTP запрашивает одноадресную информацию.

Receive Broadcast Servers Updates (Принимать обновления от серверов широковещательной передачи) - если этот параметр включен, выполняется опрос серверов SNTP для получения данных о времени от сервера широковещательной рассылки для выбранных интерфейсов. При получении пакета SNTP устройство будет синхронизировано, даже если синхронизация не запрашивалась.

Receive Anycast Servers Updates (Принимать обновления от серверов передачи любого типа) - опрашивает серверы SNTP для получения данных о времени от сервера рассылки любого типа. Устройство будет синхронизировано только после того, как оно отправит запрос о синхронизации.

Receive Unicast Servers Updates (Принимать обновления от серверов передачи любого типа) - опрашивает серверы SNTP для получения данных о времени от сервера одноадресной рассылки. Если включены все три поля - **Receive Broadcast Servers Updates** (Принимать обновления от серверов широковещательной передачи), **Receive Anycast Servers Updates** (Принимать обновления от серверов передачи любого типа) и **Receive Unicast Servers Updates** (Принимать обновления от серверов одноадресной передачи), - то системное время устанавливается в соответствии с данными времени, полученными от сервера одноадресной рассылки.

Poll Unicast Servers (Опрашивать серверы одноадресной передачи) - если этот параметр включен, отправляет запросы данных о времени сервера одноадресной рассылки SNTP на сервер SNTP.

Определение общих параметров SNTP с помощью команд консоли

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

Таблица 6-5. Определение общих параметров SNTP с помощью команд консоли

Команда консоли	Описание
<code>sntp client poll секунды таймера</code>	Устанавливает время опроса для клиента SNTP.
<code>sntp broadcast client enable</code>	Включает клиентов широковещательной передачи SNTP.
<code>sntp unicast client enable</code>	Включает предварительно определенных клиентов одноадресной передачи SNTP.
<code>sntp unicast client poll</code>	Включает опрос предварительно определенных серверов одноадресной передачи SNTP.
<code>show sntp configuration</code>	Отображает конфигурацию SNTP.
<code>show sntp status</code>	Отображает состояние SNTP.

Далее приведен пример команд консоли.

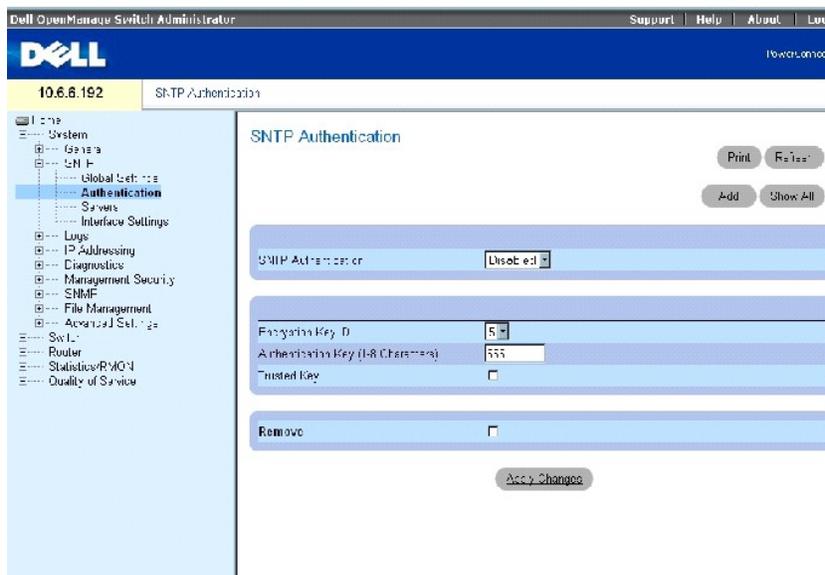
```
Console(config)# sntp anycast client enable
```

Определение методов проверки подлинности SNTP

Страница [SNTP Authentication](#) (Проверка подлинности SNTP) позволяет включить проверку подлинности SNTP между устройством и сервером SNTP. Сервер SNTP также выбирается на странице [SNTP Authentication](#) (Проверка подлинности SNTP).

Выберите **System** (Система) → **SNTP** → **Authentication** (Проверка подлинности) на панели дерева, чтобы открыть страницу [SNTP Authentication](#) (Проверка подлинности SNTP).

Рис. 6-8. Страница SNTP Authentication (Проверка подлинности SNTP)



Страница [SNTP Authentication](#) (Проверка подлинности SNTP) содержит следующие поля.

SNTP Authentication (Проверка подлинности SNTP) - включает проверку подлинности сеанса SNTP между устройством и сервером SNTP.

Encryption Key ID (Идентификатор ключа шифрования) - содержит список идентификаторов ключа, определенных пользователем, для проверки подлинности сервера SNTP и устройства. Возможные значения этого поля: от 1 до 4294967295.

Authentication Key (1-8 Characters) (Ключ проверки подлинности (от 1 до 8 символов)) - определяет ключ, используемый для проверки подлинности.

Trusted Key (Доверенный ключ) - установите этот флажок, чтобы указать, какой ключ шифрования используется (одноадресный/передача любого типа) или выбран (широковещательный) для проверки подлинности сервера SNTP.

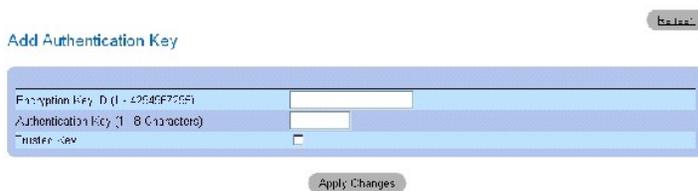
Remove (Удалить) - установите этот флажок, чтобы удалить выбранный ключ проверки подлинности.

Добавление ключа проверки подлинности SNTP

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

Откроется страница [Add Authentication Key](#) (Добавление ключа проверки подлинности).

Рис. 6-9. Страница Add Authentication Key (Добавление ключа проверки подлинности)



3. Определите поля.

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

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

Отображение таблицы ключей проверки подлинности

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

Откроется страница [Authentication Key Table](#) (Таблица ключей проверки подлинности).

Рис. 6-10. Страница Authentication Key Table (Таблица ключей проверки подлинности)



Удаление ключа проверки подлинности

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

Откроется страница [Authentication Key Table](#) (Таблица ключей проверки подлинности).

3. Выберите запись в **Authentication Key Table** (Таблице ключей проверки подлинности).
4. Установите флажок **Remove** (Удалить).
5. Нажмите кнопку **Apply Changes** (Применить изменения).

Запись будет удалена, а устройство обновлено.

Определение параметров проверки подлинности SNMP с помощью команд консоли

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

Таблица 6-6. Команды консоли для проверки подлинности SNMP

Команда консоли	Описание
<code>sntp authenticate</code>	Требует проверку подлинности для полученного трафика NTP (Network Time Protocol).
<code>sntp authentication-key число md5 значение</code>	Определяет ключ проверки подлинности для SNMP.
<code>sntp trusted-key номер_ключа</code>	Определяет ключ проверки подлинности, используемый для проверки подлинности сервера SNMP.
<code>show sntp configuration</code>	Отображает конфигурацию SNMP.

Далее приведен пример команд консоли.

```
Console(config)# snmp authentication-key 8 md5 ClkKey

Console(config)# snmp trusted-key 8

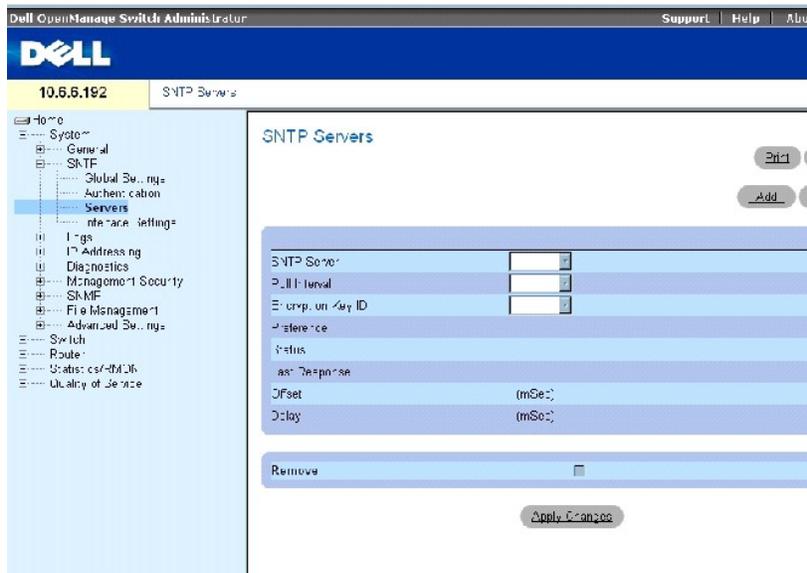
Console(config)# snmp authenticate
```

Определение серверов SNMP

Страница [SNMP Servers](#) (Серверы SNMP) содержит информацию для выбора сервера SNMP, а также позволяет добавить новый сервер SNMP.

Чтобы открыть страницу [SNMP Servers](#) (Серверы SNMP), выберите System (Система) → SNMP → Servers (Серверы) на панели дерева.

Рис. 6-11. Страница SNMP Servers (Серверы SNMP)



Страница [SNMP Servers](#) (Серверы SNMP) содержит следующие поля.

SNMP Server (Сервер SNMP) - содержит список определяемых пользователем IP-адресов сервера SNMP. Можно определить до восьми серверов SNMP.

Poll Interval (Интервал опроса) - включает опрос выбранного сервера SNMP для получения данных о времени.

Encryption Key ID (Идентификатор ключа шифрования) - содержит список идентификаторов ключа, используемых для обмена данными между сервером SNMP и устройством. Encryption Key ID (Идентификатор ключа шифрования) определяется на странице [SNMP Authentication](#) (Проверка подлинности SNMP).

Preference (Настройка) - сервер SNMP, предоставляющие данные о системном времени SNMP. Возможные значения:

Primary (Основной) - основной сервер, предоставляющий информацию SNTP.

Secondary (Дополнительный) - резервный сервер, предоставляющий информацию SNTP.

Status (Состояние) - рабочее состояние сервера SNTP. Возможные значения:

Up (Работает) - сервер SNTP работает надлежащим образом.

Down (Отключен) - сервер SNTP в настоящее время недоступен. Например, сервер SNTP в настоящее время не подключен или отключен.

In progress (Выполняется операция) - сервер SNTP отправляет или принимает информацию SNTP.

Unknown (Неизвестно) - состояние процесса передачи информации SNTP в настоящее время неизвестно. Например, устройство в настоящее время выполняет поиск интерфейса.

Last Response (Последний ответ) - время, когда был получен последний ответ от сервера SNTP.

Offset (Смещение) - разница во времени между часами устройства и временем, полученным от сервера SNTP.

Delay (Задержка) - время, необходимое для передачи пакета до сервера SNTP.

Remove (Удалить) - установите этот флажок, чтобы удалить определенный сервер SNTP из списка **SNTP Servers** (Серверы SNTP).

Добавление сервера SNTP

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

Откроется страница [Add SNTP Server](#) (Добавление сервера SNTP).

Рис. 6-12. Страница Add SNTP Server (Добавление сервера SNTP)

The screenshot shows a web interface for adding an SNTP server. At the top left is the title "Add SNTP Server" and a "Refresh" button. Below is a form with three fields: "SNTP Server" (text input with placeholder "(XXXX)"), "Port Interval" (dropdown menu currently showing "Disabled"), and "Encryption Key ID" (text input with value "5"). At the bottom of the form is an "Apply Changes" button.

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

Будет добавлен сервер SNTP, а устройство будет обновлено.

Отображение таблицы серверов SNTP

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

Откроется страница [SNTP Servers Table](#) (Таблица серверов SNTP).

Рис. 6-13. Страница SNTP Servers Table (Таблица серверов SNTP)

SNTP Server	Poll Interval	Encryption Key ID	Preference	Status	Last Response	Offset	Delay	Remove
-------------	---------------	-------------------	------------	--------	---------------	--------	-------	--------

Изменение сервера SNTP

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

Откроется страница [SNTP Servers Table](#) (Таблица серверов SNTP).

3. Выберите запись сервера SNTP.
4. Измените соответствующие поля.
5. Нажмите кнопку **Apply Changes** (Применить изменения).

Информация сервера SNTP будет обновлена.

Удаление сервера SNTP

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

Откроется страница [SNTP Servers Table](#) (Таблица серверов SNTP).

3. Выберите запись SNTP Server (Сервер SNTP).
4. Установите флажок **Remove** (Удалить).
5. Нажмите кнопку **Apply Changes** (Применить изменения).

Запись будет удалена, а устройство обновлено.

Определение серверов SNTP с помощью команд консоли

В следующей таблице приведены команды консоли для настройки полей, отображаемых на странице [SNTP Servers](#) (Серверы SNTP).

Таблица 6-7. Команды консоли для проверки подлинности SNTP

Команда консоли	Описание
-----------------	----------

<code>sntp server {ip- адрес имя_хоста} [poll] [key идентификатор_ключа]</code>	Определяет сервер SNTP, который может использоваться для синхронизации данных о времени.
<code>no sntp server ip- address</code>	Удаляет сервер из списка серверов SNTP.

Далее приведен пример команд консоли.

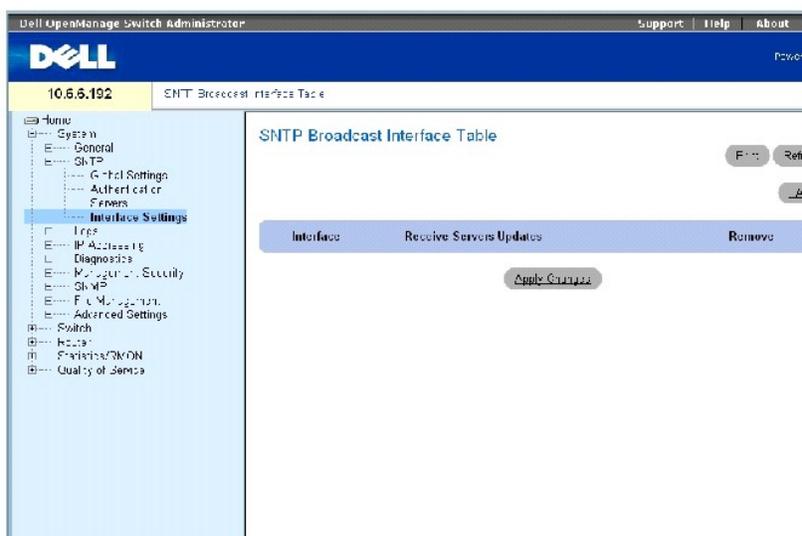
```
Console(config)# sntp server 100.1.1.1 poll key 10
```

Определение интерфейсов SNTP

Страница [SNTP Broadcast Interface Table](#) (Таблица интерфейсов широковещательной передачи SNTP) содержит поля для определения параметров SNTP для различных интерфейсов.

Чтобы открыть страницу [SNTP Broadcast Interface Table](#) (Таблица интерфейсов широковещательной передачи SNTP), выберите **System** (Система) → **SNTP** → **Interfaces Settings** (Параметры интерфейсов).

Рис. 6-14. SNTP Broadcast Interface Table (Таблица интерфейсов широковещательной передачи SNTP)



Страница [SNTP Broadcast Interface Table](#) (Таблица интерфейсов широковещательной передачи SNTP) содержит следующие поля.

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

Receive Servers Updates (Принимать обновления сервера) - включает или отключает получение обновлений SNTP для определенного интерфейса.

Remove (Удалить) - установите этот флажок, чтобы отключить SNTP для определенного интерфейса.

Включение SNTP для интерфейса

1. Откройте таблицу [SNTP Broadcast Interface Table](#) (Таблица интерфейсов широковещательной передачи SNTP).
2. Нажмите кнопку **Add** (Добавить).

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

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

Для интерфейса будет включен протокол SNTP, а устройство обновлено.

Определение параметров интерфейса SNTP с помощью команд консоли

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

 **ПРИМЕЧАНИЕ.** При настройке интерфейса широковещательной рассылки или интерфейса любого типа передачи необходимо настроить хотя бы один IP-адрес.

Таблица 6-8. Команды консоли для параметров интерфейса SNTP

Команда консоли	Описание
<code>sntp client enable</code>	Включает клиента широковещательной передачи и передачи любого типа SNTP (Simple Network Time Protocol) для интерфейса.
<code>show sntp configuration</code>	Отображает конфигурацию SNTP.

Далее приведен пример команд консоли для настройки интерфейсов SNTP.

Console (config)# interface ethernet g1
Console (config-if)# sntp client enable
Console (config-if)# end
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: g1			

Настройка портов управления вне диапазона (OOB)

В этом разделе описано управление следующими функциями устройства через порт управления вне диапазона. Он содержит информацию об удаленном сервере журнала, шлюзе по умолчанию, параметрах IP-интерфейса, сервере TACACS+ и сервере RADIUS вне диапазона.

При управлении функциями с помощью порта управления вне диапазона управление этими функциями внутри диапазона отключено. Для настройки этих функций через порт вне диапазона используйте интерфейс SNMP.

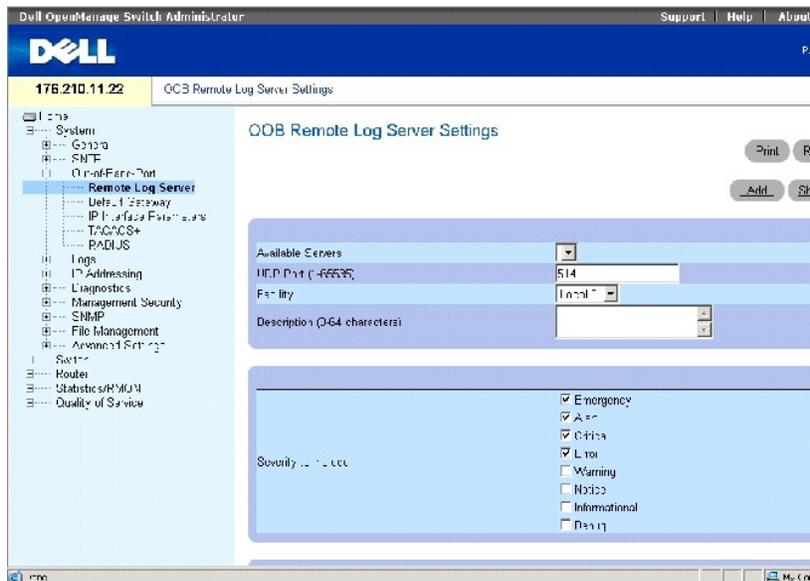
Чтобы открыть страницу OOB Configuration (Настройка OOB), выберите **System** (Система)→ **Out of Band** (Вне диапазона) на панели дерева.

Настройка удаленных серверов журналов вне диапазона

Страница [OOB Remote Log Server Settings](#) (Параметры удаленного сервера журналов OOB) содержит поля для просмотра доступных серверов журналов вне диапазона. Кроме того, можно определить новые серверы журналов вне диапазона и уровень важности журналов, отправляемых на каждый сервер.

Чтобы открыть страницу [OOB Remote Log Server Settings](#) (Параметры удаленного сервера журналов OOB), выберите **System** (Система)→ **Out of Band Port** (Порт вне диапазона)→ **Remote Log Server** (Удаленный сервер журналов) на панели дерева.

Рис. 6-15. OOB Remote Log Server Settings (Параметры удаленного сервера журналов OOB)



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

Available Servers (Доступные серверы) - серверы, на которые можно отправить журналы.

UDP Port (1-65535) (Порт UDP) - порт UDP, с которого отправляются журналы. Значение по умолчанию: 514.

Facility (Приложение) - определяемое пользователем приложение, из которого журналы системы отправляются на удаленный сервер. Для одного сервера можно назначить только одно приложение. Если назначен второй уровень приложения, первый уровень приложения отменяется. Все приложения, определенные для устройства, используют одно и то же приложение на сервере. Возможные значения этого поля: local 0, local 1, local 2, local 3, local 4, local 5, local 6 и local 7.

Description (0-64 characters) (Описание (0-64 символов)) - отображает описание сервера, задаваемое пользователем.

Severity to Include (Указываемая важность) - важность журнала. При выборе уровня важности автоматически выбираются все высокие уровни.

Delete Server (Удалить сервер) - когда флажок установлен, сервер удаляется из списка **Available Servers** (Доступные серверы).

Страница [OOB Remote Log Server Settings](#) (Параметры удаленного сервера журналов OOB) также содержит список важности. Определения важности те же, что описаны в таблице [RAM Log Table](#) (Таблица журнала ОЗУ) на [стр. 126](#).

Отправка журналов на сервер журналов вне диапазона

1. Откройте страницу [OOB Remote Log Server Settings](#) (Параметры удаленного сервера журналов OOB).
2. Определите поля **UDP Port** (Порт UDP), **Facility** (Приложение) и **Description** (Описание).
3. Выберите тип журнала и важность журнала.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Параметры журналов будут сохранены, а устройство обновлено.

 **ПРИМЕЧАНИЕ.** Перед добавлением нового сервера определите IP-адрес удаленного сервера журналов вне диапазона.

Определение нового сервера журналов вне диапазона

1. Откройте страницу [OOB Remote Log Server Settings](#) (Параметры удаленного сервера журналов OOB).
2. Нажмите кнопку **Add** (Добавить), чтобы отобразить страницу **Add an OOB Log Server** (Добавление серверов журналов OOB).
3. Введите значения в полях диалогового окна.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

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

Удаление сервера журналов вне диапазона

1. Откройте страницу [OOB Remote Log Server Settings](#) (Параметры удаленного сервера журналов OOB).
2. Нажмите кнопку **Show All** (Показать все), чтобы отобразить страницу **OOB Remote Log Servers Table** (Таблица удаленных серверов журналов OOB).
3. Выберите сервер и установите флажок **Remove** (Удалить).
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Сервер будет удален, а устройство обновлено.

Настройка удаленного сервера журналов вне диапазона с помощью команд консоли

В таблице перечислены команды консоли для работы с полями страницы [OOB Remote Log Server Settings](#) (Параметры удаленного сервера журналов OOB).

Таблица 6-9. Команды консоли для настройки параметров удаленного сервера журналов вне диапазона

Команда консоли	Описание
<code>logging oob/ip- address [port порт] [severity уровень] [facility приложение] [description текст]</code>	Определяет новый удаленный сервер журналов.

Далее приведен пример команд консоли.

```
Console(config)#logging oob/10.2.2.2 severity critical facility local0 description syslog_server_1
```

Определения шлюза по умолчанию вне диапазона

Для назначения шлюза по умолчанию используйте страницу [OOB Default Gateway](#) (Шлюз по умолчанию OOB). При отправке кадров в удаленную сеть пакеты пересылаются на IP-адрес по умолчанию. Настроенный IP-адрес должен принадлежать той же подсети IP-адресов, что и один из IP-интерфейсов. При удалении IP-интерфейса, к которому подключен шлюз по умолчанию, также удаляется и шлюз по умолчанию.

Чтобы открыть страницу [OOB Default Gateway](#) (Шлюз по умолчанию OOB), выберите **System** (Система)→ **Out of Band Port** (Порт вне диапазона)→ **Default Gateway** (Шлюз по умолчанию) на панели дерева.

Рис. 6-16. Шлюз по умолчанию OOB



Страница [OOB Default Gateway](#) (Шлюз по умолчанию) содержит следующий параметр.

Default Gateway (Шлюз по умолчанию) - показывает IP-адрес шлюза.

Выбор устройства шлюза вне диапазона

1. Откройте страницу [OOB Default Gateway](#) (Шлюз по умолчанию OOB).
2. Определите IP-адрес в поле Default Gateway (Шлюз по умолчанию).
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Шлюз вне диапазона будет определен, а устройство обновлено.

Таблица 6-10. Команды консоли для определения шлюза по умолчанию вне диапазона

Команда консоли	Описание
<code>ip default gateway ip-адрес</code>	Определяет IP-шлюз вне диапазона.

Далее приведен пример команд консоли.

```
Console(config)# interface out-of-band-eth
```

```
Console(config-oob)# ip address 10.0.0.1 /8
```

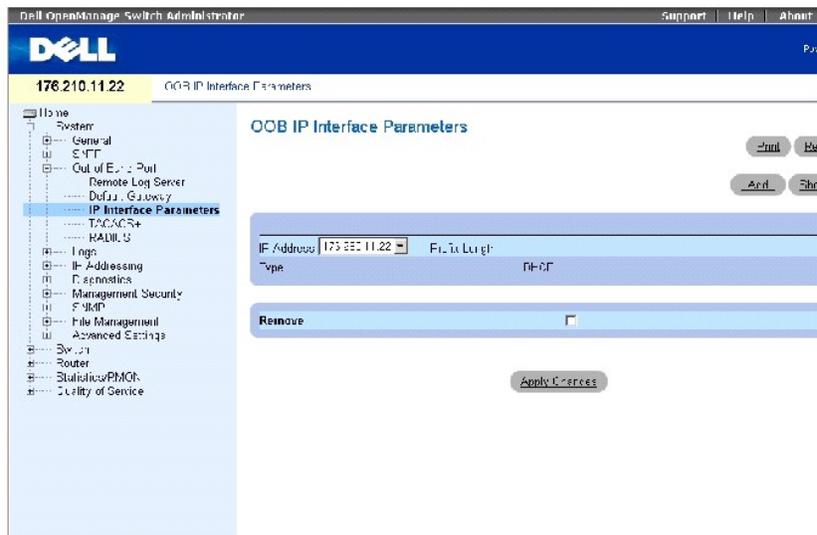
```
Console(config-oob)# ip default-gateway 10.1.1.1
```

Определение параметров IP-интерфейса вне диапазона

Страница [OOB IP Interface Parameters](#) (Параметры IP-интерфейса OOB) содержит параметры для назначения IP-адресов вне диапазона для интерфейсов.

Чтобы открыть страницу [OOB IP Interface Parameters](#) (Параметры IP-интерфейса OOB), выберите **System** (Система) → **Out of Band Port** (Порт вне диапазона) → **IP Interface Parameters** (Параметры IP-интерфейса) на панели дерева.

Рис. 6-17. Параметры IP-интерфейса OOB



Страница [OOB IP Interface Parameters](#) (Параметры IP-интерфейса OOB) содержит следующие параметры.

IP Address (IP-адрес) - IP-адрес интерфейса вне диапазона.

Prefix Length (Длина префикса) - число бит, образующих префикс исходного IP-адреса, или сетевая маска исходного IP-адреса.

Type (Тип) - показывает тип созданного IP-интерфейса OOB - DHCP или статический.

Remove (Удалить) - когда установлен этот флажок, удаляется интерфейс, выбранный в раскрывающемся списке **IP Address** (IP-адрес).

ПРИМЕЧАНИЕ. IP-адреса DHCP для управления вне диапазона можно настроить на странице [DHCP IP Interface](#) (IP-интерфейс DHCP) (System) → **IP Address** (IP-адрес) → **DHCP IP Interface** (IP-интерфейс DHCP)).

Добавление IP-интерфейса

1. Откройте страницу [OOB IP Interface Parameters](#) (Параметры IP-интерфейса OOB).
2. Нажмите кнопку **Add** (Добавить), чтобы отобразить страницу **Add a Static OOB IP Interface** (Добавление статического IP-интерфейса).
3. В поле **Network Mask** (Маска сети) укажите маску подсети исходного IP-адреса.
4. Заполните поля на этой странице.
5. Нажмите кнопку **Apply Changes** (Применить изменения).

Новый интерфейс будет добавлен, а устройство обновлено.

Удаление IP-адресов

1. Откройте страницу [OOB IP Interface Parameters](#) (Параметры IP-интерфейса OOB).
2. Нажмите кнопку **Show All** (Показать все).
3. Откроется страница **Interface Parameters Table** (Таблица параметров интерфейса).
4. Выберите IP-адрес в раскрывающемся списке **IP Address** (IP-адрес).

5. Выберите запись в **Interface Parameters Table** (Таблице параметров интерфейса).
6. Установите флажок **Remove** (Удалить).
7. Нажмите кнопку **Apply Changes** (Применить изменения).

IP-адрес будет удален, а устройство обновлено.

Определение IP-интерфейсов с помощью команд консоли

В следующей таблице приведены команды консоли для работы с полями на странице [OOB IP Interface Parameters](#) (Параметры IP-интерфейса OOB).

Таблица 6-11. Команды консоли для определения параметров IP-интерфейса вне диапазона

Команда консоли	Описание
<code>interface out-of- band-eth</code>	Настраивает порт Ethernet вне диапазона и устанавливает режим настройки интерфейса.
<code>ip address ip- адрес {маска длина_префикса}</code>	Задаёт IP-адрес.

Далее приведен пример команд консоли.

```
Console# configure
```

```
Console(config)# interface out-of-band-eth
```

```
Console(config-oob)# ip address 192.168.0.1 /8
```

Настройка серверов TACACS+ вне диапазона

Устройство предоставляет поддержку для клиентов TACACS+ (Terminal Access Controller Access Control System). TACACS+ обеспечивает централизованную систему безопасности для проверки пользователей, получающих доступ к устройству.

TACACS+ обеспечивает централизованную систему управления при соблюдении совместимости с RADIUS и другими процессами проверки подлинности. TACACS+ предоставляет следующие службы:

- 1 **Authentication** (Проверка подлинности) - обеспечивает проверку подлинности во время входа в систему, а также по именам пользователей и определенным пользователями паролям.
- 1 **Authorization** (Авторизация) - выполняется при входе. После завершения сеанса проверки подлинности запускается сеанс авторизации с использованием проверенного имени пользователя. Сервер TACACS+ проверяет привилегии пользователя.

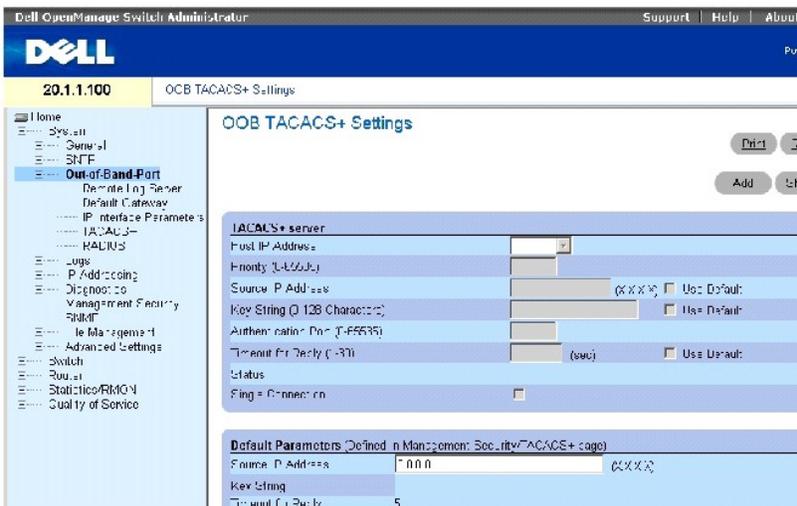
Серверы TACACS+ можно определить для портов в диапазоне с помощью страницы [TACACS+ Settings](#) (Параметры TACACS+) или для портов вне диапазона.

Протокол TACACS+ обеспечивает целостность сети благодаря обмену шифрованными данными протокола между устройством и сервером TACACS+.

Страница [OOB TACACS+ Settings](#) (Параметры TACACS+ OOB) содержит настройки TACACS+ для порта управления вне диапазона как определенные пользователем, так и настройки по умолчанию.

Чтобы открыть страницу [OOB TACACS+ Settings](#) (Параметры TACACS+ OOB), выберите **System** (Система)→ **Out-of-Band-Port** (Порт вне диапазона)→ TACACS+ на панели дерева.

Рис. 6-18. OOB TACACS+ Settings (Параметры TACACS+ OOB)



Страница [OOB TACACS+ Settings](#) (Параметры TACACS+ OOB) содержит следующие поля.

Host IP Address (IP-адрес хоста) - определяет IP-адрес сервера TACACS+.

Priority (0-65535) (Приоритет) - определяет порядок, в котором используются серверы TACACS+. Значение по умолчанию: 0.

Source IP Address (IP-адрес источника) - IP-адрес устройства источника, используемый для сеанса TACACS+ между устройством и сервером TACACS+.

Key String (0-128 Characters) (Строка ключа (1-128 символов)) - определяет проверку подлинности и ключ шифрования обмена данными TACACS+ между устройством и сервером TACACS+. Этот ключ должен соответствовать шифрованию, используемому для сервера TACACS+.

Authentication Port (0-65535) (Порт проверки подлинности) - порт проверки подлинности, через который осуществляется обмен данными во время сеансов TACACS+. По умолчанию это порт 49.

Reply Timeout (1-30) (Время для ответа) - время ожидания ответа при обмене данными между устройством и сервером TACACS+. Диапазон значений: 1-30 секунд.

Status (Состояние) - состояние соединения между устройством и сервером TACACS+. Возможные значения:

Connected (Соединение установлено) - между устройством и сервером TACACS+ установлено соединение.

Not Connected (Соединение не установлено) - отсутствует соединение между устройством и сервером TACACS+.

Single Connection (Одно соединение) - когда выбран этот параметр, поддерживается одно открытое соединение между устройством и сервером TACACS+.

В качестве параметров TACACS+ по умолчанию используются параметры по умолчанию, определенные пользователем. Параметры по умолчанию

применяются для вновь определенных серверов TACACS+. Если значения по умолчанию не определены, для новых серверов TACACS+ используются системные настройки по умолчанию. Далее показаны настройки TACACS+ по умолчанию:

Source IP Address (IP-адрес источника) - IP-адрес устройства источника, используемый по умолчанию для сеанса TACACS+ между устройством и сервером TACACS+.

Key String (0-128 Characters) (Строка ключа (1-128 символов)) - используемые по умолчанию проверка подлинности и ключ шифрования обмена данными TACACS+ между устройством и сервером TACACS+.

Timeout for Reply (1-30) - (Время для ответа) - время ожидания ответа при обмене данным между устройством и сервером TACACS+.

 **ПРИМЕЧАНИЕ.** Значения по умолчанию для описанных выше параметров можно установить на странице **TACACS+ Settings** (Параметры TACACS+) ((System (Система)→ Management Security (Безопасность управления)→ TACACS+).

Определение параметров TACACS+

1. Откройте страницу [OOB TACACS+ Settings](#) (Параметры TACACS+ OOB).
2. Определите поля.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Параметры TACACS+ для данного устройства будут изменены.

Добавление сервера TACACS+

1. Откройте страницу [OOB TACACS+ Settings](#) (Параметры TACACS+ OOB).
2. Нажмите кнопку **Add** (Добавить).

Откроется страница **Add OOB TACACS+ Host** (Добавление хоста TACACS+).

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

Будет добавлен сервер TACACS+, а устройство будет обновлено.

Удаление сервера TACACS+ из списка серверов TACACS+

1. Откройте страницу [OOB TACACS+ Settings](#) (Параметры TACACS+ OOB).
2. Нажмите кнопку **Show All** (Показать все).

Откроется страница **TACACS+ Table** (Таблица TACACS+).

3. Выберите запись таблицы **TACACS+ Table**.
4. Установите флажок **Remove** (Удалить).
5. Нажмите кнопку **Apply Changes** (Применить изменения).

Будет удален сервер TACACS+, а устройство будет обновлено.

Определение серверов TACACS+ с помощью команд консоли

В следующей таблице перечислены команды консоли для работы с полями страницы OOB [TACACS+ Settings](#) (Параметры TACACS+ OOB).

Таблица 6-12. Команды консоли для настройки параметров TACACS+ вне диапазона

Команда консоли	Описание
tacacs-server host {oob/ip-адрес имя_хоста} [single-connection] [port номер_порта] [timeout тайм-аут] [key строка_ключа] [source источник] [priority приоритет]	Определяет хост сервера TACACS+.
no tacacs-server host {ip-адрес имя_хоста}	Удаляет указанный хост сервера TACACS+.
tacacs-server key [строка_ключа]	Определяет проверку подлинности и ключ шифрования для всех обменов данными TACACS+ между устройством и сервером TACACS+. Этот ключ должен соответствовать шифрованию, используемому для демона TACACS+ (Диапазон: 0-128 символов).
no tacacs-server key	Возвращает значения по умолчанию.
tacacs-server timeout тайм-аут	Указывает значение времени ожидания в секундах (Диапазон: 1-30).
no tacacs-server timeout	Возвращает значения по умолчанию.
tacacs-server source-ip oob/ip-адрес	Определяет IP-адрес источника (Диапазон: допустимый IP-адрес).
no tacacs-server source-ip oob/ip-адрес	Возвращает значения по умолчанию.
show tacacs [oob/ip-address]	Отображает настройку и статистику для сервера TACACS+.

Далее приведен пример команд консоли.

Console(config)# tacacs-server host oob/172.16.8.1 key abc						
Console (config)# end						
Console# show tacacs						
Device Configuration						

IP address	Status	Port	Single Connection	TimeOut	Source IP	Priority
-----	-----	----	-----	-----	-----	-----
No TACACS server is configured.						
OOB host Configuration						

IP address	Status	Port	Single Connection	TimeOut	Source IP	Priority
-----	-----	----	-----	-----	-----	-----
172.16.8.1	Not Connected	49	No	Global	Global	0
Global Values						

TimeOut: 5						
Device Configuration						

Source IP: 0.0.0.0						
OOB host Configuration						

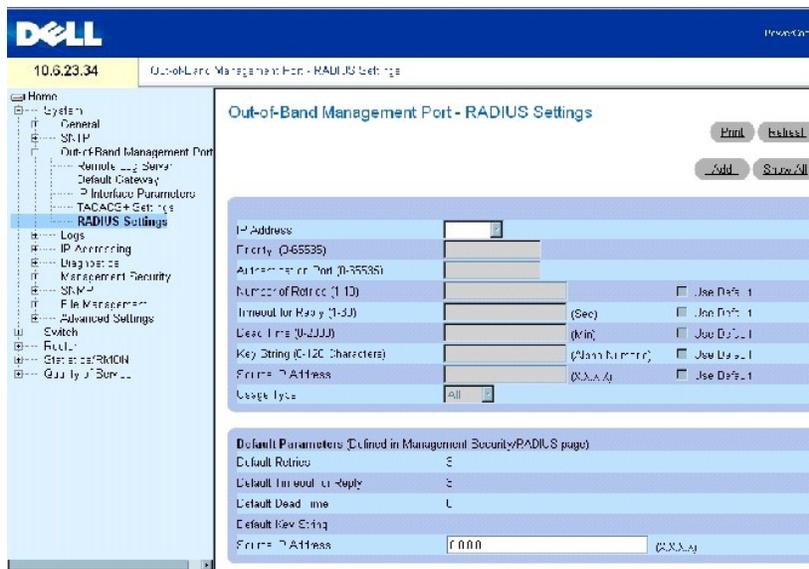
Source IP : 0.0.0.0						

Настройка серверов RADIUS вне диапазона

Страница [OOB RADIUS Settings](#) (Параметры RADIUS OOB) содержит настройки RADIUS для порта управления вне диапазона как определенные пользователем, так и настройки по умолчанию. Дополнительную информацию о серверах RADIUS см. в разделе «[Настройка параметров TACACS+](#)».

Чтобы открыть страницу [OOB RADIUS Settings](#) (Параметры RADIUS OOB), выберите **System** (Система) → **Out-of-Band Port** (Порт вне диапазона) → **RADIUS** на панели дерева (см. [OOB RADIUS Settings](#) (Параметры RADIUS OOB), [рис. 6-19](#)).

Рис. 6-19. Параметры RADIUS OOB



Страница [OOB RADIUS Settings](#) (Параметры RADIUS OOB) содержит следующие поля.

IP Address (IP-адрес) - проверка подлинности IP-адреса порта вне диапазона.

Priority (0-65535) (Приоритет) - приоритет порта вне диапазона. Возможны следующие значения: 0-65535.

Authentication Port (Порт проверки подлинности) - порт проверки подлинности, который используется для подтверждения проверки подлинности сервера RADIUS.

Number of Retries (1-10) (Число повторных попыток) - число запросов, переданных серверу RADIUS, прежде чем произошла ошибка. Возможные значения: 1-10. Значение по умолчанию: 3. Если для хоста не определено значение, для каждого хоста будет применяться общее значение.

Timeout for Reply (1-30) (Время для ответа) - время в секундах, в течение которого устройство ожидает ответа от сервера RADIUS. Возможные значения: 1-30. Значение по умолчанию: 3. Если для хоста не определено значение, для каждого хоста будет применяться общее значение.

Dead Time (0-2000) (Время отключения) - время (в минутах), в течение которого сервер RADIUS не принимает запросы на обработку. Диапазон значений: 0-2000. Если для хоста не определено значение, для каждого хоста будет применяться общее значение.

Key String (0-128 Characters) (Строка ключа (0-128 символов)) - строка ключа, используемая для проверки подлинности и шифрования всех данных RADIUS, передаваемых между устройством и сервером RADIUS. Этот ключ должен соответствовать шифрованию RADIUS. Если для хоста не определено значение, для каждого хоста будет применяться общее значение.

Source IP Address (IP-адрес источника) - IP-адрес устройства, подключающегося к серверу RADIUS.

В качестве параметров RADIUS по умолчанию используются параметры по умолчанию, определенные пользователем. Параметры по умолчанию применяются для вновь определенных серверов RADIUS. Если значения по умолчанию не определены, для новых серверов RADIUS используются системные настройки по умолчанию. Далее показаны настройки RADIUS по умолчанию.

Default Timeout for Reply (Время ожидания для ответа по умолчанию) - время по умолчанию, в течение которого устройство ожидает ответа от сервера RADIUS.

Default Retries (sec) (Число повторных попыток по умолчанию) - число запросов по умолчанию, передаваемых серверу RADIUS, прежде чем отображается ошибка.

Default Dead Time (sec) (Время отключения по умолчанию) - время по умолчанию (в минутах), в течение которого сервер RADIUS не принимает запросы на обработку. Диапазон значений: 0-2000.

Default Key String (Строка ключа по умолчанию) - строка ключа, используемая для проверки подлинности и шифрования всех данных RADIUS, передаваемых между устройством и сервером RADIUS. Этот ключ должен соответствовать шифрованию RADIUS.

 **ПРИМЕЧАНИЕ.** Значения по умолчанию для описанных выше параметров можно установить на странице [RADIUS Settings](#) (Параметры RADIUS) (System (Система)→ Management Security (Безопасность управления)→ RADIUS).

Source IP Address (IP-адрес источника) - IP-адрес по умолчанию устройства, подключающегося к серверу RADIUS.

Определение параметров RADIUS вне диапазона

1. Откройте страницу [OOB RADIUS Settings](#) (Параметры RADIUS OOB).
2. Определите следующие поля. **Default Timeout for Reply** (Время ожидания для ответа по умолчанию), **Default Retries** (Число повторных попыток по умолчанию), **Default Dead Time** (Время отключения по умолчанию) и **Default Key** (Ключ по умолчанию).
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Параметры RADIUS для данного устройства будут изменены.

Добавление сервера RADIUS вне диапазона

1. Откройте страницу [OOB RADIUS Settings](#) (Параметры RADIUS OOB).
2. Нажмите кнопку **Add** (Добавить), чтобы отобразить страницу **Add OOB RADIUS Server** (Добавить сервер RADIUS OOB).
3. Введите значения в полях диалогового окна.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Новый сервер RADIUS будет добавлен, а устройство обновлено.

Удаление сервера RADIUS вне диапазона из списка серверов RADIUS

1. Откройте страницу [OOB RADIUS Settings](#) (Параметры RADIUS OOB).
2. Нажмите кнопку **Show All** (Показать все), чтобы отобразить список **OOB RADIUS Servers** (Серверы RADIUS OOB).
3. Выберите сервер RADIUS и установите флажок **Remove** (Удалить).
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Сервер RADIUS будет удален из списка серверов RADIUS.

Определение серверов RADIUS с помощью команд консоли

В следующей таблице перечислены команды консоли для работы с полями страницы [OOB RADIUS Settings](#) (Параметры RADIUS OOB).

Таблица 6-13. Команды консоли для настройки параметров RADIUS вне диапазона

Команда консоли	Описание
<code>radius-server host ip-адрес [auth-port номер_порта_аутентификации] [timeout количество_секунд] [retransmit количество_попыток] [deadtime количество_секунд] [key строка_ключа] [source источник] [priority приоритет]</code>	Определяет хост сервера RADIUS.
	Удаляет указанный хост сервера RADIUS.

no radius-server host <i>ip- адрес</i>	
radius-server source-ip <i>источник</i>	Определяет исходный IP-адрес, который используется для связи с серверами RADIUS.
no radius-server-ip	Возвращает значения по умолчанию.
radius-server timeout <i>количество_секунд</i>	Задаёт интервал, в течение которого маршрутизатор ожидает ответа сервера.
no radius-server deadtime	Устанавливает время отключения, равное 0.

Далее приведен пример команд консоли.

```
console(config)#interface out-of-band eth 1
```

```
console radius-server host oob/10.2.2.2 key 123
```

Управление журналами

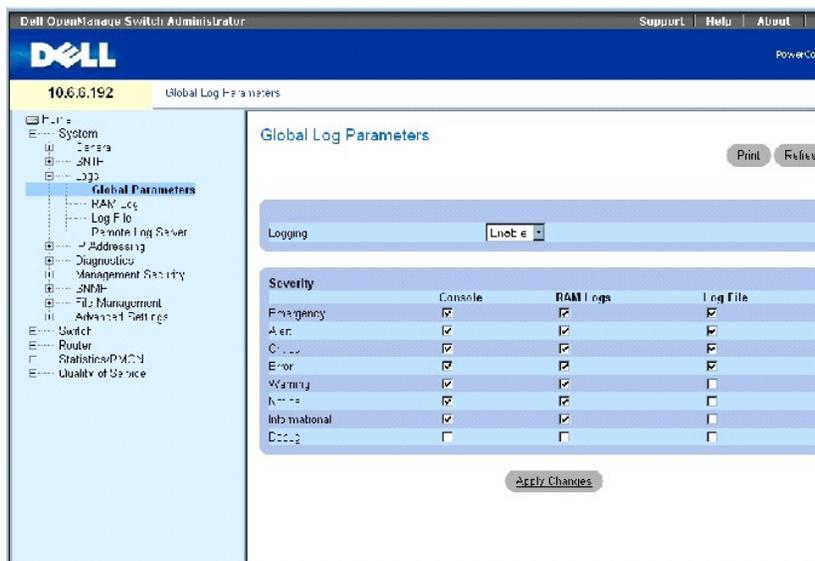
Страница [Logs \(Журналы\)](#) содержит ссылки на страницы разных журналов. Чтобы отобразить страницу [Logs \(Журналы\)](#), выберите **System (Система)**→ **Logs (Журналы)** на панели дерева.

Страница [Global Log Parameters \(Общие параметры журналов\)](#)

Страница [Global Log Parameters \(Общие параметры журналов\)](#) содержит поля для общего включения журналов и поля для определения параметров журналов. Сообщения журнала Severity (Важность) перечисляются в порядке от большей важности к меньшей.

Чтобы открыть страницу [Global Log Parameters \(Общие параметры журналов\)](#), выберите **System (Система)**→ **Logs (Журналы)**→ **Global Parameters (Общие параметры)** на панели дерева.

Рис. 6-20. Страница [Global Log Parameters \(Общие параметры журналов\)](#)



Страница [Global Log Parameters](#) (Общие параметры журналов) содержит следующие поля.

Logging (Регистрация) - включает функции создания глобальных журналов для кэширования, файлов и серверов на устройстве. Все журналы, которые распечатываются на консоли, сохраняются в файлах журналов. Возможные значения:

Enable (Включить) - включает сохранение журналов в кэше (ОЗУ), файле (FLASH) и на внешнем сервере.

Disable (Отключить) - отключает сохранение журналов. Регистрацию журналов, отображаемых на консоли, невозможно отключить.

Emergency (Аварийное) - наивысший уровень предупреждения. Если устройство выключено или работает неправильно, на устройстве сохраняется аварийный журнал.

Alert (Сигнал о сбое) - второй уровень аварийного предупреждения. Журнал сохраняется при серьезных отклонениях в работе устройства, например, если все функции устройства отключены.

Critical (Критическое) - третий уровень аварийного предупреждения. Критический журнал сохраняется в том случае, если происходят критические отклонения в работе устройства, например, если не работают два порта устройства, в то время как остальные по-прежнему работают.

Error (Ошибка) - произошла ошибка устройства, например, если порт отключен.

Warning (Предупреждение) - самый низкий уровень предупреждения устройства.

Notice (Замечание) - предоставляет сетевым администраторам информацию об устройстве.

Informational (Информационное) - предоставляет информацию об устройстве.

Debug (Отладка) - предоставляет подробные сведения о журнале. Уровень отладки должен использоваться только квалифицированным техническим персоналом.

Флажки устанавливаются в следующих трех столбцах:

Console (Консоль) - отправка журналов на консоль.

RAM Logs (Журналы ОЗУ) - отправка журналов в (кэш) ОЗУ.

Log File (Файл журнала) - отправка журналов в файл (флэш-память).

Включение журналов

1. Откройте страницу [Global Log Parameters](#) (Общие параметры журналов).
2. Выберите **Enable** (Включить) в раскрывающемся меню **Logging** (Регистрация).
3. С помощью флажков выберите тип и важность журнала.



ПРИМЕЧАНИЕ. При выборе уровня важности автоматически выбираются все более высокие уровни.

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

Параметры журналов будут сохранены, а устройство обновлено.

Включение общих параметров журналов с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для работы с полями, отображаемыми на странице [Global Log Parameters](#) (Общие параметры журналов).

Таблица 6-14. Команды консоли для общих параметров журналов

Команда консоли	Описание
logging on	Включает регистрацию сообщений об ошибках.
logging ip-address [port порт] [severity уровень] [facility приложение] [description текст]	Регистрирует сообщения на сервере системных журналов.
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.

Далее приведен пример команд консоли.

```
Console (config)# logging on
```

```
Console (config)# logging 10.1.1.1 severity critical
```

```
Console (config)# logging console errors
```

```
Console (config)# logging buffered debugging
```

```
Console (config)# logging file alerts
```

```
Console # clear logging
```

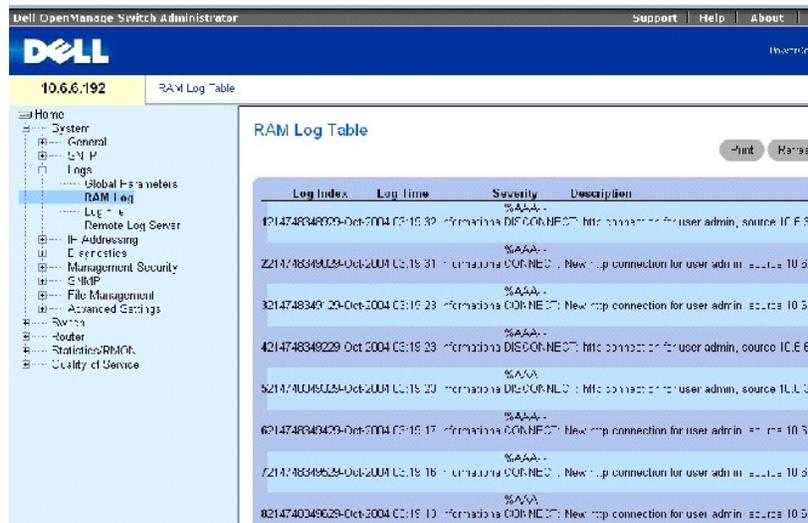
```
Clear Logging Buffer [y/n]? y
```

Таблица журнала ОЗУ

Таблица [RAM Log Table](#) (Таблица журнала ОЗУ) содержит сведения об определенных записях журнала, хранящегося в ОЗУ, включая время, когда был введен журнал, важность журнала и описание.

Чтобы отобразить таблицу [RAM Log Table](#) (Таблица журнала ОЗУ), выберите System (Система)→ Logs (Журналы)→ RAM Log (Таблица журнала ОЗУ) на панели дерева (см. [рис. 6-21](#)).

Рис. 6-21. Страница RAM Log Table (Таблица журнала ОЗУ)



Log Index	Log Time	Severity	Description
6214748349229	Oct-2004 09:16:32	Informational DISCONNECT	HTTP connection for user admin, source 10.5.3...
7214748349229	Oct-2004 09:16:31	Informational DISCONNECT	New http connection for user admin, source 10.5.3...
3214748349229	20-Oct-2004 09:16:29	Informational DISCONNECT	New http connection for user admin, source 10.5.3...
4214748349229	Oct-2004 09:16:28	Informational DISCONNECT	HTTP connection for user admin, source 10.5.3...
5214748349229	Oct-2004 09:16:27	Informational DISCONNECT	HTTP connection for user admin, source 10.5.3...
6214748349229	Oct-2004 09:16:17	Informational DISCONNECT	New http connection for user admin, source 10.5.3...
7214748349229	Oct-2004 09:16:16	Informational DISCONNECT	New http connection for user admin, source 10.5.3...
8214740349229	Oct-2004 09:16:13	Informational DISCONNECT	New http connection for user admin, source 10.5.3...

Таблица [RAM Log Table](#) (Таблица журнала ОЗУ) содержит следующие поля.

Log Index (Индекс журнала) - показывает номер журнала в таблице журнала ОЗУ.

Log Time (Время журнала) - время, когда журнал был введен в таблицу журнала ОЗУ.

Severity (Важность) - указывает важность журнала.

Description (Описание) - описание журнала.

Удаление информации журнала

1. Откройте страницу [RAM Log Table](#) (Таблица журнала ОЗУ).
2. Выберите **Clear Logs** (Очистить журналы).

Информация журнала будет удалена из таблицы файлов журналов, а устройство обновлено.

Просмотр [RAM Log Table](#) (Таблицы журнала ОЗУ) с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для просмотра полей, отображаемых на странице [RAM Log Table](#) (Таблица журнала ОЗУ).

Таблица 6-15. Команды консоли для просмотра [таблицы журнала ОЗУ](#)

Команда консоли	Описание
show logging	Отображает состояние журнала и системные сообщения, хранящиеся во внутреннем буфере.
clear logging	Удаляет сообщения из буфера журнала.

Далее приведен пример команд консоли.

```
Console # show logging
```

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

```
Buffer Logging: Level info. Buffer Messages: 30 Logged, 30 Displayed, 200 Max.
```

```
File Logging: Level error. File Messages: 1 Logged, 30 Dropped.
```

```
1 messages were not logged
```

```
10-Jan-2003 16:53:44 :%MSCM-I-NEWTERM: New TELNET connection from 143.166.155.18
```

```
10-Jan-2003 16:53:14 :%MSCM-I-TERMTERMINATED: TELNET connection from 143.166.155.18 terminated
```

```
10-Jan-2003 16:41:26 :%MSCM-I-NEWTERM: New TELNET connection from 143.166.155.18
```

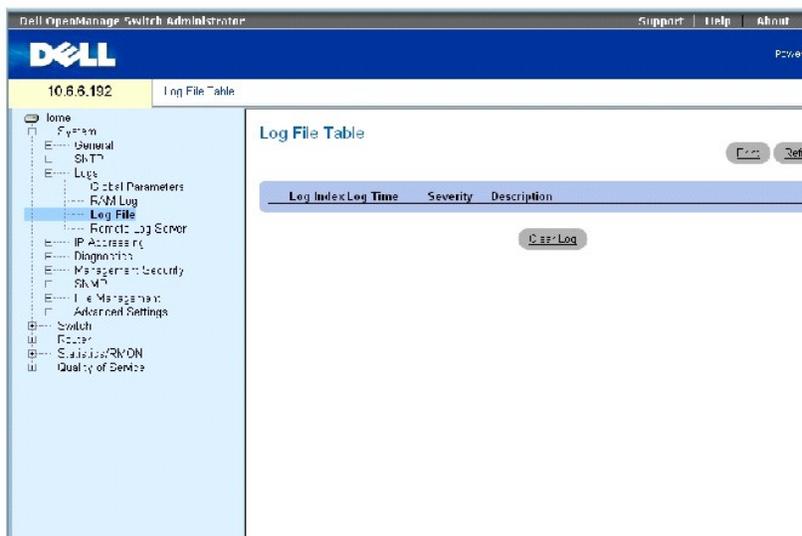
```
10-Jan-2003 09:24:59 :%INIT-I-Startup: Cold Startup
```

Таблица файла журнала

Таблица [Log File Table](#) (Таблица файла журналов) содержит сведения об определенных записях журналов, включая время, когда был введен журнал, важность журнала и описание журнала.

Чтобы отобразить таблицу [Log File Table](#) (Таблица файла журналов), выберите System (Система)→ Logs (Журналы)→ Log File (Файл журнала) на панели дерева (см. [таблицу 6-22](#)).

Рис. 6-22. Страница Log File Table (Таблица файла журналов)



Страница [Log File Table](#) (Таблица файла журналов) содержит следующие поля.

- 1 **Log Index** (Индекс журнала) - номер журнала в Log File Table (Таблице файла журналов).
- 1 **Log Time** (Время журнала) - время, когда журнал был введен в Log File Table (Таблицу файла журналов).
- 1 **Severity** (Важность) - указывает важность журнала.
- 1 **Description** (Описание) - описание журнала.

Вывод таблицы файла журналов с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для просмотра полей, отображенных в таблице [Log File Table](#) (Таблица файла журналов).

Таблица 6-16. Команды консоли для [таблицы файла журналов](#)

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

Далее приведен пример команд консоли.

```
Console # show logging file
```

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

Buffer Logging: Level info. Buffer Messages: 30 Logged, 30 Displayed, 200 Max.

File Logging: Level error. File Messages: 1 Logged, 30 Dropped.

1 messages were not logged

10-Jan-2003 16:53:44 :%MSCM-I-NEWTERM: New TELNET connection from 143.166.155.18

10-Jan-2003 16:53:14 :%MSCM-I-TERMTERMINATED: TELNET connection from 143.166.155.18 terminated

10-Jan-2003 16:41:26 :%MSCM-I-NEWTERM: New TELNET connection from 143.166.155.18

10-Jan-2003 09:24:59 :%INIT-I-Startup: Cold Startup

10-Jan-2003 09:22:51 :%LINK-I-Up: Oob-eth 1

10-Jan-2003 09:22:51 :%LINK-W-Down: g24

10-Jan-2003 09:22:51 :%LINK-W-Down: g23

10-Jan-2003 09:22:51 :%LINK-W-Down: g22

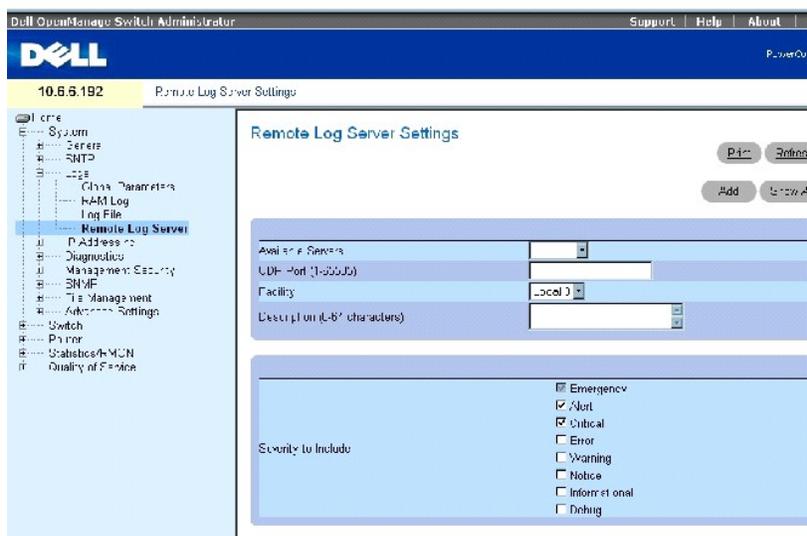
10-Jan-2003 09:22:51 :%LINK-W-Down: g21

удаленного сервера журналов

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

Чтобы открыть страницу [Remote Log Server Settings](#) (Параметры удаленного сервера журналов), выберите System (Система)→ Logs (Журналы)→ Remote Log Server (Удаленный сервер журналов)

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



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

Available Servers (Доступные серверы) - список серверов, на которые можно отправить журналы.

UDP Port (1-65535) (Порт UDP) - порт UDP, с которого отправляются журналы. Значение по умолчанию: 514.

Facility (Приложение) - определяемое пользователем приложение, из которого журналы системы отправляются на удаленный сервер. Для одного сервера можно назначить только одно приложение. Если назначен второй уровень приложения, первый уровень приложения отменяется. Все приложения, определенные для устройства, используют одно и то же приложение на сервере. Возможные значения этого поля: Local 0 - Local 7.

Description (Описание) - описание журнала. Максимальная длина составляет 64 символа.

Severity (Важность) - указывает важность журнала. При выборе уровня важности автоматически выбираются все высокие уровни.

Delete Server (Удалить сервер) - удаление сервера из списка **Available Server** (Доступные серверы). Установите флажок, чтобы удалить сервер из списка. Чтобы оставить сервер в списке, не устанавливайте флажок.

Страница [Remote Log Server Settings](#) (Параметры удаленного сервера журналов) также содержит список важности. Определения важности такие же, как и на странице [RAM Log Table](#) (Таблица журнала ОЗУ).

Отправка журналов на сервер

1. Откройте страницу [Remote Log Server Settings](#) (Параметры удаленного сервера журналов).
2. Определите поля **UDP Port** (Порт UDP), **Facility** (Приложение) и **Description** (Описание).
3. Выберите тип журнала и важность журнала, установив флажки для **Log Parameters** (Параметры журналов).

 **ПРИМЕЧАНИЕ.** При выборе уровня важности автоматически выбираются все более высокие уровни.

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

Параметры журналов будут сохранены, а устройство обновлено.

Определение нового сервера

1. Откройте страницу [Remote Log Server Settings](#) (Параметры удаленного сервера журналов).
2. Нажмите кнопку **Add** (Добавить), чтобы отобразить страницу **Add a Log Server** (Добавить сервер журналов).

 **ПРИМЕЧАНИЕ.** Перед добавлением нового сервера определите IP-адрес удаленного сервера журналов.

3. Введите значения в полях диалогового окна и нажмите кнопку **Apply Changes** (Применить изменения).

На странице [Remote Log Server](#) (Удаленный сервер журналов) сервер отображается в списке **Available Server** (Доступные серверы) только после обновления страницы вручную.

Удаление сервера журналов

1. Откройте страницу [Remote Log Server Settings](#) (Параметры удаленного сервера журналов).
2. Нажмите кнопку **Show All** (Показать все), чтобы отобразить страницу **Log Server Table** (Таблица серверов журналов).
3. Выберите сервер и установите флажок **Remove** (Удалить).
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Сервер будет удален, а устройство обновлено.

Работа с удаленным сервером журналов с помощью команд консоли

В таблице перечислены команды консоли для работы с удаленным сервером журналов.

Таблица 6-17. Команды консоли для удаленного сервера журналов

Команда консоли	Описание
<code>logging ip-адрес [port порт] [severity уровень] [facility приложение] [текст описания]</code>	Регистрирует сообщения на удаленном сервере.

Далее приведен пример команд консоли.

```
Console (config) # logging 10.1.1.1 severity critical
```

Определение IP-адресации

Для назначения IP-адресов интерфейса и шлюзов по умолчанию и для определения параметров ARP и DHCP для интерфейсов используйте страницу **IP Addressing** (IP-адресация).

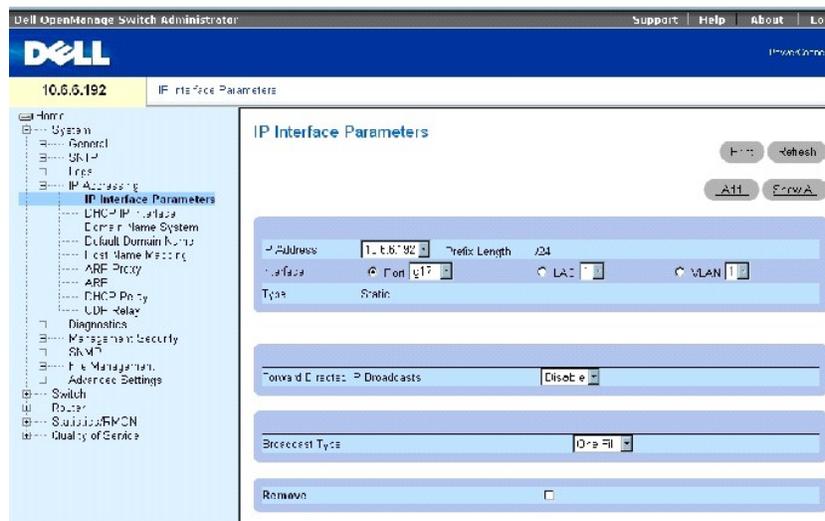
Чтобы открыть страницу **IP Addressing** (IP-адресация), выберите **System** (Система) → **IP Addressing** (IP-адресация) на панели дерева.

Определение IP-интерфейсов

Страница [IP Interface Parameters](#) содержит параметры для назначения IP-адресов интерфейсов.

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

Рис. 6-24. Страница IP Interface Parameters (Параметры IP-интерфейса)



Страница [IP Interface Parameters](#) (Параметры IP-интерфейса) содержит следующие поля.

IP Address (IP-адрес) - IP-адрес интерфейса.

Prefix Length (Длина префикса) - число бит, образующих префикс исходного IP-адреса, или сетевая маска исходного IP-адреса.

Interface (Интерфейс) - тип интерфейса, для которого определен IP-адрес. В это поле можно ввести следующие значения Port, LAG или VLAN.

Дополнительную информацию о настройке объединенных групп каналов (LAGs) см. в разделе «[Объединение портов](#)». Для получения сведений о настройке групп VLAN см. раздел «[Настройка групп VLAN](#)».

Type (Тип) - показывает, был ли IP-адрес определен как статический.

Forward Directed IP Broadcasts (Пересылать направленные IP-передачи) - включает передачу направленной широковещательной передачи на физические устройства широковещательной передачи. Если этот параметр отключен, направленные на IP-адрес широковещательные передачи будут отбрасываться и не будут переадресовываться.

Broadcast Type (Тип широковещательной передачи) - определяет адрес широковещательной передачи интерфейса.

One Fill (Заполнение единицами) - адрес широковещательной передачи интерфейса - 255.255.255.255.

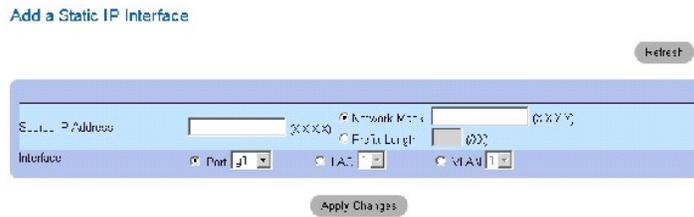
Zero Fill (Заполнение нулями) - адрес широковещательной передачи интерфейса - 0.0.0.0.

Remove (Удалить) - когда установлен этот флажок, удаляется интерфейс, выбранный в раскрывающемся меню **IP Address** (IP-адрес).

Добавление IP-интерфейса

1. Откройте страницу [IP Interface Parameters](#) (Параметры IP-интерфейса).
2. Нажмите кнопку **Add** (Добавить), чтобы открыть страницу [Add a Static IP Interface](#) (Добавление статического IP-интерфейса).

Рис. 6-25. Страница Add a Static IP Interface (Добавление статического интерфейса)



3. Заполните поля на этой странице.

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

Каждый элемент IP-адреса должен начинаться с цифры, отличной от 0. Например, IP-адреса 001.100.192.6 и 192.001.10.3 являются недопустимыми.

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

Новый интерфейс будет добавлен, а устройство обновлено.

Изменение параметров IP-адреса

1. Откройте страницу [IP Interface Parameters](#) (Параметры IP-интерфейса).
2. Выберите IP-адрес в раскрывающемся списке **IP Address** (IP-адрес).
3. Измените необходимые поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Параметры будут изменены, а устройство обновлено.

Удаление IP-адресов

1. Откройте страницу [IP Interface Parameters](#) (Параметры IP-интерфейса).
2. Нажмите кнопку **Show All** (Показать все), чтобы отобразить страницу [Interface Parameters Table](#) (Таблица параметров интерфейса).
3. Выберите IP-адрес и установите флажок **Remove** (Удалить).
4. Нажмите кнопку **Apply Changes** (Применить изменения).

IP-адрес будет удален, а устройство обновлено.

Определение параметров IP Interface с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для работы с полями на странице [IP Interface Parameters](#) (Параметры IP-интерфейса).

Таблица 6-18. Команды консоли для определения параметров IP-интерфейса

Команда консоли	Описание
<code>ip address ip-адрес {mask prefix-length}</code>	Задаёт IP-адрес.
<code>no ip address [ip-адрес]</code>	Удаляет IP-адрес.
<code>show ip interface [ethernet s vlan идентификатор_vlan номер_порта-канала]</code>	Отображает состояние готовности настроенных IP-интерфейсов.
<code>directed-broadcast</code>	Включает передачу направленной широковещательной рассылки на физическую широковещательную рассылку.

Далее приведен пример команд консоли.

```
Console (config)# interface vlan 1
```

```
Console(config-if)# ip address 192.168.1.1 255.255.255.0
```

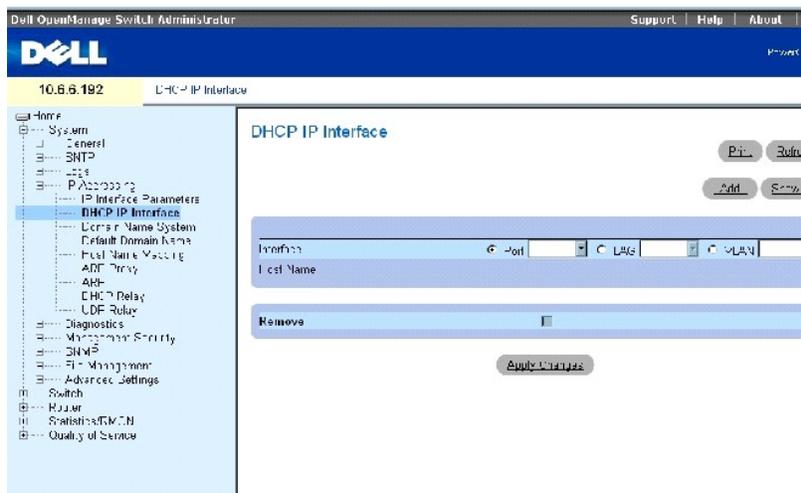
```
Console (config-if)# no ip address 192.168.1.1
```

Определение параметров IP-интерфейса DHCP

На странице [DHCP IP Interface](#) (IP-интерфейс DHCP) указываются клиенты DHCP, подключенные к устройству.

Чтобы открыть страницу [DHCP IP Interface](#) (IP-интерфейс DHCP), выберите **System** (Система) → **IP Addressing** (IP-адресация) → **DHCP IP Interface** (IP-интерфейс DHCP) на панели дерева.

Рис. 6-26. Страница DHCP IP Interface (IP-интерфейс DHCP)



Страница [DHCP IP Interface](#) (IP-интерфейс DHCP) содержит следующие поля.

Interface (Интерфейс) - определяет интерфейс, подключенный к устройству. Для выбора интерфейса, подключенного к устройству, выберите параметр **Port** (Порт), **LAG** или **VLAN**.

Host Name (Имя хоста) - имя системы.

Remove (Удалить) - когда установлен этот флажок, клиенты DHCP удаляются.

Добавление клиента DHCP

1. Откройте страницу [DSCP IP Interface](#) (IP-интерфейс DHCP).
2. Нажмите кнопку **Add** (Добавить), чтобы отобразить страницу **Add DHCP IP Interface** (Добавление IP-интерфейса DHCP).
3. Введите значения в поля на этой странице и нажмите кнопку **Apply Changes** (Применить изменения).

IP-интерфейс DHCP будет добавлен, а устройство обновлено.

Изменение IP-интерфейса DHCP

1. Откройте страницу [DSCP IP Interface](#) (IP-интерфейс DHCP).
2. Измените поля.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Запись будет изменена, а устройство обновлено.

Удаление IP-интерфейса DHCP

1. Откройте страницу [DSCP IP Interface](#) (IP-интерфейс DHCP).
2. Нажмите кнопку **Show All** (Показать все), чтобы открыть страницу **DHCP IP Interface Table** (IP-интерфейс DHCP).
3. Выберите запись клиента DHCP.
4. Установите флажок **Remove** (Удалить).
5. Нажмите кнопку **Apply Changes** (Применить изменения).

Запись будет удалена, а устройство обновлено.

Определение IP-интерфейсов DHCP с помощью команд консоли

В следующей таблице приведены команды консоли для определения IP-интерфейсов DHCP.

Таблица 6-19. Команды консоли для определения IP-интерфейсов DHCP

Команда консоли	Описание
<code>ip address dhcp [hostname имя_хоста]</code>	Для получения IP-адреса интерфейса Ethernet по протоколу DHCP (Dynamic Host Configuration Protocol)

Далее приведен пример команды консоли:

```
Console (config-if)# ip address dhcp hostname LA01
```

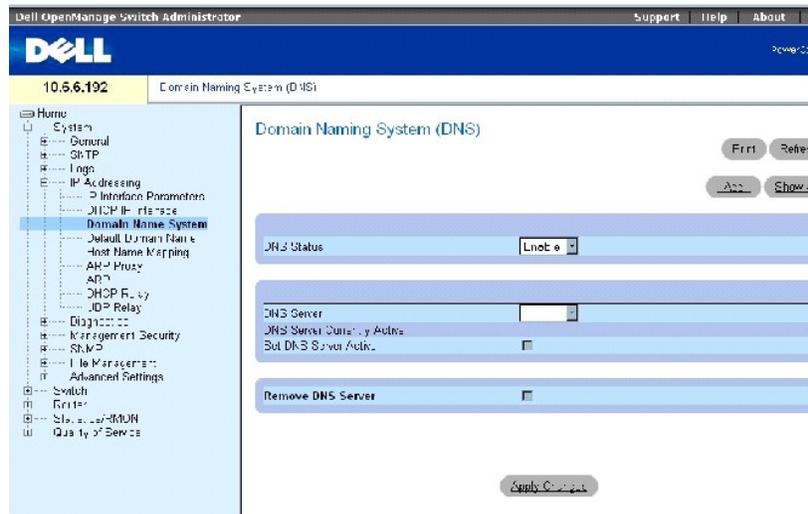
Настройка системы имен доменов

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

Страница [Domain Naming System \(DNS\)](#) (Система имен доменов) содержит поля для включения и активизации определенных серверов DNS.

Чтобы открыть страницу [Domain Naming System \(DNS\)](#) (Система имен доменов), выберите System (Система) → IP Addressing (IP-адресация) → Domain Name System (Система имен доменов) на панели дерева.

Рис. 6-27. Страница Domain Naming System (DNS) (Система имен доменов)



Страница [Domain Naming System \(DNS\)](#) (Система имен доменов) содержит следующие поля.

DNS Status (Состояние DNS) - включает или отключает перевод имен DNS в IP-адреса.

DNS Server (Сервер DNS) - содержит список серверов DNS. Серверы DNS добавляются на странице [Add DNS Server](#) (Добавление сервера DNS).

DNS Server Currently Active (Сервер DNS в настоящее время активен) - сервер DNS, который в настоящее время является активным сервером DNS.

Remove DNS Server (Удалить сервер DNS) - когда выбран этот параметр, серверы DNS удаляются.

Добавление сервера DNS

1. Откройте страницу [Domain Naming System \(DNS\)](#) (Система имен доменов).
2. Нажмите кнопку **Add** (Добавить).

Откроется страница [Add DNS Server](#) (Добавление сервера DNS).

Рис. 6-28. Страница Add DNS Server (Добавление сервера DNS)

Страница [Add DNS Server](#) (Добавление сервера DNS) содержит следующие поля.

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

DNS Server Currently Active (Сервер DNS в настоящее время активен) - указывает активный в настоящее время сервер DNS.

Set DNS Server Active (Сделать сервер DNS активным) - установите флажок, чтобы определить сервер DNS как активный сервер DNS.

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

Будет определен новый сервер DNS, а устройство обновлено.

Отображение таблицы серверов DNS

1. Откройте страницу [Domain Naming System \(DNS\)](#) (Система имен доменов).
2. Нажмите кнопку **Show All** (Показать все).

Откроется страница [DNS Server Table](#) (Таблица серверов DNS)

Рис. 6-29. Таблица DNS Server Table (Таблица серверов DNS)

Удаление серверов DNS

1. Откройте страницу [Domain Naming System \(DNS\)](#) (Система имен доменов).
2. Нажмите кнопку **Show All** (Показать все).
3. Откроется страница [DNS Server Table](#) (Таблица серверов DNS).
4. Выберите запись **DNS Server Table** (Таблица серверов DNS).
5. Установите флажок **Remove** (Удалить).
6. Нажмите кнопку **Apply Changes** (Применить изменения).

Выбранный сервер DNS будет удален, а устройство обновлено.

Настройка серверов DNS с помощью команд консоли

В следующей таблице приведены команды консоли для настройки серверов DNS.

Таблица 6-20. Команды консоли для сервера DNS

Команда консоли	Описание
<code>ip name-server</code> <i>адрес_сервера</i>	Задаёт доступные имена серверов. Можно определить до восьми имен серверов.
<code>no ip name-server</code> <i>адрес_сервера</i>	Удаляет имя сервера.
<code>ip domain-name</code> <i>имя</i>	Определяет имя домена по умолчанию, которое используется программой, если имена хостов указаны неправильно (Диапазон: 1-158 символов).
<code>no ip domain-name</code>	Удаляет имя домена по умолчанию (DNS).
<code>clear host</code> {name *}	Удаляет записи из кэша имя хоста-адрес.
<code>show hosts</code> [<i>имя</i>]	Отображает имя домена по умолчанию, список хостов сервера имен, статические имена и адреса, а также список имен и адресов из кэша.
<code>ip domain-lookup</code>	Включает систему DNS для преобразования имен хостов в IP-адреса.
<code>no ip domain-lookup</code>	Отключает систему DNS для преобразования имен хостов в IP-адреса.

Далее приведен пример команд консоли.

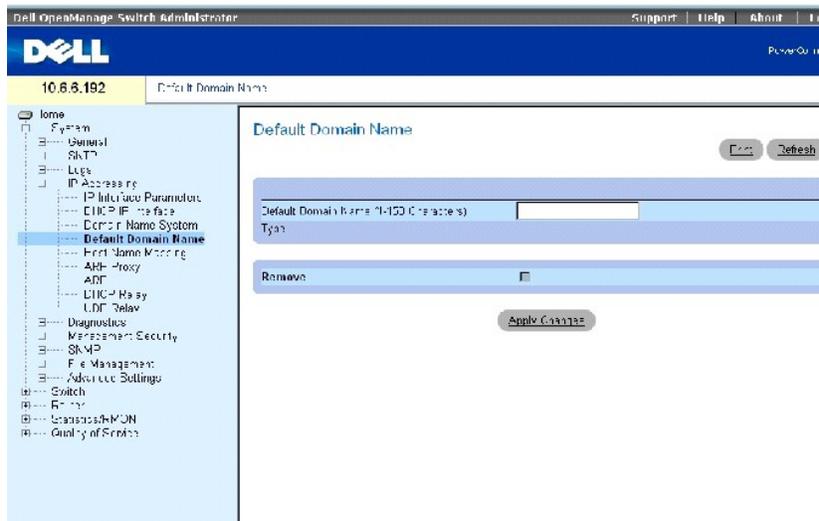
```
console (config)# ip name-server 176.16.1.18
```

Определение доменов по умолчанию

Страница [Default Domain Name](#) (Имя домена по умолчанию) содержит сведения для определения имен доменов DNS по умолчанию.

Чтобы открыть страницу [Default Domain Name](#) (Имя домена по умолчанию), выберите **System** (Система) → **IP Addressing** (IP-адресация) → **Default Domain Name** (Имя домена по умолчанию).

Рис. 6-30. Страница Default Domain Name (Имя домена по умолчанию)



Страница [Default Domain Name](#) (Имя домена по умолчанию) содержит следующие поля.

Default Domain Name (1-158 characters) (Имя домена по умолчанию (1-158 символов)) - содержит имя сервера доменов DNS, определяемое пользователем. При настройке применяется имя домена по умолчанию, если имена хостов указаны неправильно.

Type (Тип) - указывает, как создано имя домена - статически или динамически.

Remove (Удалить) - когда установлен этот флажок, удаляется имя домена по умолчанию.

Определение имен доменов DNS с помощью команд консоли

В следующей таблице приведены команды консоли для настройки имен доменов DNS.

Таблица 6-21. Команды консоли имен доменов DNS

Команда консоли	Описание
<code>ip domain-name имя</code>	Определяет имя домена по умолчанию, которое используется программой, если имена хостов указаны неправильно.
<code>no ip domain-name</code>	Удаляет имя домена по умолчанию (DNS).
<code>show hosts [VMSR]</code>	Отображает имя домена по умолчанию, список хостов сервера имен, статические имена и адреса, а также список имен и адресов из кэша.

Далее приведен пример команд консоли.

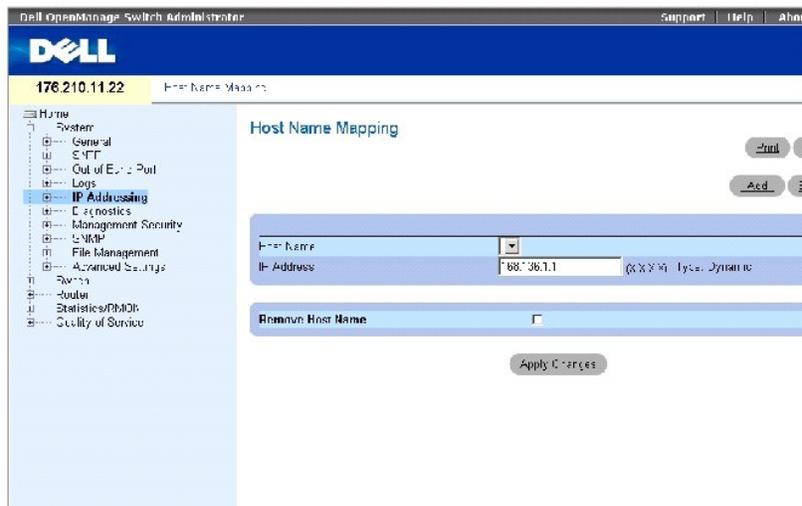
```
Console(config)# ip domain-name dell.com
```

Отображение хоста домена

Страница [Host Name Mapping](#) (Отображение имени хоста) содержит параметры для назначения IP-адресов для статических имен хостов. Страница [Host Name Mapping](#) (Отображение имени хоста) предоставляет один IP-адрес для каждого хоста.

Чтобы открыть страницу [Host Name Mapping](#) (Отображение имени хоста), выберите System (Система)→ IP Addressing (IP-адресация)→ Host Name Mapping (Отображение имени хоста).

Рис. 6-31. Страница Host Name Mapping (Отображение имени хоста)



Страница [Host Name Mapping](#) (Отображение имени хоста) содержит следующие поля.

Host Name (Имя хоста) - содержит список имен хостов. Имена хостов определяются на странице [Add Host Name Mapping](#) (Добавление отображения имени хоста). Каждый хост предоставляет один IP-адрес.

IP Address (X.X.X.X) (IP-адрес) - предоставляет IP-адрес, который назначается для определенного имени хоста.

Type (Тип) - тип IP-адреса. Возможные значения:

Dynamic (Динамический) - IP-адрес, который создается динамически.

Static (Статический) - статический IP-адрес.

Remove Host Name (Удалить имя хоста) - когда этот флажок установлен, удаляется отображение хоста DNS.

Добавление имен домена хоста

1. Откройте страницу [Host Name Mapping](#) (Отображение имени хоста).
2. Нажмите кнопку **Add** (Добавить).

Откроется страница [Add Host Name Mapping](#) (Добавление отображения имени хоста).

Рис. 6-32. Страница Add Host Name Mapping (Добавление отображения имени хоста)

[Refresh](#)

Add Host Name Mapping

Host Name (A-Z, 0-9, - characters)	<input type="text"/>
IP Address	<input type="text" value="192.168.1.100"/>

[Apply Changes](#)

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

IP-адрес будет сопоставлен с именем хоста, а устройство обновлено.

Отображение Host Names Mapping Table (Таблицы отображения имен хостов)

1. Откройте страницу [Host Name Mapping](#) (Отображение имени хоста).
2. Нажмите кнопку **Show All** (Показать все).

Откроется страница [Hosts Name Mapping Table](#) (Таблица отображения имен хостов).

Рис. 6-33. Host Name Mapping Table (Таблица отображения имен хостов)

[Refresh](#)

Host Name	IP Address	Remove Use as: All
1	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="checkbox"/>

[Apply Changes](#)

Удаление имени хоста из таблицы отображения IP-адресов

1. Откройте страницу [Host Name Mapping](#) (Отображение имени хоста).
2. Нажмите кнопку **Show All** (Показать все).

Откроется страница [Hosts Name Mapping Table](#) (Таблица отображения имен хостов).

3. Выберите запись [Host Name Mapping Table](#) (Таблица отображения имен хостов).
4. Установите флажок **Remove** (Удалить).
5. Нажмите кнопку **Apply Changes** (Применить изменения).

Запись таблицы [Host Name Mapping Table](#) (Таблица отображения имен хостов) будет удалена, а устройство обновлено.

Сопоставление IP-адреса с именами хостов домена с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для сопоставления имен хостов домена с IP-адресами.

Таблица 6-22. Команды консоли имен хостов домена

Команда консоли	Описание
	Определяет соответствие статических имен хостов адресам в кэше хоста.

<code>ip host name address</code>	
	Удаляет соответствие имен хостов адресам.
<code>no ip host name</code>	
	Удаляет записи из кэша имя хоста-адрес.
<code>clear host {name *}</code>	
	Удаляет записи из кэша имя хоста-адрес, полученные по протоколу DHCP (Dynamic Host Configuration Protocol).
<code>clear host dhcp {name *}</code>	
	Отображает имя домена по умолчанию, список хостов сервера имен, статические имена и адреса, а также список имен и адресов из кэша.
<code>show hosts [name]</code>	

Далее приведен пример команд консоли.

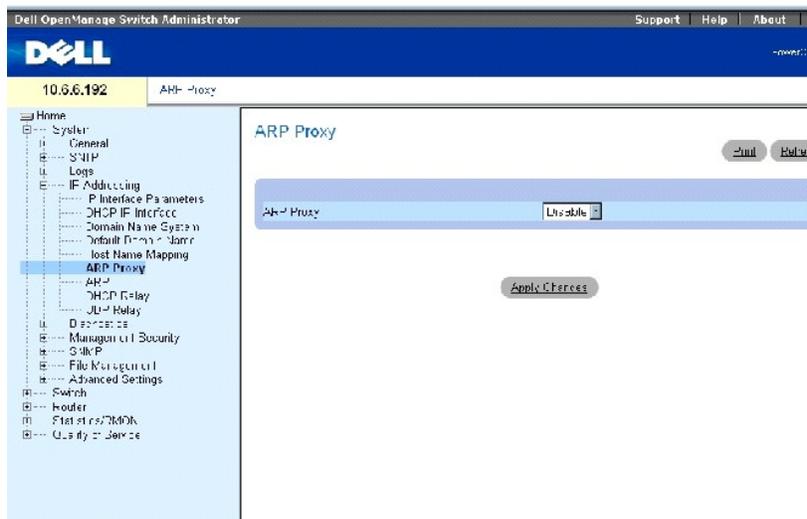
```
console (config)# ip host accounting.abc.com 176.10.23.1
```

Включение прокси-сервера ARP

Протокол разрешения адресов Address Resolution Protocol (ARP) - это протокол TCP/IP для преобразования IP-адресов в физические адреса. Администраторы сети могут включать на коммутаторе прокси-сервер ARP с помощью страницы [ARP Proxy](#) (Прокси-сервер ARP).

Чтобы открыть страницу [ARP Proxy](#) (Прокси сервер ARP), выберите **System** (Система) → **IP Addressing** (IP-адресация) → **ARP Proxy** (Прокси-сервер ARP) на панели.

Рис. 6-34. Прокси-сервер ARP



Поле **ARP Proxy** (Прокси-сервер ARP) позволяет устройству распознавать запросы ARP локальных узлов. Если этот параметр отключен, устройство отвечает и передает свой собственный MAC-адрес.

Включение ARP

1. Откройте страницу [ARP Proxy](#) (Прокси-сервер ARP).
2. Выберите значение **Enabled** (Включено) в поле **ARP Proxy** (Прокси-сервер ARP).

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

Функция прокси-сервера ARP будет включена на устройстве.

Включение прокси-сервера ARP с помощью команд консоли

В следующей таблице приведены команды консоли для включения прокси-сервера ARP.

Таблица 6-23. Команды консоли для прокси-сервера ARP

Команда консоли	Описание
<code>ip proxy-arp</code>	Включает прокси-сервер ARP
<code>no ip proxy-arp</code>	Отключает прокси-сервер ARP

Далее приведен пример команд консоли.

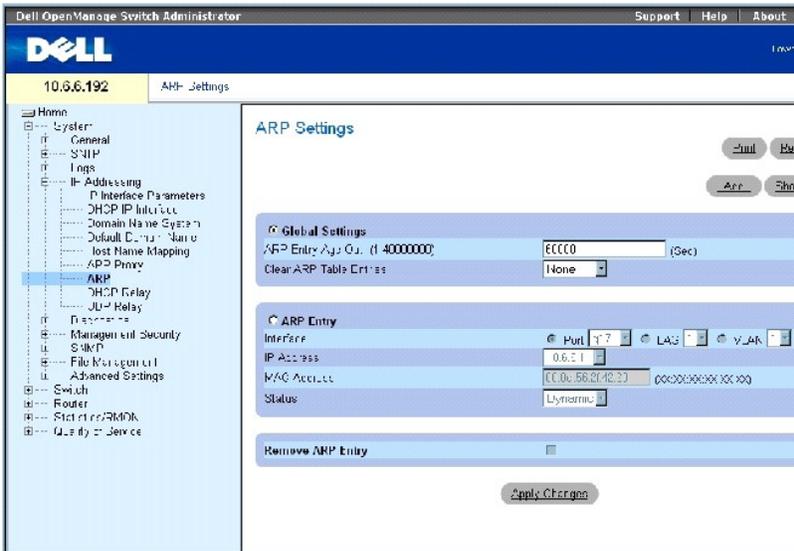
```
Console (config)# ip proxy-arp
```

Определение параметров ARP

Для определения параметров ARP для IP-интерфейса используется страница [ARP Settings](#) (Параметры ARP). Таблица ARP используется для отслеживания взаимосвязи между MAC-адресом и соответствующим ему IP-адресом. Пользователь может добавить статические записи в таблицу ARP. При определении статической записи ARP в таблицу помещается постоянная запись, которую система использует для перевода IP-адресов в MAC-адреса.

Чтобы открыть страницу [ARP Settings](#) (Параметры ARP), выберите **System** (Система) → **IP Addressing** (IP-адресация) → **ARP** на панели дерева.

Рис. 6-35. Страница ARP Settings (Параметры ARP)



Страница [ARP Settings](#) (Параметры ARP) содержит следующие поля.

Global Settings (Общие параметры) - выберите этот параметр для активизации полей общих параметров ARP.

ARP Entry Age Out (0- 40000000) (Срок хранения записи ARP) - время (в секундах) для всех устройств, которое проходит между запросами ARP по записям таблицы ARP. По истечении этого периода запись удаляется из таблицы. Диапазон значений: 0 - 4000000, ноль указывает, что запись никогда не удаляется из кэша.

Clear ARP Table Entries (Удалить записи таблицы ARP) - тип записей ARP, которые удаляются на всех устройствах. Возможные значения:

None (Нет) - записи ARP не удаляются.

All (Все) - все записи ARP удаляются.

Dynamic (Динамические) - удаляются только динамические записи ARP.

Static (Статические) - удаляются только статические записи ARP.

ARP Entry (Запись ARP) - выберите этот параметр, чтобы активизировать поля параметров ARP для одного устройства.

Interface (Интерфейс) - номер интерфейса порта, группы LAG или VLAN, которые подключены к устройству.

IP Address (IP-адрес) - IP-адрес станции, который связан с MAC-адресом, указанным ниже.

MAC Address (MAC-адрес) - MAC-адрес станции, который связан в таблице ARP с IP-адресом.

Status (Состояние) - состояние записи таблицы ARP. Возможные значения этого поля:

Other (Другая) - запись ARP не является ни динамически распознаваемой, ни статической записью.

Invalid (Недопустимая) - запись ARP недопустима.

Dynamic (Динамическая) - запись ARP была распознана динамически.

Static (Статическая) - запись ARP статическая.

Remove ARP Entry (Удалить запись ARP) - когда установлен этот флажок, запись ARP удаляется.

Добавление записи в таблицу ARP

1. Откройте страницу [ARP Settings](#) (Параметры ARP).
2. Нажмите кнопку **Add** (Добавить), чтобы отобразить страницу **Add ARP Entry** (Добавление записи ARP).

Рис. 6-36. Страница Add ARP Entry (Добавление записи ARP)

Add ARP Entry Назад

Interface	<input type="text" value="Port 3"/>	<input type="text" value="LAG 1"/>	<input type="text" value="VLAN 2"/>
IP Address	<input type="text" value="1.1.1.1"/>	<input type="text" value="XXXX"/>	
MAC Address	<input type="text" value="00:00:00:00:00:00"/>	<input type="text" value="XXXX"/>	

Apply Changes

3. Выберите интерфейс и введите значения в полях на странице.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Статическая запись таблицы ARP будет добавлена, а устройство обновлено.

Изменение записи в таблице ARP

1. Откройте страницу [ARP Settings](#) (Параметры ARP).
2. Выберите запись таблицы.
3. Измените необходимые поля для данного интерфейса.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Статическая запись таблицы ARP будет изменена, а устройство обновлено.

Удаление записи таблицы ARP

1. Откройте страницу [ARP Settings](#) (Параметры ARP).
2. Нажмите кнопку **Show All** (Показать все), чтобы отобразить страницу **ARP Table** (Таблица ARP).
3. Выберите запись таблицы.
4. Установите флажок **Remove** (Удалить).
5. Нажмите кнопку **Apply Changes** (Применить изменения).

Запись таблицы будет удалена, а устройство обновлено.

Настройка ARP с помощью команд консоли

В следующей таблице приведены команды консоли для настройки прокси-сервера ARP.

Таблица 6-24. Команды консоли для настройки ARP

Команда консоли	Описание
<code>arp ip_адрес аппаратный_адрес {ethernet interface- number vlan идентификатор_vlan port-channel number out-of-band-eth oob- interface}</code>	Добавляет постоянную запись в
<code>arp timeout</code>	Настраивает срок хранения запи
<code>show arp</code>	Отображает записи в таблице А

Далее приведен пример команд консоли.

```
Console (config)# arp timeout 5
```

```
Console (config)# arp 10.1.1.1 0060.704C.73FF ethernet g5
```

```
Console# show arp
```

```
Interface IP Address HW Address Status
```

```
-----
```

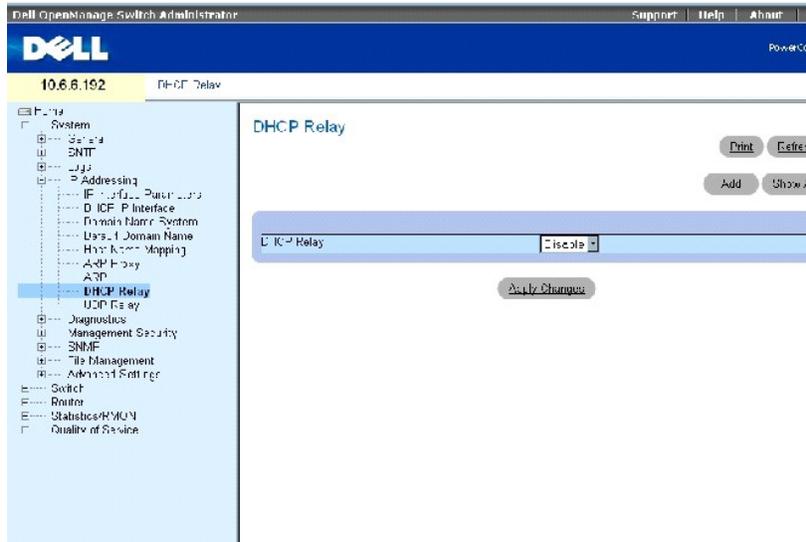
```
g20 10.1.1.1 0060.704c.73ff dynamic
```

Определение параметров ретрансляции DHCP

Для определения данных для настройки конфигурации DHCP с несколькими серверами DHCP и обеспечения избыточности используйте страницу [DHCP Relay](#) (Ретрансляция DHCP). Управление и распределение IP-адресов осуществляется последовательно для предотвращения перегрузки устройства.

Чтобы открыть страницу [DHCP Relay](#) (Ретрансляция DHCP), выберите **System** (Система) → **IP Addressing** (IP-адресация) → **DHCP Relay** (Ретрансляция DHCP) на панели дерева.

Рис. 6-37. DHCP Relay (Ретрансляция DHCP)



Включение ретрансляции DHCP

1. Откройте страницу [DHCP Relay](#) (Ретрансляция DHCP).
2. Выберите **Enable** (Включить) в раскрывающемся меню **DHCP Relay** (Ретрансляция DHCP).
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Запись DHCP Relay (Ретрансляция DHCP) будет добавлена в таблицу DHCP Relay Table (Таблица ретрансляции DHCP).

Добавление записи ретрансляции DHCP

1. Откройте страницу [DHCP Relay](#) (Ретрансляция DHCP).
2. Нажмите кнопку **Add** (Добавить), чтобы отобразить страницу **Add DHCP Server** (Добавление сервера DHCP).
3. Введите **значение** в поле **New DHCP Server** (Новый сервер DHCP).

Серверы DHCP выполняются ретрансляция DHCP в том случае, если этот параметр не равен 0.0.0.0. Ретрансляция запросов DHCP выполняется в том случае, если значение в их поле SEC больше или равно пороговому значению. Благодаря этому сначала отвечают локальные серверы DHCP.

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

Сервер DHCP будет добавлен в таблицу ретрансляции DHCP.

Удаление записи в таблице ретрансляции DHCP

1. Откройте страницу [DHCP Relay](#) (Ретрансляция DHCP).
2. Нажмите кнопку **Show All** (Показать все), чтобы открыть страницу **DHCP Servers Table** (Таблица серверов DHCP).
3. Выберите **DHCP Server** (Сервер DHCP) и установите флажок **Remove** (Удалить).
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Запись будет удалена, а устройство обновлено.

Определение серверов ретрансляции DHCP с помощью команд консоли

В следующей таблице приведены команды консоли для определения серверов ретрансляции DHCP.

Таблица 6-25. Команды консоли для серверов ретрансляции DHCP

Команда консоли	Описание
ip dhcp relay enable	Включает функции ретрансляции Dynamic Host Configuration Protocol (DHCP) на маршрутизаторе.
ip dhcp relay address ip_адрес	Делает серверы DHCP доступными для ретрансляции DHCP.

Далее приведен пример команд консоли для включения службы ретрансляции DHCP:

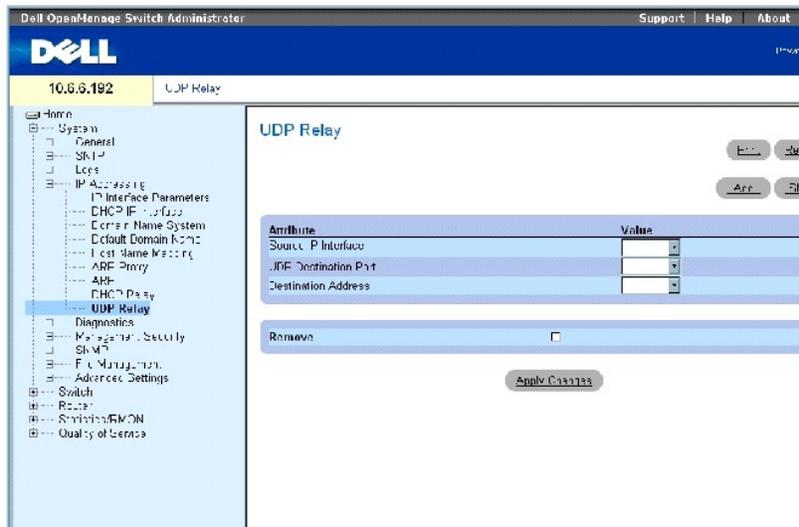
```
Console (config)# ip dhcp relay enable
```

Настройка ретрансляции UDP

Ретрансляция UDP обеспечивает передачу пакетов UDP в другие сети. Эта функция позволяет выполнять просмотр с рабочих станций данных на серверах в других сетях.

Чтобы открыть страницу [UDP Relay](#) (Ретрансляция UDP), выберите **System** (Система) → **IP Addressing** (IP-адресация) → **UDP Relay** (Ретрансляция UDP) на панели дерева.

Рис. 6-38. UDP Relay (Ретрансляция UDP)



Страница [UDP Relay](#) (Ретрансляция UDP) содержит следующие поля.

Source IP Interface (IP-адрес источника) - IP-интерфейс источника, ретранслирующего пакеты UDP. Если в этом поле указан адрес 255.255.255.255, то выполняется ретрансляция пакетов UDP со всех интерфейсов. Следующие диапазоны адресов являются недопустимыми:

с 0.0.0.0 по 0.255.255.255.

с 127.0.0.0 по 127.255.255.255.

UDP Destination Port (1-65535) (UDP порт назначения) - идентификационный номер порта назначения UDP для ретрансляции пакетов UDP. В следующей таблице представлен список выделенных портов UDP.

Таблица 6-26. Выделенные порты UDP

Номер порта UDP	Сокращение	Применение
7	Echo	Echo
11	SysStat	Активный пользователь
15	NetStat	Netstat
17	Цитата	Цитата дня
19	CHARGEN	Генератор символов
20	FTP-data	Данные FTP
21	FTP	FTP
37	Время	Время
42	NAMESERVER	Сервер имен хоста
43	NICNAME	Who is
53	DOMAIN	Сервер DNS
69	TFTP	Trivial File Transfer
111	SUNRPC	Sun Microsystems Rpc
123	NTP	Network Time
137	NetBiosNameService	Подключения сервера NT к станции
138	NetBiosDatagramService	Подключения сервера NT к станции
139	NetBios	SessionService Подключения сервера NT к станции
161	SNMP	Simple Network Management
162	SNMP-trap	Прерывания Simple Network Management
513	who	Демон Unix Rwho
514	syslog	Системный журнал
525	timed	Демон времени

Destination Address (Адрес назначения) - IP-интерфейс, получающий ретранслируемые пакеты UDP. Если в этом поле указан адрес 0.0.0.0, то пакеты UDP отбрасываются. Если в этом поле указан адрес 255.255.255.255, то пакеты UDP передаются на все IP-интерфейсы.

Добавление записи ретрансляции UDP

1. Откройте страницу [UDP Relay](#) (Ретрансляция UDP).
2. Нажмите кнопку **Add** (Добавить), чтобы отобразить страницу **Add UDP Relay** (Добавление ретрансляции UDP).
3. Введите IP-адрес сервера UDP в поле **UDP Destination Port** (Порт назначения UDP).
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Сервер DHCP будет добавлен в таблицу ретрансляции DHCP.

Удаление записи в таблице ретрансляции UDP

 **ПРИМЕЧАНИЕ.** Если ретрансляция UDP включена, но не указан номер порта UDP, устройство по умолчанию пересылает пакеты широковещательной рассылки UDP следующим службам: IEN-116 Name Service (порт 42), DNS (порт 53), NetBIOS Name Server (порт 137), NetBIOS Datagram Server (порт 138), TACACS Server (порт 49) и Time Service (порт 37).

1. Откройте страницу [UDP Relay](#) (Ретрансляция UDP).
2. Определите поля.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Запись UDP будет добавлена в **UDP Relay Table** (Таблица ретрансляции UDP), а устройство обновлено.

Удаление записи в таблице ретрансляции UDP

1. Откройте страницу [UDP Relay](#) (Ретрансляция UDP).
2. Нажмите кнопку **Show All** (Показать все), чтобы отобразить страницу **UDP Relay Table** (Таблица ретрансляции UDP).
3. Выберите сервер ретрансляции UDP и установите флажок **Remove** (Удалить).
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Запись будет удалена, а устройство обновлено.

Настройка таблицы ретрансляции UDP с помощью команд консоли

В следующей таблице приведены команды консоли для настройки ретрансляции UDP.

Таблица 6-27. Команды консоли для настройки ретрансляции UDP

Команда консоли	Описание
<code>helper-address адрес [список_портов_udp]</code>	Включает пересылку широковещательной рассылки UDP (User Datagram Protocol), получаемой Эта команда не разрешает пересылку пакетов по протоколам BOOTP/DHCP. Для пересылки пакетов BOOTP/DHCP используйте команды ретрансляции <code>ip dhcp relay enable</code> , <code>ip dhcp relay address</code> и <code>ip dhcp relay server</code> . Дополнительную информацию об этих командах см. в разделе « Определение параметров ретрансляции ».

Далее приведен пример команды консоли:

```
Console (config-ip)# helper-address 172.16.9.9 49 53
```

Запуск диагностики кабелей

Страница **Diagnostics** (Диагностика) используется для виртуального тестирования медных и оптических кабелей.

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

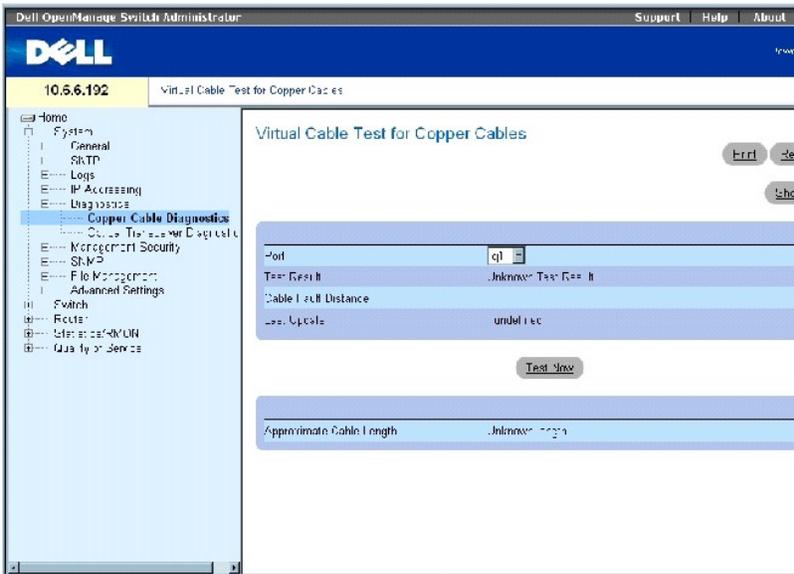
На странице **Diagnostics** (Диагностика) находятся ссылки на страницы для тестирования медных и оптических трансиверов.

Просмотр диагностики медных кабелей

Страница [Virtual Cable Test for Copper Cables](#) (Виртуальное тестирование медных кабелей) используется для тестирования медных кабелей. В ходе тестирования кабеля отображается информация о неисправностях кабеля, времени выполнения последнего теста кабеля и типе неисправности кабеля. В тестах используется технология TDR (Time Domain Reflectometry) для проверки качества и характеристик медного кабеля, подключенного к порту. Можно тестировать кабели длиной до 120 метров. Проверка кабелей выполняется при отключенных портах. Исключение составляет тест примерной длины кабеля (Approximated Cable Length).

Чтобы открыть страницу [Virtual Cable Test for Copper Cables](#) (Виртуальное тестирование медных кабелей), выберите **System** (Система) → **Diagnostics** (Диагностика) → **Copper Cable Diagnostics** (Диагностика медного кабеля) на панели дерева.

Рис. 6-39. Virtual Cable Test for Copper Cables (Виртуальное тестирование медных кабелей)



Страница [Virtual Cable Test for Copper Cables](#) (Виртуальное тестирование медных кабелей) содержит следующие поля.

Port (Порт) - порт, к которому подключен кабель.

Test Result (Результат теста) - результаты теста кабеля. Возможные значения:

No Cable (Нет кабеля) - кабель не подключен к порту.

Open Cable (Оборванный кабель) - кабель оборван.

Short Cable (Короткозамкнутый кабель) - короткое замыкание в кабеле.

OK - кабель прошел тестирование.

Fiber Cable (Оптоволоконный кабель) - к порту подключен оптоволоконный кабель.

Cable Fault Distance (Расстояние до повреждения) - расстояние от порта до точки повреждения кабеля.

Last Update (Последнее обновление) - время последнего тестирования порта.

Approximate Cable Length (Примерная длина кабеля) - примерная длина кабеля. Тест можно выполнить, если порт включен и работает на скорости 1 Гбит/с.

Выполнение теста кабеля

1. Убедитесь, что оба конца медного кабеля подключены к устройству.
2. Откройте страницу [Virtual Cable Test for Copper Cables](#) (Виртуальное тестирование медных кабелей).
3. Нажмите кнопку **Test Now** (Тестировать).

Будет выполнен тест медного кабеля и результаты отображены на странице [Virtual Cable Test for Copper Cables](#) (Виртуальное тестирование медных кабелей).

Отображение таблицы результатов виртуального тестирования кабелей

1. Откройте страницу [Virtual Cable Test for Copper Cables](#) (Виртуальное тестирование медных кабелей).
2. Нажмите кнопку **Show All** (Показать все), чтобы отобразить страницу **Virtual Cable Test Results Table** (Таблица результатов виртуального тестирования кабелей).

Выполнение тестирования медных кабелей с помощью команд консоли

В следующей таблице приведены команды консоли для выполнения тестирования медных кабелей.

Таблица 6-28. Команды консоли для выполнения тестирования медных кабелей

Команда консоли	Описание
<code>test copper-port tdr интерфейс</code>	Выполняет виртуальное тестирование кабеля.
<code>show copper-port tdr интерфейс</code>	Отображает результаты последнего виртуального тестирования кабеля для порта.
<code>show copper-port cable-length интерфейс</code>	Отображает предположительную длину кабеля, подключенного к порту.

Далее приведен пример команд консоли.

```
Console# show copper-ports cable-length
```

```
Port Length [метры]
```

```
-----
```

```
g1 < 50
```

```
g2 Copper not active
```

```
g3 110-140
```

```
g4 Fiber
```

ПРИМЕЧАНИЕ. Длина кабеля, возвращаемая процедурой виртуального тестирования, аппроксимируется до следующих величин: до 50 метров, от 50 до 80 метров, от 80 до 110 метров, от 110 до 120 метров или более 120 метров. Отклонение может составлять до 20 метров, и измерение длины кабеля невозможно для каналов связи со скоростью 10 Мбит/с.

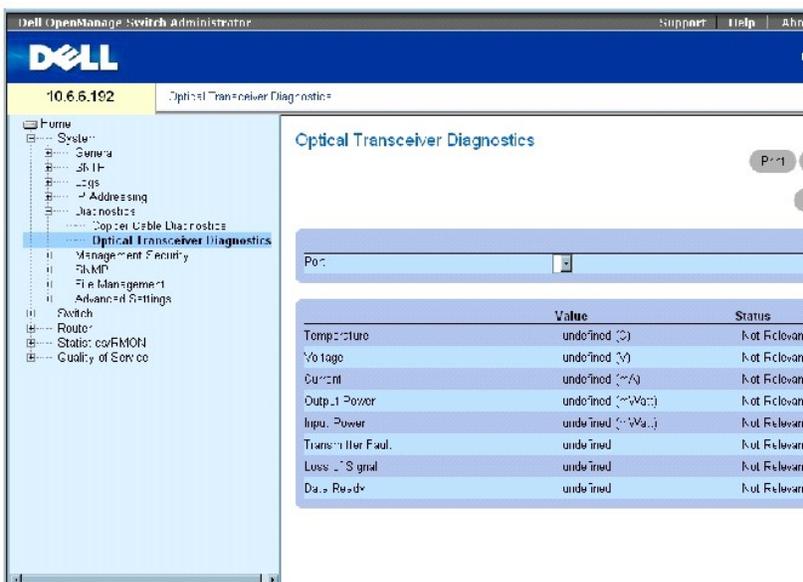
Просмотр диагностики оптического трансивера

С помощью страницы [Optical Transceiver Diagnostics](#) (Диагностика оптоволоконного трансивера) можно выполнить тестирование оптоволоконных кабелей.

Чтобы открыть страницу [Optical Transceiver Diagnostics](#) (Диагностика оптического трансивера), выберите System (Система)→ Diagnostics (Диагностика)→ Optical Transceiver Diagnostics (Диагностика оптического трансивера) на панели дерева.

ПРИМЕЧАНИЕ. Диагностика оптического трансивера может быть выполнена только в том случае, если установлено соединение.

Рис. 6-40. Optical Transceiver Diagnostics (Диагностика оптического трансивера)



Страница [Optical Transceiver Diagnostics](#) (Диагностика оптического трансивера) содержит следующие поля.

Port (Порт) - IP-адрес порта, кабель которого тестируется.

Temperature (Температура) - рабочая температура (C) кабеля.

Voltage (Напряжение) - рабочее напряжение кабеля.

Current (Ток) - рабочий ток кабеля.

Output Power (Выходная мощность) - значение выходной мощности.

Input Power (Входная мощность) - значение входной мощности.

Transmitter Fault (Сбой передатчика) - указывает, что произошла ошибка во время передачи.

Loss of Signal (Потеря сигнала) - указывает, возникла ли потеря сигнала.

Data Ready (Готовность к передаче данных) - показывает, что на трансивер подается питание и он готов к передаче данных.

Отображение таблицы тестов диагностики оптического трансивера

1. Откройте страницу [Optical Transceiver Diagnostics](#) (Диагностика оптического трансивера).
2. Нажмите кнопку **Show All** (Показать все), чтобы открыть страницу **Virtual Cable Test Results Table** (Таблица результатов виртуального тестирования кабелей).

Выполнение тестирования оптоволоконных кабелей с помощью команд консоли

В следующей таблице приведены команды консоли для выполнения тестирования оптических кабелей.

Таблица 6-29. Команды консоли для выполнения тестирования оптоволоконных кабелей

Команда консоли	Описание
<code>show fiber-ports optical- transceiver [интерфейс][detailed]</code>	Отображает данные диагностики оптического трансивера.

Далее приведен пример команды консоли:

```
console# show fiber-ports optical-transceiver
```

На экране появляются следующие столбцы:

- 1 **Temp** (Температура) - измеренная внутренняя температура трансивера
- 1 **Voltage** (Напряжение) - измеренное внутреннее напряжение питания
- 1 **Current** (Ток) - измеренное отклонение тока TX
- 1 **Output Power** (Выходная мощность) - измеренная выходная мощность передачи (TX) в милливаттах
- 1 **Input Power** (Входная мощность) - измеренная входная мощность приема (RX) в милливаттах
- 1 **TX Fault** (Сбой передатчика) - сбой передатчика

 **ПРИМЕЧАНИЕ.** Трансиверы Finisar не поддерживают диагностическую проверку неисправности.

- 1 **LOS** - потеря сигнала
- 1 **Data Ready** (Готовность к передаче данных) - показывает, что на трансивер подается питание и он готов к передаче данных
- 1 **N/A** - недоступно, **N/S** - не поддерживается, **W** - предупреждение, **E** - ошибка

 **ПРИМЕЧАНИЕ.** Функция анализа оптоволоконной сети работает только на трансиверах SFP, которые поддерживают стандарт диагностики SFF-4872.

Управление безопасностью устройств

Страница **Management Security** (Безопасность управления) предоставляет возможность управлять параметрами безопасности для порта, пользователя и безопасности сервера.

Чтобы открыть страницу **Management Security** (Безопасность управления), выберите **System** (Система)→ **Management Security** (Безопасность управления) на панели дерева.

Defining Access Profiles (Определение профилей доступа)

Страница **Access Profiles** (Профили доступа) позволяет определять профили и правила для доступа к устройству. Можно ограничить доступ к функциям управления группам пользователей, которые определены входящими интерфейсами и исходными IP-адресами или маской исходной подсети.

Доступ к управлению может быть отдельно определен для каждого метода доступа к управлению, включая Web (HTTP), безопасный web (HTTPS), Telnet, безопасный Telnet и SNMP.

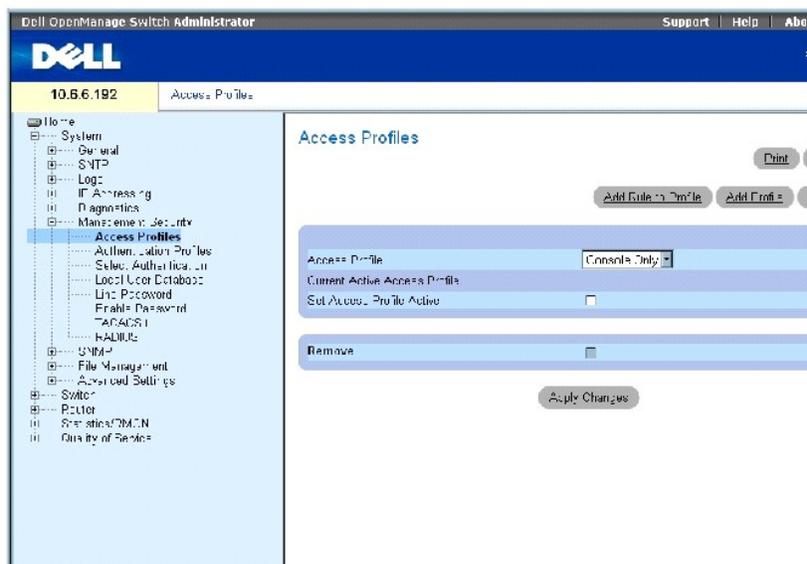
Доступ к различным методам управления может быть различным для разных групп пользователей. Например, «Группа пользователей 1» может получать доступ к устройству только через сеанс HTTP, а «Группа пользователей 2» может получать доступ к устройству через сеансы HTTP и Telnet.

Management Access Lists (Списки управления доступом) содержат привила, определяющие, как и каким способом, пользователь может управлять устройством. Пользователям может быть запрещен доступ к устройству.

Страница **Access Profiles** (Профили доступа) позволяет настроить списки управления и назначить их для определенных интерфейсов.

Чтобы открыть страницу **Access Profiles** (Профили доступа), выберите **System** (Система)→ **Management Security** (Безопасность управления)→ **Access Profiles** (Профили доступа) на панели дерева.

Рис. 6-41. Страница Access Profiles (Профили доступа)



Access Profile (Профиль доступа) - содержит список профилей доступа. Значение для списка по умолчанию - **Console Only** (Только консоль), к нему добавляются профили доступа, определенные пользователем. Если выбрать **Console Only** (Только консоль) в качестве имени **Access Profile** (Профиля доступа), сеанс будет прерван, а затем разрешен доступ к устройству только с консоли.

Current Active Access Profile (Текущий активный профиль доступа) - активный в настоящий момент профиль доступа.

Set Access Profile Active (Сделать профиль доступа активным) - активизирует профиль доступа.

Remove (Удалить) - когда установлен этот флажок, профиль доступа удаляется из списка Access Profile Name (Имя профилей доступа).

Добавление профиля доступа

1. Откройте страницу [Access Profiles](#) (Профили доступа).
2. Нажмите кнопку Add Profile (Добавить профиль), чтобы отобразить страницу [Add an Access Profile](#) (Добавление профиля доступа).

Рис. 6-42. Add an Access Profile (Добавление профиля доступа)

The screenshot shows the 'Add an Access Profile' configuration page. At the top right is a 'Cancel' button. Below it is a text input field for 'Access Profile Name (1-32 Characters)'. The main configuration area includes: 'Rule Priority (1-255)' dropdown menu; 'Management Method' dropdown menu set to 'All'; 'Interface' section with a checkbox for 'Interface' and sub-options for 'Ethernet' (with 'Port' and 'LAG' checkboxes) and 'VLAN'; 'Source IP Address' section with checkboxes for 'Source IP Address' and 'Network Mask', and a 'Prefix Length' input field; and an 'Action' dropdown menu set to 'Permit'. At the bottom center is an 'Apply Changes' button.

Страница [Add an Access Profile](#) (Добавление профиля доступа) содержит следующие поля.

Access Profile Name (Имя профиля доступа) - определенное пользователем имя профиля доступа.

Rule Priority (Приоритет правила) - показывает приоритет правила. Если пакет соответствует правилу, группам пользователей либо предоставляет, либо запрещается доступ для управления устройством. Порядок правила задается путем определения номера правила в таблице Profile Rules (Правила профиля). Номер правила является важным для сопоставления пакетов правилам, поскольку сопоставление пакетов выполняется на основе схемы первого совпадения. Приоритеты правил назначаются в таблице Profile Rules Table (Таблица правил профиля).

Management Method (Метод управления) - метод управления, для которого определен профиль доступа. Пользователи с таким профилем доступа могут осуществлять доступ к устройству, используя выбранный метод управления.

Interface (Интерфейс) - тип интерфейса, к которому относится правило. Это необязательное поле. Можно назначить это правило для выбранного порта, группы LAG или VLAN, установив флажок и выбрав соответствующий параметр и интерфейс.

ПРИМЕЧАНИЕ. Назначение интерфейсу профиля доступа означает, что в доступе через другие интерфейсы отказано. Если профиль доступа не назначен ни для одного интерфейса, устройство будет доступно для всех.

Source IP Address (IP-адрес источника) - исходный IP-адрес интерфейса, для которого применяется правило. Это дополнительное поле, показывающее, что правило действительно для этой подсети.

Network Mask (Маска сети) - маска подсети IP-адреса.

Prefix Length (Длина префикса) - число бит, образующих префикс исходного IP-адреса, или сетевая маска исходного IP-адреса.

Action (Действие) - определяет, разрешен или запрещен доступ для управления для определенного интерфейса.

3. Введите имя профиля в текстовом поле Access Profile Name (Имя профиля доступа).
4. Введите в полях значения и нажмите кнопку Apply Changes (Применить изменения).

Новый профиль доступа будет добавлен, а устройство обновлено.

Активизация профиля доступа

1. Откройте страницу [Access Profiles](#) (Профили доступа).
2. Выберите в списке профиль доступа.
3. Установите флажок **Set Access Profile Active** (Активизировать профиль доступа).
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Профиль доступа включен для пользователя.

Добавление правил для профиля доступа

1. Откройте страницу [Access Profiles](#) (Профили доступа).
2. Выберите **Access Profile** (Профиль доступа) в раскрывающемся меню.

Это профиль, в который будут добавлены правила при открытии страницы [Add an Access Profile Rule](#) (Добавление правила профиля доступа).

3. Нажмите кнопку **Add Rule to Profile** (Добавить правило для профиля), чтобы отобразить страницу [Add an Access Profile Rule](#) (Добавление правила профиля доступа).

Рис. 6-43. Add An Access Profile Rule (Добавление правила профиля доступа)

Back

Access Profile Name Console Only

Priority (0-9999)

Management Method

Interface Port LAG VLAN

Source Address Network Mask Prefix Length

Action Permit

Apply Changes

4. Введите значения в полях диалогового окна и нажмите кнопку **Apply Changes** (Применить изменения).

Правило будет добавлено в профиль доступа, а устройство обновлено.

Удаление правила

1. Откройте страницу [Access Profiles](#) (Профили доступа).
2. Нажмите кнопку **Show All** (Показать все), чтобы отобразить страницу **Profile Rules Table** (Таблица правил профиля).
3. Выберите правило.
4. Установите флажок **Remove** (Удалить) и нажмите кнопку **Apply Changes** (Применить изменения).

Правило будет удалено, а устройство обновлено.

Определение профилей доступа с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для настройки профилей доступа.

Таблица 6-30. Команды консоли для профилей доступа

Команда консоли	Описание
<code>management access-list имя</code> ПРИМЕЧАНИЕ: <i>И м е н а</i> , содержащие пробелы, следует заключать в двойные кавычки. Например, «workgroup 1»	Определяет список доступа для управления и вводит контекст списка доступа для конфигурации.
<code>permit [ethernet номер_интерфейса vlan идентификатор_vlan port- channel номер] [service служба]</code>	Задаёт разрешающие условия для списка доступа к управлению для порта.
<code>permit ip-source ip_адрес [mask маска длина_префикса] [ethernet номер_интерфейса vlan идентификатор_vlan port- channel номер] [service служба]</code>	Задаёт для порта разрешающие условия списка доступа для управления и выбранный метод управления.
<code>deny [ethernet номер_интерфейса vlan идентификатор_vlan port- channel номер] [service служба]</code>	Задаёт для порта запрещающие условия списка доступа для управления и выбранный метод управления.
<code>deny ip-source ip_адрес [mask маска длина-префикса] [ethernet номер-интерфейса vlan идентификатор_vlan port-channel номер] [service служба]</code>	Задаёт для порта запрещающие условия списка доступа к управлению и выбранный метод управления.
<code>management access-class {console-only имя}</code>	Определяет, какой список доступа используются в качестве активных соединений для управления.
<code>show management access-list [имя]</code>	Отображает активные списки доступа для управления.
<code>show management access-class</code>	Отображает информацию о классе доступа для управления.

Далее приведен пример команд консоли.

```
Console (config)# management access-list mlist
```

```
Console (config-macl)# permit ethernet g1
```

```
Console (config-macl)# permit ethernet g9
```

```
Console (config-macl)# exit
```

```
Console# show management access-class
```

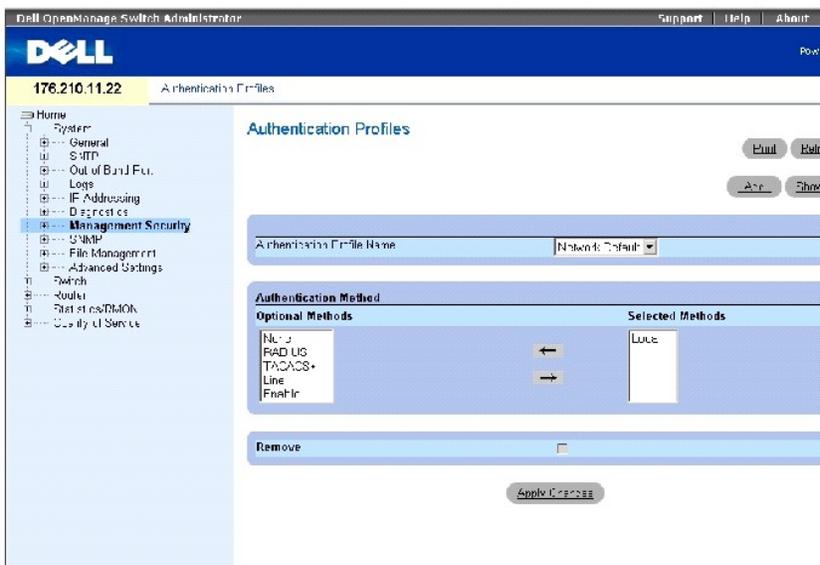
Класс доступа к управлению включен с использованием списка доступа mlist

Определение профилей проверки подлинности

Проверка подлинности пользователей выполняется локально и на внешнем сервере. С помощью страницы [Authentication Profiles](#) (Профили проверки подлинности) можно выбирать метод проверки подлинности пользователя на устройстве.

Чтобы открыть страницу [Authentication Profiles](#) (Профили проверки подлинности), выберите System (Система)→ Management Security (Безопасность управления)→ Authentication Profiles (Профили проверки подлинности) на панели дерева.

Рис. 6-44. Страница Authentication Profiles (Профили проверки подлинности)



Страница [Authentication Profiles](#) (Проверка подлинности профилей) содержит следующие поля.

Authentication Profile Name (Имя профиля проверки подлинности) - списки определяемых пользователем профилей проверки подлинности, в которые добавляются определяемые пользователем профили проверки подлинности. По умолчанию используются **Network Default** (По умолчанию для сети) и **Console Default** (По умолчанию для консоли).

Optional Methods (Дополнительные методы) - определяемые пользователем методы проверки подлинности. Возможные значения:

None (Нет) - проверка подлинности пользователя не выполняется.

Local (Локально) - проверка подлинности пользователя выполняется на уровне устройства; для проверки подлинности устройство проверяет имя пользователя и пароль.

RADIUS - проверка подлинности выполняется на сервере RADIUS. Дополнительную информацию о серверах RADIUS см. в разделе «[Настройка параметров RADIUS](#)».

TACACS+ - проверка подлинности пользователя проверяется на сервере TACACS+. Дополнительную информацию о серверах TACACS+ см. в разделе «[Настройка параметров TACACS+](#)».

Line (Канал) - для проверки подлинности пользователя используется пароль канала связи.

Enable (Включение) - для проверки подлинности используется пароль включения.

ПРИМЕЧАНИЕ. Проверка подлинности пользователя происходит в том порядке, в каком выбраны методы. Если при проверке подлинности происходит ошибка, используется следующий выбранный метод. Например, если выбраны сразу и параметр **Local** (Локально), и параметр **RADIUS**, проверка подлинности пользователя сначала выполняется локально, а затем на внешнем сервере.

Selected Methods (Выбранные методы) - выбранный метод проверки подлинности.

Добавление профиля проверки подлинности

1. Откройте страницу **Authentication Profiles** (Профили проверки подлинности).
2. Нажмите кнопку **Add** (Добавить), чтобы отобразить страницу **Add Authentication Profile** (Добавление профиля проверки подлинности).
3. Введите имя профиля из 1-12 символов в поле **Profile Name** (Имя профиля).

 **ПРИМЕЧАНИЕ.** Имя профиля не должно содержать пробелы.

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

Сеансам будет назначен профиль проверки подлинности.

Выбор метода проверки подлинности

1. Откройте страницу [Authentication Profiles](#) (Профили проверки подлинности).
2. Выберите элемент из списка в поле **Authentication Profile Name** (Имя профиля проверки подлинности).
3. С помощью клавиш со стрелками выберите значение в поле **Optional Methods** (Дополнительные методы).
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Профиль проверки подлинности для этого устройства будет изменен.

Удаление записи профиля проверки подлинности

1. Откройте страницу [Authentication Profiles](#) (Профили проверки подлинности).
2. Нажмите кнопку **Show All** (Показать все).

Откроется **Authentication Profile Table** (Таблица профилей проверки подлинности).

3. Установите флажок **Remove** (Удалить) рядом с профилем, который необходимо удалить.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Запись будет удалена.

Настройка профиля проверки подлинности с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для определения профилей проверки подлинности.

Таблица 6-31. Команды консоли для профилей проверки подлинности

Команда консоли	Описание
<code>aaa authentication login {default имя_списка} метод1 [метод2...]</code>	Настраивает проверку подлинности при входе в систему.
<code>no aaa authentication login {default имя_списка}</code>	Удаляет профиль проверки подлинности при входе в систему.
<code>show authentication methods</code>	Отображает информацию о методах проверки подлинности.

Далее приведен пример команд консоли.

```
Console (config)# aaa authentication login default radius local enable none
```

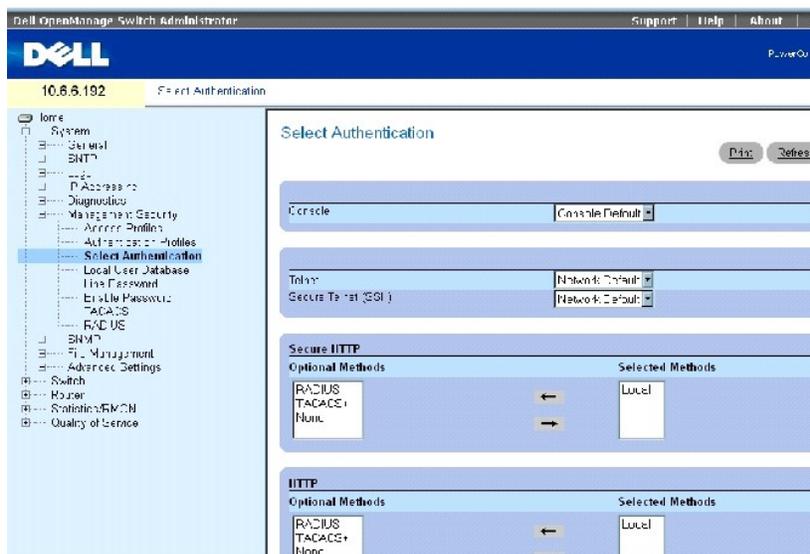
```
configConsole (config)# no aaa authentication login default
```

Выбор профиля проверки подлинности

После того как профили проверки подлинности определены, их можно применять к методам доступа для управления. Например, проверка подлинности пользователей консоли может выполняться по списку профилей проверки подлинности 1, в то время как проверка подлинности пользователей Telnet выполняется по списку методов проверки подлинности 2.

Чтобы открыть страницу [Select Authentication](#) (Выбор проверки подлинности), выберите System (Система)→ Management Security (Безопасность управления)→ Select Authentication (Выбор проверки подлинности) на панели дерева.

Рис. 6-45. Страница Select Authentication (Выбор проверки подлинности)



Страница [Select Authentication](#) (Выбор проверки подлинности) содержит следующие поля.

Console (Консоль) - профили проверки подлинности, используемые для проверки подлинности пользователей консоли.

Telnet - профили проверки подлинности, используемые для проверки подлинности пользователей Telnet.

Secure Telnet (SSH) - профили проверки подлинности, используемые для проверки подлинности пользователей Secure Shell (SSH). Протокол SSH предоставляет клиентам безопасные и зашифрованные удаленные соединения с устройством.

HTTP и Secure HTTP - метод проверки подлинности, используемый для доступа к HTTP и Secure HTTP соответственно. Возможные значения этого поля:

None (Нет) - не используется никакой метод проверки подлинности пользователя для доступа.

Local (Локально) - проверка подлинности выполняется локально.

RADIUS - проверка подлинности выполняется на сервере RADIUS.

TACACS+ - проверка подлинности выполняется на сервере TACACS+.

Local, None (Локально, Нет) - проверка подлинности сначала выполняется локально. Если невозможно выполнить проверку подлинности, то не используется никакой метод проверки подлинности.

RADIUS, None (RADIUS, Нет) - проверка подлинности сначала выполняется на сервере RADIUS. Если невозможно выполнить проверку подлинности, то не используется никакой метод проверки подлинности.

TACACS+, None (TACACS+, Нет) - проверка подлинности сначала выполняется на сервере TACACS+. Если невозможно выполнить проверку подлинности, то не используется никакой метод проверки подлинности.

Local, RADIUS (Локально, RADIUS) - проверка подлинности сначала выполняется локально. Если невозможно выполнить проверку подлинности локально, то проверка подлинности выполняется на сервере RADIUS. Если сервер RADIUS не может выполнить проверку подлинности, сеанс блокируется.

Local, TACACS+ (Локально, TACACS+) - проверка подлинности сначала выполняется локально. Если невозможно выполнить проверку подлинности локально, то проверка подлинности выполняется на сервере TACACS+. Если сервер TACACS+ не может выполнить проверку подлинности, сеанс блокируется.

RADIUS, Local (RADIUS, Локально) - проверка подлинности сначала выполняется на сервере RADIUS. Если невозможно выполнить проверку подлинности на сервере RADIUS, то проверка подлинности сеанса выполняется локально. Если невозможно выполнить проверку подлинности локально, сеанс блокируется.

TACACS+, Local (TACACS+, Локально) - проверка подлинности сначала выполняется на сервере TACACS+. Если невозможно выполнить проверку подлинности на сервере TACACS+, то проверка подлинности сеанса выполняется локально. Если невозможно выполнить проверку подлинности локально, сеанс блокируется.

Local, RADIUS, None (Локально, RADIUS, Нет) - проверка подлинности сначала выполняется локально. Если невозможно выполнить проверку подлинности локально, то проверка подлинности выполняется на сервере RADIUS. Если сервер RADIUS не может выполнить проверку подлинности, сеанс блокируется.

RADIUS, Local, None (RADIUS, Локально, Нет) - проверка подлинности сначала выполняется на сервере RADIUS. Если невозможно выполнить проверку подлинности на сервере RADIUS, то проверка подлинности сеанса выполняется локально. Если невозможно выполнить проверку подлинности локально, сеанс блокируется.

Local, TACACS+, None (Локально, TACACS+, Нет) - проверка подлинности сначала выполняется локально. Если невозможно выполнить проверку подлинности локально, то проверка подлинности выполняется на сервере TACACS+. Если сервер TACACS+ не может выполнить проверку подлинности, сеанс блокируется.

TACACS+, Local, None (TACACS+, Локально, Нет) - проверка подлинности сначала выполняется на сервере TACACS+. Если невозможно выполнить проверку подлинности на сервере TACACS+, то проверка подлинности сеанса выполняется локально. Если невозможно выполнить проверку подлинности локально, сеанс блокируется.

Применение списка методов проверки подлинности к сеансам консоли

1. Откройте страницу [Select Authentication](#) (Выбор проверки подлинности).
2. Выберите профиль проверки подлинности в поле **Console** (Консоль).
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Сеансам консоли будет назначен список методов проверки подлинности.

Применение списка проверки подлинности к сеансам Telnet

1. Откройте страницу [Select Authentication](#) (Выбор проверки подлинности).
2. Выберите профиль проверки подлинности в поле Telnet.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Сеансам консоли будут назначены профили проверки подлинности.

Применение профилей проверки подлинности к сеансам Secure Telnet (SSH)

1. Откройте страницу [Select Authentication](#) (Выбор проверки подлинности).
2. Выберите профиль проверки подлинности в поле Secure Telnet (SSH).
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Сеансам Secure Telnet (SSH) будут назначены профили проверки подлинности.

Назначение сеансам HTTP последовательности проверки подлинности

1. Откройте страницу [Select Authentication](#) (Выбор проверки подлинности).
2. Для сеанса HTTP в поле **Optional Methods** (Дополнительные методы) выберите метод проверки подлинности и нажмите кнопку со стрелкой вправо.

Выбранный метод проверки подлинности будет перенесен в поле Selected Methods (Выбранные методы).

3. Повторяйте это действие до тех пор, пока необходимая последовательность проверки подлинности не отобразится в поле Selected Methods (Выбранные методы).
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Сеансам HTTP будет назначена последовательность проверки подлинности.

Назначение сеансам Secure HTTP последовательности проверки подлинности

1. Откройте страницу [Select Authentication](#) (Выбор проверки подлинности).
2. Для сеанса Secure HTTP в поле **Optional Methods** (Дополнительные методы) выберите метод проверки подлинности и нажмите кнопку со стрелкой вправо.

Выбранный метод проверки подлинности будет перенесен в поле Selected Methods (Выбранные методы).

3. Повторяйте это действие до тех пор, пока необходимая последовательность проверки подлинности не отобразится в поле Selected Methods (Выбранные методы).
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Сеансам Secure HTTP будет назначена последовательность проверки подлинности.

Назначение профилей или последовательностей методов проверки подлинности доступа с помощью команд консоли

В следующей таблице приведены команды консоли для назначения методов доступа, списков методов или последовательностей проверки подлинности.

Таблица 6-32. Команды консоли для методов доступа

--	--

Команда консоли	Описание
<code>enable authentication {default имя_списка}</code>	Указывает список методов проверки подлинности, когда пользователь переходит на уровне с более высокими привилегиями в удаленном сеансе telnet или консоли.
<code>login authentication {default имя_списка}</code>	Определяет список методов проверки подлинности при входе в систему с помощью подключения telnet или консоли.
<code>ip http authentication метод1 [метод2...]</code>	Определяет методы проверки подлинности для пользователей серверов http.
<code>ip https authentication метод1 [метод2...]</code>	Определяет методы проверки подлинности для пользователей серверов https.
<code>show authentication methods</code>	Отображает информацию о методах проверки подлинности.

Далее приведен пример команд консоли.

```
Console# show authentication methods
```

```
Login Authentication Method Lists
```

```
-----
```

```
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

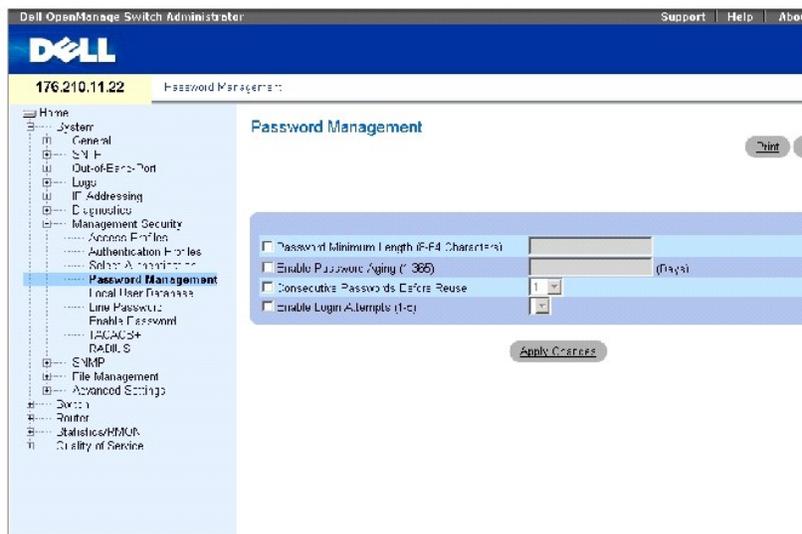
Управление паролями

Управление паролями повышает безопасность сети и улучшает контроль паролей. Паролям для доступа SSH, Telnet, HTTP, HTTPS и SNMP назначаются функции безопасности, включая следующие.

1. Определение минимальной длины пароля
1. Истечение срока пароля
1. Предотвращение частого повторного использования паролей
1. Блокировка входа пользователей после неудачных попыток ввода пароля

Чтобы открыть страницу [Password Management](#) (Управление паролями), выберите **System** (Система)→ **Management Security** (Безопасность управления)→ **Password Management** (Управление паролями) на панели дерева.

Рис. 6-46. Страница Password Management (Управление паролями)



Страница [Password Management](#) (Управление паролями) содержит следующие поля.

Password Minimum Length (8-64 Characters) (Минимальная длина пароля (8-64 символов)) - когда установлен этот флажок, указывает минимальную длину пароля. Например, администратор может определить, что минимальное количество символов для всех паролей канала - 10.

Enable Password Aging (1-365) (Включить срок хранения пароля) - когда установлен этот флажок, указывает временной интервал для хранения пароля. Значение для этого поля находится в диапазоне: 1-365 дней.

Consecutive Passwords Before Reuse (Последовательные пароли перед повторным использованием) - указывает количество изменений пароля перед тем, как использовать его повторно. Возможные значения: 1 - 10.

 **ПРИМЕЧАНИЕ.** Пользователь уведомляется о необходимости изменить пароль перед истечением срока пароля. Веб-пользователи не видят этого уведомления.

Enable Login Attempts (1-5) (Включить контроль попыток ввода пароля) - включает блокировку входа пользователя устройства при использовании неверного пароля определенное количество раз. Например, если определено, что число попыток ввода пароля равно пяти, и пользователь вводит пароль неправильно пять раз, то при шестой попытке устройство блокирует пользователя. Диапазон значений для этого поля: 1-5 попытки.

Определение ограничений для пароля

1. Откройте страницу [Password Management](#) (Управление паролями)
2. Определите соответствующие поля.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Ограничения для пароля будут определены, а устройство обновлено.

Определение ограничений для пароля с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для настройки паролей на странице [Password Management](#) (Управление паролями).

Таблица 6-33. Команды консоли для управления паролями

Команда консоли	Описание
<code>password min-length length</code>	Определяет требуемую минимальную длину пароля.
<code>passwords aging days</code>	Определяет время истечения срока действия пароля в локальной базе данных.
<code>passwords history number</code>	Определяет число требуемых изменения пароля перед повторным его использованием в локальной базе данных.
<code>passwords lock-out number</code>	Блокирует учетную запись пользователя после указанного количества неудачных попыток ввода пароля.
<code>show password configuration</code>	Отображает информацию об управлении паролями.

Далее приведен пример команд консоли.

```
Console (config)# password min-length 8
```

```
Console (config)# password aging 120
```

```
Console (config)# passwords history 2
```

```
Console (config)# passwords lock-out 3
```

```
Console (config) # exit
```

```
Console# show passwords configuration
```

```
Minimal length: 8
```

```
Aging: 120 days
```

History: 2

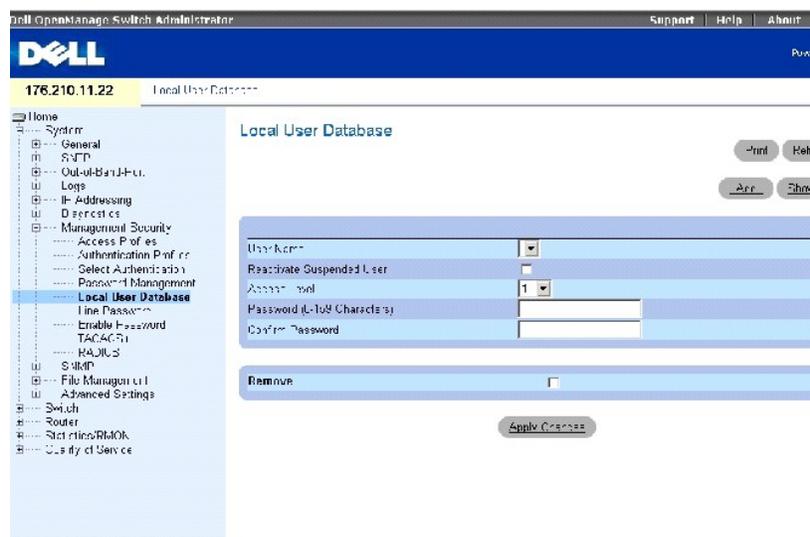
Lock-out: Disabled

Определение локальных баз данных пользователей

Для определения паролей, прав доступа для пользователей и возобновления приостановленных учетных записей пользователей используйте страницу [Local User Database](#) (Локальная база данных пользователей).

Чтобы открыть страницу [Local User Database](#) (Локальная база данных пользователей), выберите System (Система)→ Management Security (Безопасность управления)→ Local User Database (Локальная база данных пользователей) на панели дерева.

Рис. 6-47. Страница Local User Database (Локальная база данных пользователей)



Страница [Local User Database](#) (Локальная база данных пользователей) содержит следующие поля.

User Name (Имя пользователя) - список пользователей.

Reactivated Suspended User (Возобновление приостановленных пользователей) - выберите этот параметр, чтобы возобновить права доступа указанного пользователя. Права доступа могут быть приостановлены после неудачной попытки входа в систему.

Access Level (1-15) (Уровень доступа) - уровень доступа пользователя. Самый низкий уровень доступа пользователя - 1, а самый высокий -15.

Password (Пароль) - пароль, определенный пользователем.

Confirm Password (Подтверждение пароля) - подтверждение задаваемого пользователем пароля.

Remove (Удалить) - когда установлен этот флажок, удаляется пользователь в списке **User Name** (Имя пользователя).

Назначение прав доступа пользователю

1. Откройте страницу [Local User Database](#) (Локальная база данных пользователей).
2. Выберите пользователя в поле **User Name** (Имя пользователя).
3. Определите поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Права доступа пользователя и пароли будут определены, а устройство обновлено.

Добавление пользователя в локальную базу данных пользователей

1. Откройте страницу [Local User Database](#) (Локальная база данных пользователей).
2. Нажмите кнопку **Add** (Добавить), чтобы отобразить страницу **Add User** (Добавление пользователя).
3. Заполните поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Новый пользователь будет определен, а устройство обновлено.

 **ПРИМЕЧАНИЕ.** На устройстве можно определить 30 пользователей.

Возобновление приостановленных прав пользователя.

1. Откройте страницу [Local User Database](#) (Локальная база данных пользователей).
2. Нажмите кнопку **Show All** (Показать все), чтобы открыть страницу **Local User Table** (Локальная таблица пользователей).
3. Выберите запись **User Name** (Имя пользователя).
4. Установите флажок для параметра **Reactivate Suspended User** (Возобновить приостановленные права пользователя).
5. Нажмите кнопку **Apply Changes** (Применить изменения).

Права доступа пользователя и пароли будут возобновлены, а устройство обновлено.

Удаление пользователей из локальной базы данных пользователей

1. Откройте страницу [Local User Database](#) (Локальная база данных пользователей).
2. Нажмите кнопку **Show All** (Показать все), чтобы открыть страницу **Local User Table** (Локальная таблица пользователей).
3. Выберите **User Name** (Имя пользователя).
4. Установите флажок **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 для просмотра полей на странице **Local User Database** (Локальная база данных пользователей).

Таблица 6-34. Команды консоли для локальной базы данных пользователей

Команда консоли	Описание
<code>username имя [password пароль] [privilege уровень] [encrypted]</code>	Устанавливает проверку подлинности по имени пользователя.

set username name active	Возобновляет заблокированную учетную запись пользователя.
--------------------------	---

Далее приведен пример команд консоли.

```
Console (config)#username bob password lee privilege 15
```

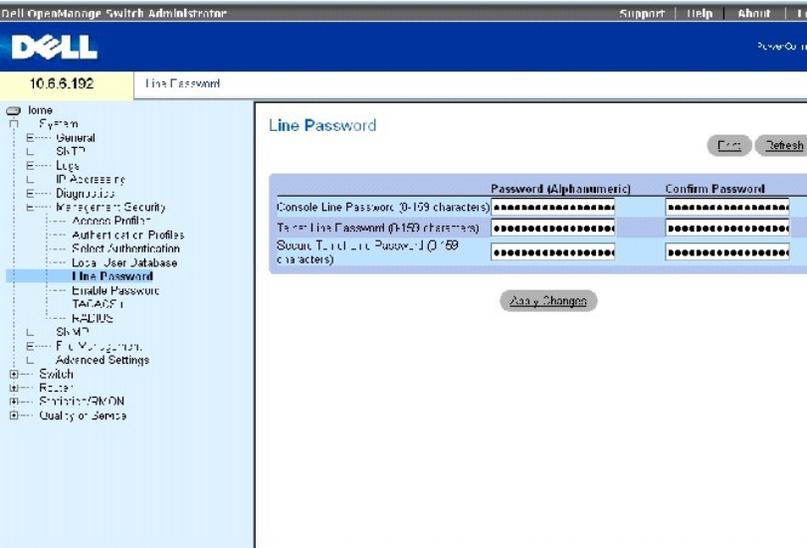
```
console# set username bob active
```

Defining Line Passwords

Страница [Line Password](#) (Пароль канала связи) позволяет определять пароли каналов для методов управления.

Чтобы открыть страницу [Line Password](#) (Пароль канала), выберите System (Система)→ Management Security (Безопасность управления)→ Line Password (Пароль каналов) на панели дерева.

Рис. 6-48. Страница Line Password (Пароль канала)



Страница [Line Password](#) (Пароль канала) содержит следующие поля.

Line Password for Console/Telnet/Secure Telnet (Пароль канала для консоли/Telnet/Secure Telnet) - пароль канала для доступа к устройству через сеанс консоли, Telnet или Secure Telnet.

Confirm Password (Подтвердить пароль) - подтверждение нового пароля канала. Пароль отображается в формате *****.

Defining Line Passwords

1. Откройте страницу [Line Password](#) (Пароль канала).
2. Определите поле Line Password (Пароль канала) для типа сеанса, который используется для подключения к устройству.

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

Пароль канала для типа сеанса будет определен, а устройство обновлено.

Назначение паролей каналов с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для определения паролей канала.

Таблица 6-35. Команды консоли для пароля канала

Команда консоли	Описание
<code>password <i>пароль</i> [encrypted]</code>	Задаёт пароль канала.

Далее приведен пример команд консоли.

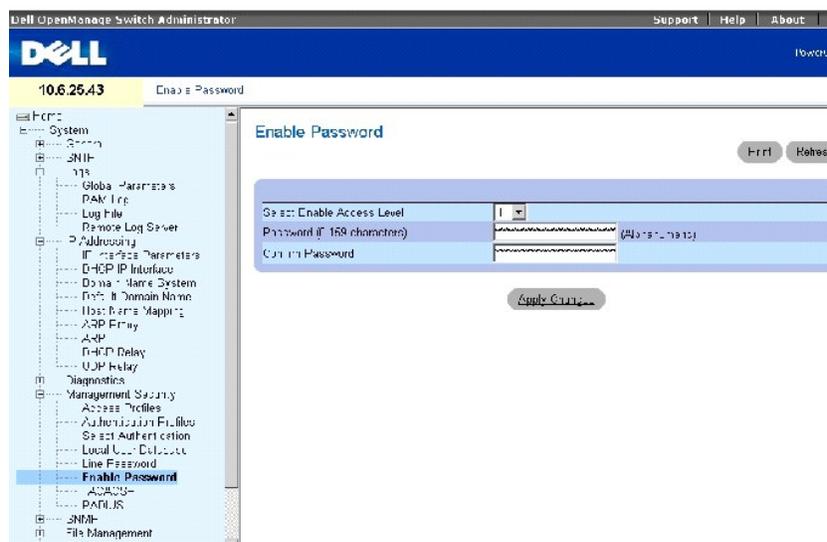
```
Console (config-line)# password ****
```

Определение пароля включения

Страница [Modify Enable Password](#) (Изменение пароля включения) задаёт локальный пароль для контроля доступа с различными уровнями привилегий (1-15).

Чтобы открыть страницу [Modify Enable Password](#) (Изменение пароля включения), выберите **System** (Система) → **Management Security** (безопасность управления) → **Enable Password** (Пароль включения) на панели дерева.

Рис. 6-49. Страница Modify Enable Password (Изменение пароля включения)



Страница [Modify Enable Password](#) (Изменение пароля включения) содержит следующие поля.

Select Enable Access Level (Выбор уровня доступа для включения) - уровень доступа, связанный с паролем включения. Возможные значения этого поля: 1-15.

Password (Пароль) - текущий пароль включения.

Confirm Password (Подтвердить пароль) - подтверждение нового пароля включения. Пароль отображается в формате *****.

Определение нового пароля включения

1. Откройте страницу [Modify Enable Password](#) (Изменение пароля включения).
2. Введите значения в полях диалогового окна.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Новый пароль будет определен, а устройство обновлено.

Назначение паролей включения с помощью команд консоли

В следующей таблице приведены команды консоли для настройки полей, отображаемых на странице [Modify Enable Password](#) (Изменение пароля включения).

Таблица 6-36. Команды консоли для паролей включения

Команда консоли	Описание
<code>enable password [level уровень] пароль [encrypted]</code>	Задаёт локальный пароль для управления доступом для уровней пользователей и привилегий.
<code>show users accounts</code>	Отображает сведения о локальной базе данных пользователей.

Далее приведен пример команд консоли.

```
Console (config)# enable password level 15 dell
```

```
Console# show users accounts
```

```
Username Privilege
```

```
-----
```

```
Bob 15
```

```
Jim 15
```

```
Dell 1515
```

Настройка параметров TACACS+

Устройство предоставляет поддержку для клиентов TACACS+ (Terminal Access Controller Access Control System). TACACS+ обеспечивает централизованную систему безопасности для проверки пользователей, получающих доступ к устройству.

TACACS+ обеспечивает централизованную систему управления при соблюдении совместимости с RADIUS и другими процессами проверки подлинности. TACACS+ предоставляет следующие службы:

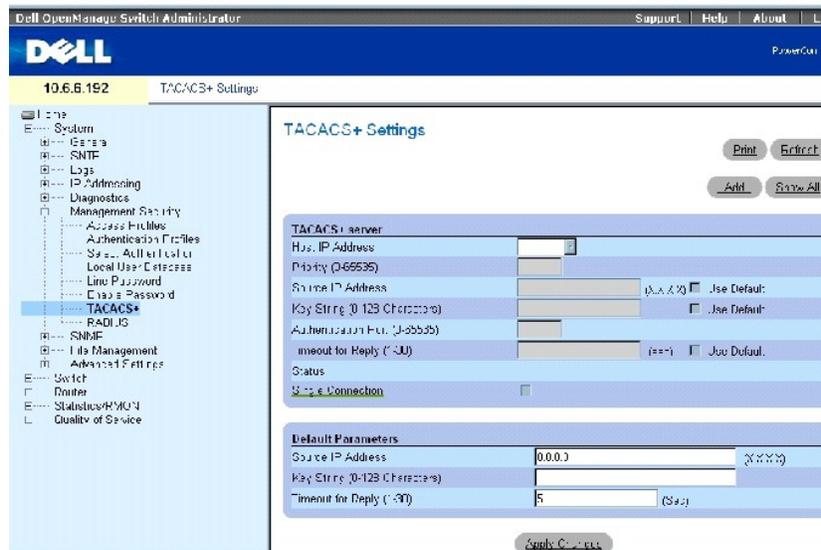
- 1 **Authentication** (Проверка подлинности) - обеспечивает проверку подлинности во время входа, а также по именам пользователей и определенным пользователям паролям.
- 1 **Authorization** (Авторизация) - выполняется при входе. После завершения сеанса проверки подлинности запускается сеанс авторизации с использованием проверенного имени пользователя. Сервер TACACS+ проверяет привилегии пользователя.

Протокол TACACS+ обеспечивает целостность сети благодаря обмену шифрованными данными протокола между устройством и сервером TACACS+.

Страница [TACACS+ Settings](#) (Параметры TACACS+) содержит настройки TACACS+ для порта управления в диапазоне как определенные пользователем, так и настройки по умолчанию.

Чтобы открыть страницу [TACACS+ Settings](#) (Параметры TACACS+), выберите **System** (Система) → **Management Security** (Безопасность управления) → **TACACS+** на панели дерева.

Рис. 6-50. Страница TACACS+ Settings (Параметры TACACS+)



Страница параметры [TACACS+](#) содержит следующие поля.

Host IP Address (IP-адрес хоста) - определяет IP-адрес сервера TACACS+.

Priority (0-65535) (Приоритет) - определяет порядок, в котором используются серверы TACACS+. Значение по умолчанию: 0.

Source IP Address (IP-адрес источника) - IP-адрес устройства источника, используемый для сеанса TACACS+ между устройством и сервером TACACS+.

Key String (0-128 Characters) (Строка ключа (1-128 символов)) - определяет проверку подлинности и ключ шифрования обмена данными TACACS+ между устройством и сервером TACACS+. Этот ключ должен соответствовать шифрованию, используемому для сервера TACACS+.

Authentication Port (0-65535) (Порт проверки подлинности) - порт проверки подлинности, через который осуществляется обмен данными во время сеансов TACACS+. По умолчанию это порт 49.

Timeout for Reply (1-30) (Время для ответа) - время ожидания ответа при обмене данными между устройством и сервером TACACS+. Диапазон значений: 1-30 секунд.

Status (Состояние) - состояние соединения между устройством и сервером TACACS+. Возможные значения:

Connected (Соединение установлено) - между устройством и сервером TACACS+ установлено соединение.

Not Connected (Соединение не установлено) - отсутствует соединение между устройством и сервером TACACS+.

Single Connection (Одно соединение) - когда выбран этот параметр, поддерживается одно открытое соединение между устройством и сервером TACACS+.

В качестве параметров TACACS+ по умолчанию используются параметры по умолчанию, определенные пользователем. Параметры по умолчанию применяются для вновь определенных серверов TACACS+. Если значения по умолчанию не определены, для новых серверов TACACS+ используются системные настройки по умолчанию. Далее показаны настройки TACACS+ по умолчанию:

Source IP Address (IP-адрес источника) - IP-адрес устройства источника, используемый по умолчанию для сеанса TACACS+ между устройством и сервером TACACS+.

Key String (0-128 Characters) (Строка ключа (1-128 символов)) - используемые по умолчанию проверка подлинности и ключ шифрования обмена данными TACACS+ между устройством и сервером TACACS+.

Timeout for Reply (1-30) - (Время для ответа) - время ожидания ответа при обмене данным между устройством и сервером TACACS+.

 **ПРИМЕЧАНИЕ.** Вышеупомянутые значения также следует использовать и на странице [OOB TACACS+ Settings](#) (Параметры TACACS+ OOB) (System (Система)→ Out-of- Band-Port (Порт вне диапазона)→ TACACS+).

Определение параметров TACACS+

1. Откройте страницу [TACACS+ Settings](#) (Параметры TACACS+).
2. Определите поля.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Параметры TACACS+ для данного устройства будут изменены.

Добавление сервера TACACS+

1. Откройте страницу [TACACS+ Settings](#) (Параметры TACACS+).
2. Нажмите кнопку **Add** (Добавить).

Откроется страница **Add TACACS+ Host** (Добавление хоста TACACS+).

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

Будет добавлен сервер TACACS+, а устройство будет обновлено.

Device Configuration						

IP address	Status	Port	Single Connection	TimeOut	Source IP	Priority
-----	-----	----	-----	-----	-----	-----
-						
171.16.8.1	Not Connected	49	No	Global	Global	0
OOB Host Configuration						
IP address	Status	Port	Single Connection	TimeOut	Source IP	Priority
-----	-----	----	-----	-----	-----	-----
-						
No TACACS server is configured.						
Device Configuration						

Source IP: 0.0.0.0						
OOB host Configuration						

Source IP : 0.0.0.0						

Настройка параметров RADIUS

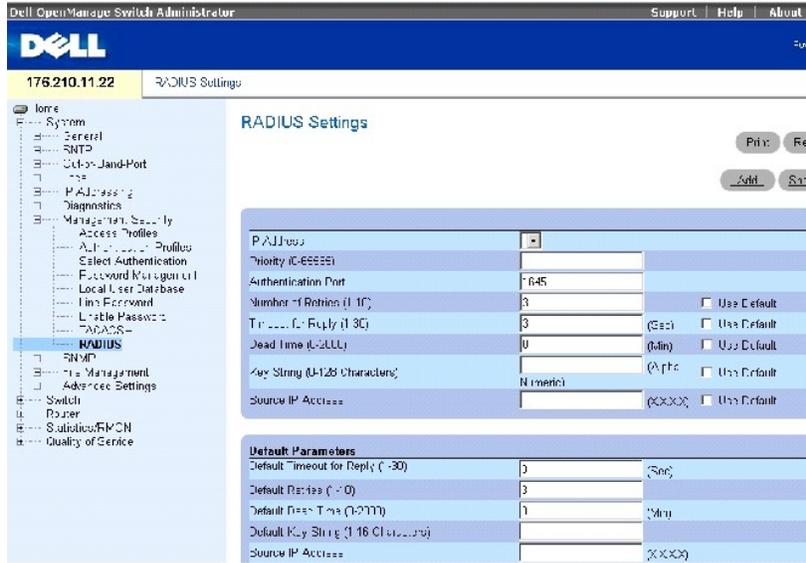
Серверы RADIUS (RADIUS - Remote Authorization Dial-In User Service) обеспечивают дополнительную защиту сетей. На RADIUS сервере ведется база данных пользователей, содержащая данные проверки подлинности для каждого пользователя. Серверы RADIUS обеспечивают централизованный метод проверки подлинности:

- 1 Доступ Telnet
- 1 Доступ по Интернету
- 1 Доступ к коммутатору с консоли

Страница [RADIUS Settings](#) (Параметры RADIUS) содержит параметры сервера RADIUS, определяемые пользователем, и параметры по умолчанию.

Чтобы открыть страницу [RADIUS Settings](#) (Параметры RADIUS), выберите **System Management** (Управление системой) → **Security** (Безопасность) → **RADIUS** на панели дерева.

Рис. 6-51. Страница RADIUS Settings (Параметры RADIUS)



Страница [RADIUS Settings](#) (Параметры RADIUS) содержит следующие поля.

IP Address (IP-адрес) - IP-адрес порта проверки подлинности.

Priority (0-65535) (Приоритет) - указывает приоритет порта. Возможны следующие значения: 0-65535.

Authentication Port (Порт проверки подлинности) - указывает порт проверки подлинности, который используется для проверки подлинности сервера RADIUS.

Number of Retries (1-10) (Число повторных попыток) - число запросов, переданных серверу RADIUS, прежде чем произошла ошибка. Возможные значения этого поля: 1 - 10. Значение по умолчанию: 3. Если для хоста не определено значение, для каждого хоста будет применяться общее значение. Чтобы использовать значения по умолчанию, нажмите кнопку **Use Default** (Использовать значения по умолчанию).

Timeout for Reply (1-30) (Время для ответа) - время (в секундах), в течение которого устройство ожидает ответа от сервера RADIUS. Возможные значения этого поля: 1 - 30. Значение по умолчанию: 3. Если для хоста не определено значение, для каждого хоста будет применяться общее значение. Чтобы использовать значения по умолчанию, нажмите кнопку **Use Default** (Использовать значения по умолчанию).

Dead Time (0-2000) (Время отключения) - определяет время (в минутах), в течение которого сервер RADIUS не принимает запросы на обработку. Диапазон значений: 0-2000. Если для хоста не определено значение, для каждого хоста будет применяться общее значение. Чтобы использовать значения по умолчанию, нажмите кнопку **Use Default** (Использовать значения по умолчанию).

Key String (0-128 Characters) (Строка ключа (1-128 символов)) - строка ключа, используемая для проверки подлинности и шифрования всех данных RADIUS, передаваемых между устройством и сервером RADIUS. Этот ключ должен соответствовать шифрованию RADIUS. Если для хоста не определено значение, для каждого хоста будет применяться общее значение.

Source IP Address (IP-адрес источника) - IP-адрес для устройства, подключающегося к серверу RADIUS.

 **ПРИМЕЧАНИЕ.** Параметры по умолчанию для этой страницы определяются пользователем.

Default Retries (1-10) (Число повторных попыток по умолчанию) - число запросов по умолчанию, передаваемых серверу RADIUS, прежде чем произошла ошибка.

Default Timeout for Reply (1-30) (Время на ответ по умолчанию) - число запросов по умолчанию, переданных серверу RADIUS прежде, чем произошла ошибка. Возможные значения этого поля: 1 - 30.

Default Dead time (0-2000) (Время отключения по умолчанию) - определяет время по умолчанию (в минутах), в течение которого сервер RADIUS не принимает запросы на обработку. Диапазон значений: 0-2000.

Default Key String (0-128 characters) (Строка ключа по умолчанию (1-128 символов)) - строка ключа по умолчанию, используемая для проверки подлинности и шифрования всех данных RADIUS, передаваемых между устройством и сервером RADIUS. Этот ключ должен соответствовать шифрованию RADIUS.

Source IP Address (IP-адрес источника) - IP-адрес по умолчанию для устройства, подключающегося к серверу RADIUS.

Добавление сервера RADIUS

1. Откройте страницу [RADIUS Settings](#) (Параметры RADIUS).
2. Нажмите кнопку **Add** (Добавить), чтобы отобразить страницу **Add RADIUS Server** (Добавить сервер RADIUS).
3. Определите поля в диалоговом окне.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Новый сервер RADIUS будет добавлен, а устройство обновлено.

Определение параметров RADIUS

1. Откройте страницу [RADIUS Settings](#) (Параметры RADIUS).
2. Определите поля в диалоговом окне.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Параметры RADIUS для данного устройства будут изменены.

Изменение параметров сервера RADIUS

1. Откройте страницу [RADIUS Settings](#) (Параметры RADIUS).
2. Нажмите кнопку **Show All** (Показать все), чтобы отобразить список **RADIUS Servers List** (Список серверов RADIUS).
3. Измените значения в полях диалогового окна.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Параметры RADIUS будут сохранены, а устройство обновлено.

Удаление сервера RADIUS из списка серверов RADIUS

1. Откройте страницу [RADIUS Settings](#) (Параметры RADIUS).
2. Нажмите кнопку **Show All** (Показать все), чтобы отобразить список **RADIUS Servers List** (Список серверов RADIUS).
3. Выберите сервер RADIUS и установите флажок **Remove** (Удалить).

Сервер RADIUS будет удален из списка.

Определение серверов RADIUS с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для определения полей, отображаемых на странице [RADIUS Settings](#) (Параметры RADIUS).

Таблица 6-38. Команды консоли для сервера RADIUS

Команда консоли	Описание
<code>radius-server timeout количество_секунд</code>	Задаёт интервал, в течение которого маршрутизатор ожидает ответа сервера.
<code>radius-server retransmit количество_попыток</code>	Определяет, сколько раз программа выполняет поиск списка хостов сервера RADIUS.
<code>radius-server deadtime количество_секунд</code>	Настраивает пропуск недоступных серверов.
<code>radius-server key строка_ключа</code>	Задаёт проверку подлинности и ключ шифрования для всех связей RADIUS между маршрутизатором и окружением RADIUS.
<code>radius-server host ip-адрес [auth-port номер_порта_идентификации] [timeout количество_секунд] [retransmit количество_попыток] [deadtime количество_секунд] [key строка_ключа] [source источник] [priority приоритет]</code>	Определяет хост сервера RADIUS.
<code>show radius-servers</code>	Отображает параметры сервера RADIUS.

Далее приведен пример команд консоли:

```
Console (config)# radius-server timeout 5
```

```
Console (config)# radius-server retransmit 5
```

```
Console (config)# radius-server deadtime 10
```

```
Console (config)# 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. Устройство поддерживает протокол *SNMP* версии 1, 2 и 3.

ПРИМЕЧАНИЕ. По умолчанию на устройстве автоматически включается протокол *SNMP* версии 2. Чтобы включить протокол *SNMP* версия 3, для устройства должен быть определен локальный идентификатор механизма. Локальный идентификатор механизма может представлять собой строку, определенную пользователем, или строку по умолчанию на основе *MAC*-адреса устройства. Дополнительную информацию о настройке локального идентификатора механизма см. в разделе «[Определение общих параметров SNMP](#)».

SNMP версии 1 и версии 2

Агент *SNMP* поддерживает 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.

SNMP версии 3

По протоколу *SNMP* версии 3 также осуществляется контроль доступа и применяется новый механизм системных прерываний для устройств распределения питания (*PDU*), поддерживающих протоколы *SNMP* версии 1 и 2. Кроме того, для протокола *SNMP* версии 3 определяется модель *USM* (*User Security Model*), которая включает в себя следующее.

- 1 **Authentication** (Проверка подлинности) - обеспечивает сохранность и проверку подлинности источника данных.
- 1 **Privacy** (Конфиденциальность) - предотвращает раскрытие содержания сообщения. Для шифрования используется режим *CBC* (*Cipher-Block-Chaining*). Для сообщения по протоколу *SNMP* включается или проверка подлинности, или и проверка подлинности, и конфиденциальность данных. Однако функция обеспечения конфиденциальности не может быть включена без проверки подлинности.
- 1 **Timeliness** (Своевременность) - предотвращает отсрочку или дублирование сообщений. Агент *SNMP* сравнивает входящее сообщение с данными о времени сообщения.
- 1 **Key Management** (Управление ключами) - генерация ключа, обновления ключа и использование ключа.

Устройство поддерживает фильтры уведомлений *SNMP* на основе идентификаторов объекта (*OID*). Система использует идентификаторы объекта (*OID*) для управления функциями устройства. Протокол *SNMP* версии 3 поддерживает следующие функции.

- 1 Безопасность
- 1 Функция контроля доступа
- 1 Системные прерывания

Ключи проверки подлинности и конфиденциальности изменяются в модели [USM \(User Security Model\)](#) протокола *SNMP* версии 3.

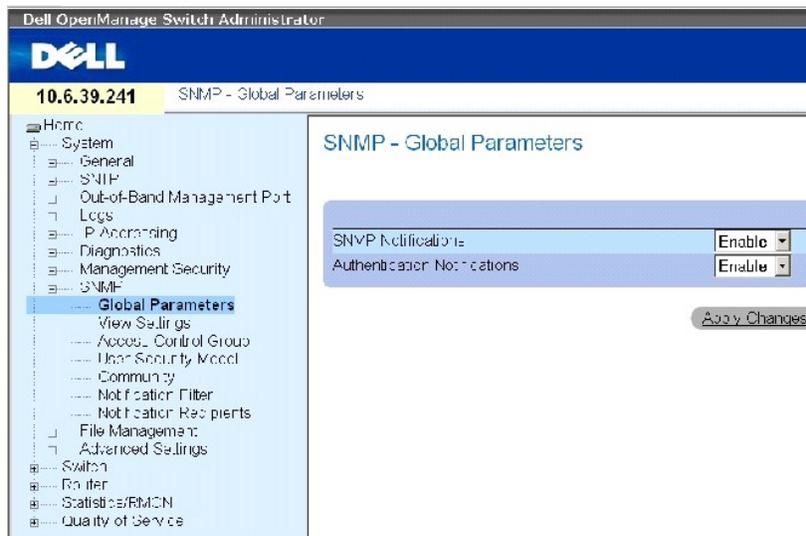
Используйте страницу *SNMP* для определения параметров *SNMP*. Чтобы открыть страницу *SNMP*, выберите **System** (Система)→ **SNMP** на панели дерева.

Определение общих параметров SNMP

Для включения *SNMP* и уведомлений о проверке подлинности используйте страницу [Global Parameters](#) (Общие параметры).

Чтобы открыть страницу [Global Parameters](#) (Общие параметры), выберите **System** (Система)→ **SNMP**→ **Global Parameters** (Общие параметры) на панели дерева.

Рис. 6-52. Страница Global Parameters (Общие параметры)



Страница [Global Parameters](#) (Общие параметры) содержит следующие параметры.

SNMP Notifications (Уведомления SNMP) - включает или отключает отправку устройством уведомлений SNMP.

Authentication Notifications (Уведомления о проверке подлинности) - включает или отключает отправку системных прерываний SNMP при ошибке проверки подлинности.

Включение уведомлений SNMP

1. Откройте страницу [Global Parameters](#) (Общие параметры).
2. Выберите **Enable** (Включить) в поле **SNMP Notifications** (Уведомления SNMP).
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Уведомления SNMP будут включены, а устройство обновлено.

Включение уведомлений о проверке подлинности

1. Откройте страницу [Global Parameters](#) (Общие параметры).
2. Выберите **Enable** (Включить) в поле **SNMP Notifications** (Уведомления SNMP).
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Уведомления о проверке подлинности будут включены, а устройство обновлено.

Включение уведомлений SNMP с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для определения полей, отображаемых на странице [Global Parameters](#) (Общие параметры).

Таблица 6-39. Команды консоли для уведомлений SNMP

--	--

Команда консоли	Описание
<code>snmp-server engineID local {строка_id_механизма default}</code>	Определяет идентификатор механизма SNMP на локальном устройстве.
<code>show snmp</code>	Показывает текущую конфигурацию SNMP устройства.

Далее приведен пример команд консоли:

Console (config)# snmp-server enable traps		
Console (config)# snmp-server trap authentication		
Console (config)# end		
console# show snmp		
Community-String	Community-Access	IP address
-----	-----	-----
public	read only	All
private	read write	172.16.1.1
private	read write	172.17.1.1
OOB management stations		
Community-String	Community-Access	IP address
-----	-----	-----
private	read write	176.16.8.9
Traps are enabled.		
Authentication trap is enabled.		
Trap-Rec-Address	Trap-Rec-Community	Version
192.122.173.42	public	2

OOB trap receivers		
Trap-Rec-Address	Trap-Rec-Community	Version
176.16.8.9	public	2
System Contact: Robert		
System Location: Marketing		

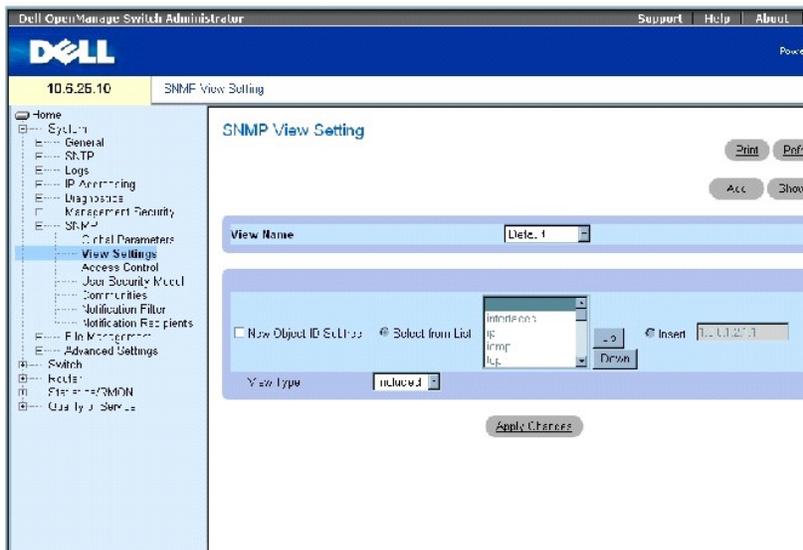
Определение представлений SNMP

Представления SNMP обеспечивают или блокируют доступ к функциям или аспектам функций. Например, можно определить вид, который устанавливает, что SNMP-группа А имеет доступ к маршрутизации только для чтения, тогда как SNMP-группа В имеет доступ к маршрутизации с возможностью чтения и записи. Доступ к функциям предоставляется с помощью имени MIB или идентификатора объекта MIB.

Для определения представлений SNMP используйте страницу [SNMP View Setting](#) (Параметры представления SNMP).

Чтобы открыть страницу [SNMP View Setting](#) (Параметры представления SNMP), выберите **System** (Система) → **SNMP** → **View Settings** (Параметры представлений SNMP) на панели дерева.

Рис. 6-53. Страница SNMP View Setting (Параметры представления SNMP)



Страница [SNMP View Setting](#) (Параметры представления SNMP) содержит следующие поля.

View Name (Имя вида) - содержит список видов, определенных пользователем. Имя вида может содержать не более 30 буквенно-цифровых символов.

New Object ID Subtree (Новая ветвь идентификатора объекта) - указывает наличие или отсутствие идентификатора объекта функции устройства в представлении SNMP.

View Type (Тип представления) - разрешает доступ к выбранной функции или подфункции в представлении SNMP.

Добавление представления

1. Откройте страницу [SNMP View Setting](#) (Параметры представления SNMP).
2. Нажмите кнопку **Add** (Добавить).

Откроется страница [Add A View](#) (Добавление представления)

Рис. 6-54. Страница Add A View (Добавление представления)

Form fields and controls:

- View Name (1-31 Characters): [Text Input]
- Subtree ID: Tree: [Text Input]
- Select from List: [Dropdown]
- Up: [Button]
- Down: [Button]
- View Type: [Dropdown menu showing 'Included']
- Apply Changes: [Button]

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

Будет добавлено представление SNMP, а устройство обновлено.

Отображение таблицы представлений

1. Откройте страницу [SNMP View Setting](#) (Параметры представления SNMP).
2. Нажмите кнопку **Show All** (Показать все).

Откроется страница [View Table](#) (Таблица представлений).

Рис. 6-55. Страница View Table (Таблица представлений)

Table structure:

Object ID Subtree	View Type	Remove
1	Included	<input type="checkbox"/>
2 1.3.6.1.6.3.1.6	Exclude	<input type="checkbox"/>
3 1.3.6.1.6.3.1.1.2	Exclude	<input type="checkbox"/>
4 1.3.6.1.4.1.28.2.2	Exclude	<input type="checkbox"/>

Buttons: View Name: Def..1, Apply Changes

Удаление представлений SNMP

1. Откройте страницу [SNMP View Setting](#) (Параметры представления SNMP).

2. Нажмите кнопку **Show All** (Показать все).

Откроется страница [View Table](#) (Таблица представлений).

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

Представление SNMP будет удалено, а устройство обновлено.

Определение представлений SNMP с помощью команд консоли

В следующей таблице приведены команды консоли для определения полей, отображаемых на странице [SNMP View Setting](#) (Параметры представления SNMP).

Таблица 6-40. Команды консоли для определения представления SNMP

Команда консоли	Описание
<code>show snmp views [имя_представления]</code>	Отображает конфигурацию представлений.

Далее приведен пример команд консоли:

Console (config)# snmp-server view user1 1 included		
Console (config)# end		
Console # show snmp views		
Name	OID Tree	Тип
-----	-----	-----
user1	iso	included
Значение по умолчанию	iso	included
Значение по умолчанию	snmpVacmMIB	excluded
Значение по умолчанию	usmUser	excluded
Значение по умолчанию	rndCommunityTable	excluded
DefaultSuper	iso	included

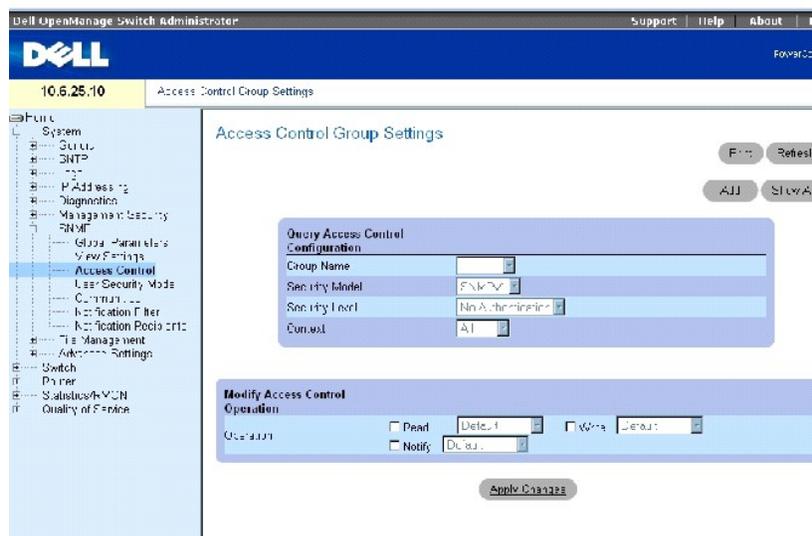
Определение контроля доступа по протоколу SNMP

На странице [Access Control Group](#) (Группа контроля доступа) представлена информация для создания групп SNMP и назначения привилегий доступа по протоколу SNMP. Выделив группы, администраторы сети могут назначать права доступа к отдельным функциям устройства или аспектам функций.

При использовании SNMP функций порт вне диапазона рассматривается как самостоятельное устройство. Можно выбрать просмотр только MIB вне диапазона, MIB устройства или всех MIB.

Чтобы открыть страницу [Access Control Group](#) (Группа контроля доступа), выберите System (Система)→ SNMP→ Access Control (Контроль доступа) на панели дерева.

Рис. 6-56. Страница Access Control Group (Группа контроля доступа)



Страница [Access Control Group](#) (Группа контроля доступа) содержит следующие поля.

Group Name (Имя группы) - содержит список групп, определенных пользователем, к которым применяются правила контроля доступа. Имя группы может содержать не более 30 буквенно-цифровых символов.

Security Model (Модель безопасности) - определяет версию SNMP, используемую для группы. Возможные значения:

SNMPv1 (SNMP версия 1) - для группы определен протокол SNMP версии 1.

SNMPv2 (SNMP версия 2) - для группы определен протокол SNMP версии 2.

SNMPv3 (SNMP версия 3) - для группы определен протокол SNMP версии 3.

Security Level (Уровень безопасности) - уровень безопасности, применяемый к группе. Уровни безопасности применяются только для групп SNMP версии 3. Возможные значения:

No Authentication (Нет проверки подлинности) - для группы не назначаются ни проверка подлинности, ни уровни безопасности для обеспечения конфиденциальности данных.

Authentication (Проверка подлинности) - проверка подлинности сообщений SNMP без их шифрования.

Privacy (Конфиденциальность) - проверка подлинности сообщений SNMP с их шифрованием.

Operation (Работа) - определяет права доступа группы. Возможные значения:

Read (Чтение) - выберите представление, которое запрещает доступ к управлению для просмотра содержания агента. Если ни одно представление не выбрано, то возможен просмотр всех объектов кроме таблицы сообществ, пользователя SNMP версии 3 и таблиц доступа.

Write (Запись) - выберите представление, в котором разрешен доступ для чтения и записи содержания агента, но запрещен доступ к управлению сообществом.

Notify (Уведомление) - выберите представление, в котором разрешена отправка системных прерываний SNMP или сообщений.

Context (Контекст) - контекст, для которого настроена группа доступа. Возможные значения:

Router (Маршрутизатор) - группа доступа настроена для управления внутри диапазона.

OOB (Вне диапазона) - группа доступа настроена для управления вне диапазона.

All (Все) - группа доступа настроена для управления как внутри, так и вне диапазона.

Определение групп SNMP

1. Откройте страницу [Access Control Group](#) (Группа контроля доступа).
2. Нажмите кнопку **Add** (Добавить).

Откроется страница [Add an Access Control Group](#) (Добавление группы контроля доступа).

Рис. 6-57. Страница Add an Access Control Group (Добавление группы контроля доступа)

Refresh

Add an Access Control Configuration

Group Name (1-31 Characters)	Select list item...	New
SNMP Version	SNMPv1	
Security Level	No Authentication	
Operation	<input type="checkbox"/> Read <input type="checkbox"/> Write <input type="checkbox"/> Notify	Default

Apply Changes

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

Группа будет добавлена, а устройство обновлено.

Отображение таблицы доступа

1. Откройте страницу [Access Control Group](#) (Группа контроля доступа).
2. Нажмите кнопку **Show All** (Показать все).

Откроется страница [Access Table](#) (Таблица доступа).

Рис. 6-58. Страница Access Table (Таблица доступа)



Удаление группы

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

Группа будет удалена, а устройство обновлено.

Определение контроля доступа SNMP с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для определения полей, отображаемых на странице [Access Control Group](#) (Группа контроля доступа).

Таблица 6-41. Команды консоли для определения контроля доступа SNMP

Команда консоли	Описание
<code>snmp-server group groupname {v1 v2 v3 {noauth auth priv}} [read чтение] [write запись] [notify уведомление]</code>	Определяет конфигурацию группы SNMP (Simple Network Management Protocol) или таблицы, в которой устанавливается соответствие между пользователями SNMP и представлениями SNMP.
<code>show snmp groups [имя_группы]</code>	Отображает конфигурацию групп.

Далее приведен пример команд консоли.

```
Console (config)# snmp-server group user-group v3 priv read user- view
```

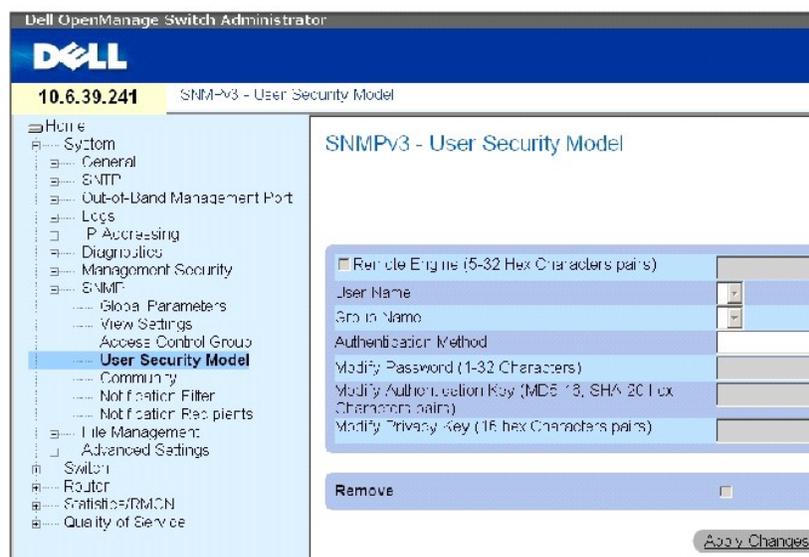
Назначение уровня безопасности SNMP пользователя

С помощью страницы [SNMPv3 User Security Model \(USM\)](#) (Модель USM протокола SNMP версии 3) можно назначить группу SNMP пользователей

системы и определить метода проверки подлинности пользователей.

Чтобы открыть страницу [SNMPv3 User Security Model \(USM\)](#) (Модель USM протокола SNMP версии 3), выберите System (Система) → SNMP → User Security Model (Модель USM) на панели дерева.

Рис. 6-59. Страница SNMPv3 User Security Model (USM) (Модель USM протокола SNMP версии 3)



Страница [SNMPv3 User Security Model \(USM\)](#) (Модель USM протокола SNMP версии 3) содержит следующие поля.

Engine ID (Идентификатор механизма) - определяет удаленное устройство, поддерживающее протокол SNMP версии 3, к которому подключен выбранный пользователь.

Remote Engine ID (Идентификатор удаленного механизма) - показывает, что пользователь определен на удаленном устройстве, поддерживающем SNMP версии 3. Если определен идентификатор механизма, удаленные устройства получают уведомления.

User Name (Имя пользователя) - содержит список имен пользователя, определенных пользователем.

Group Name (Имя группы) - содержит список групп SNMP, определенных пользователем. Группы SNMP определяются на странице [Access Control Group](#) (Группа контроля доступа).

Authentication Method (Метод проверки подлинности) - определяет метод проверки подлинности, используемый для определения подлинности пользователей. Возможные значения:

None (Нет) - проверка подлинности пользователей не используется.

MD5 Password (Пароль MD5) - проверка пользователей осуществляется с использованием уровня проверки подлинности HMAC-MD5-96. Пользователь должен указать пароль.

SHA Password (Пароль SHA) - проверка пользователей осуществляется с использованием уровня проверки подлинности HMAC-SHA-96. Пользователь должен ввести пароль.

MD5 Key (Ключ MD5) - проверка подлинности пользователей осуществляется с использованием уровня проверки подлинности HMAC-MD5-96. Пользователь должен ввести ключи проверки подлинности и конфиденциальности данных.

SHA Key (Ключ SHA) - проверка подлинности пользователей осуществляется с использованием уровня HMAC-SHA-96. Пользователь должен ввести ключи проверки подлинности и конфиденциальности данных.

Password (0-32 Characters) (Пароль (0-32 символов)) - изменяет определенный пользователем пароль для группы. Пароли могут содержать не более 32 символов. Пароли определяются только при использовании метода проверки подлинности MD5 или SHA Password (Пароль MD5 или Пароль SHA).

Authentication Key (MD5-16; SHA-20 hexa chars) (Ключ проверки подлинности (MD5-16; SHA-20 шестнадцатеричных символов)) - определяет ключ проверки подлинности. Ключ проверки подлинности определяется только при использовании метода проверки подлинности MD5 Key (Ключ MD5) или SHA Key (Ключ SHA).

Privacy Key (16 hexa chars) (Ключ конфиденциальности (16 шестнадцатеричных символов)) - указывает пароль для проверки подлинности и генерации ключа DES для обеспечения конфиденциальности данных. Ключ конфиденциальности определяется только при использовании метода проверки подлинности MD5 Key (Ключ MD5) или SHA Key (Ключ SHA).

Remove (Удалить) - когда установлен этот флажок, удаляет указанного пользователя из указанной группы.

Добавление пользователей SNMP версии 3 в группу

1. Откройте страницу [SNMPv3 User Security Model \(USM\)](#) (Модель USM протокола SNMP версии 3).
2. Нажмите кнопку **Add** (Добавить).

Откроется страница [Add SNMPv3 User Name](#) (Добавление имени пользователя SNMP версии 3).

Рис. 6-60. Страница Add SNMPv3 User Name (Добавление имени пользователя SNMP версии 3)

The screenshot shows a web form titled "Add User Name". At the top right is a "Refresh" button. The form contains several input fields and a dropdown menu:

- Remove Entry (0-62 Hex Characters p4-1)
- User Name (1-32 Characters)
- Group Name
- Authentication Method: None
- Password (1-62 Characters)
- Authentication Key (MD5-16; SHA-20 Hex Characters p4-1)
- Privacy Key (16 Hex Characters p4-1)

At the bottom center is an "Apply Changes" button.

3. Определите соответствующие поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения).
5. Пользователь будет добавлен к группе, а устройство обновлено.

Просмотр таблицы USM (User Security Model)

1. Откройте страницу [SNMPv3 User Security Model \(USM\)](#) (Модель USM протокола SNMP версии 3).
2. Нажмите кнопку **Show All** (Показать все).

Откроется страница [SNMPv3 User Security Model Table](#) (Таблица модели USM протокола SNMP версии 3)

Рис. 6-61. Страница SNMPv3 User Security Model Table (Таблица модули USM протокола SNMP версии 3)

Reset

User Security Model Table

User Name	Group Name	Remote Engine	Authentication	Remove
-----------	------------	---------------	----------------	--------

Apply Changes

Удаление записи в таблице USM (User Security Model)

1. Откройте страницу [SNMPv3 User Security Model \(USM\)](#) (Модель USM протокола SNMP версии 3).
2. Нажмите кнопку **Show All** (Показать все).

Откроется страница [SNMPv3 User Security Model Table](#) (Таблица модели USM протокола SNMP версии 3)

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

Запись будет удалена, а устройство обновлено.

Определение пользователей SNMP с помощью команд консоли

В следующей таблице приведены команды консоли для определения полей, отображаемых на странице [SNMPv3 User Security Model \(USM\)](#) (Модель USM протокола SNMP версии 3).

Таблица 6-42. Команды консоли для определения пользователя SNMP

Команда консоли	Описание
<code>show snmp users [имя_пользователя]</code>	Отображает конфигурацию пользователей.

```

Console (config)# snmp-server user John auth-md5 1234

Console (config)# end

Console (config)# show snmp users

```

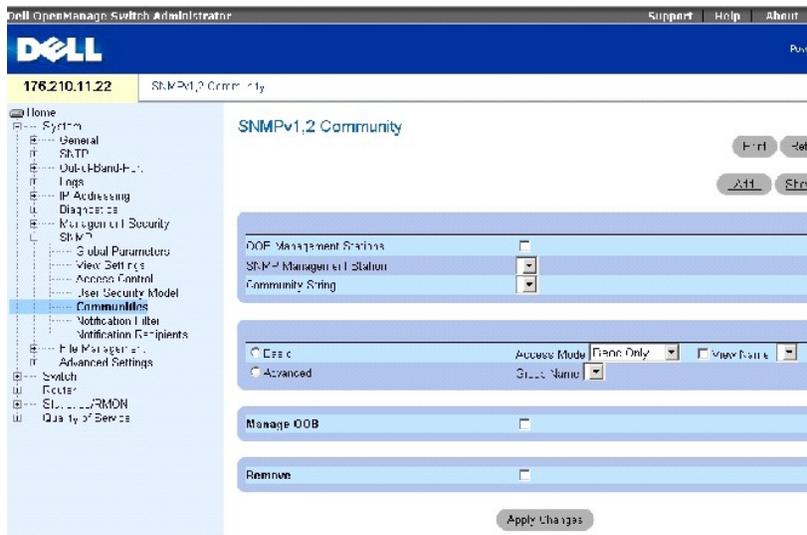
Name	Group Name	Auth Method	Remote
-----	-----	-----	-----
John	user-group	md5	

Определение сообщества

Управление правами доступа осуществляется путем определения сообществ на странице [SNMPv1,2 Community](#) (Сообщество SNMP версии 1 и 2). При изменении имен сообществ изменяются также и права доступа. Сообщества SNMP определяются только для протоколов SNMP версии 1 и SNMP версии 2.

Чтобы открыть страницу [SNMPv1,2 Community](#) (Сообщество SNMP версии 1, 2), выберите **System** (Система)→ **SNMP**→ **Communities** (Сообщества) на панели дерева.

Рис. 6-62. Страница SNMPv1,2 Community (Сообщество SNMP версии 1, 2)



Страница [SNMPv1,2 Community](#) (Сообщество SNMP версии 1, 2) содержит следующие поля.

OOB Management Station (Станция управления OOB) - установите этот флажок, чтобы создать отдельное сообщество SNMP для порта вне диапазона. Если этот флажок не установлен, доступ к устройству осуществляется со станции управления через порты внутри диапазона.

SNMP Management Station (Станция управления SNMP) - содержит список IP-адресов станции управления, для которой были определены строки сообщества.

ПРИМЕЧАНИЕ. Использовать одно и то же сообщество для настройки портов вне диапазона и внутри диапазона могут только привилегированные пользователи.

Community String (Строка сообщества) - содержит список строк сообщества, определенных пользователем, которые являются паролем и используются для проверки подлинности станции управления SNMP на устройстве. Строка сообщества может содержать не более 20 символов.

Basic (Основной) - включает режим SNMP Basic (Основной SNMP) для выбранного сообщества. Возможные значения:

Access Mode (Режим доступа) - определяет права доступа для сообщества. Возможные значения:

Read-Only (Только чтение) - доступ к управлению ограничивается доступом только для чтения, изменения сообщества невозможны.

Read-Write (Чтение и запись) - при доступе к управлению можно выполнять чтение и запись и вносить изменения в конфигурацию устройства, но не сообщества.

SNMP-Admin (Администратор SNMP) - пользователь имеет доступ ко всем параметрам конфигурации устройства, а также имеет право изменять сообщество.

View Name (Имя представления) - содержит список представлений SNMP, определенных пользователем.

Advanced (Расширенный) - содержит список групп, определенных пользователем. При выборе режима SNMP Advanced (Расширенный SNMP) правила контроля доступа SNMP, определенные для группы, будут включены для выбранного сообщества. В режиме Advanced (Расширенный) группы SNMP включаются для определенных сообществ SNMP. Режим SNMP Advanced (Расширенный SNMP) определяется только для протокола SNMP версии 3.

Manage OOB (Управление OOB) - если этот флажок установлен, управление SNMP станциями управления вне диапазона, подключенными к устройству, осуществляется только через порт вне диапазона.

Remove (Удалить) - когда установлен этот флажок, сообщество удаляется.

Определение нового сообщества

1. Откройте страницу [SNMPv1, 2 Community](#) (Сообщество SNMP версии 1, 2).
2. Нажмите кнопку **Add** (Добавить).

Откроется страница [Add SNMPv1,2 Community](#) (Добавление сообщества SNMP версии 1, 2).

Рис. 6-63. Страница Add SNMPv1,2 Community (Добавление сообщества SNMP версии 1, 2)

Refresh

Add SNMPv1,2 SNMP Community

OOB Management Stations

SNMP Management Station (0.0.0)

Community String (1-20 Characters)

Basic Access Mode: Read-Only View Name: Default

Advanced Group Name:

Manage OOB

Apply Changes

3. Заполните соответствующие поля.

В дополнение к полям на странице [SNMPv1, 2 Community](#) (Сообщество SNMP версии 1, 2) страница [Add SNMPv1,2 Community](#) (Добавление сообщества SNMP версии 1, 2) содержит поле **All (0.0.0.0)** (Все), которое указывает, определено ли сообщество SNMP для отдельной станции управления или для всех станций управления.

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

Новое сообщество будет сохранено, а устройство обновлено.

Удаление сообществ

1. Откройте страницу [SNMPv1, 2 Community](#) (Сообщество SNMP версия 1, 2).
2. Нажмите кнопку **Show All** (Показать все).

Откроется страница [SNMPv1, 2 Community Table](#) (Таблица сообщества SNMP версия 1, 2).

3. Выберите сообщество и установите флажок **Remove** (Удалить).
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Запись сообщества будет удалена, а устройство обновлено.

Настройка сообществ с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для определения полей, отображенных на странице [SNMPv1, 2 Community](#) (Сообщество SNMP версия 1, 2).

Таблица 6-43. Команды консоли для сообщества SNMP

Команда консоли	Описание
<code>snmp-server community community [ro rw su] [ip-адрес][view имя_представления][type {router oob}]</code>	Задаёт строку доступа сообщества для разрешения доступа по протоколу SNMP.
<code>snmp-server community-group community group-name [ip-адрес] [type {router oob}]</code>	Задаёт строку доступа сообщества для разрешения ограниченного доступа по протоколу SNMP на основе прав доступа группы.
<code>show snmp</code>	Отображает текущую конфигурацию устройства SNMP.

Далее приведен пример команд консоли:

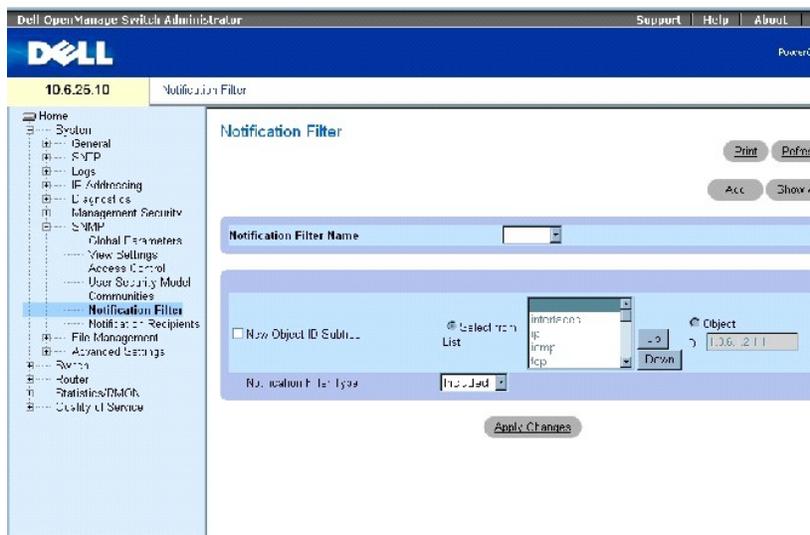
```
Console (config)# snmp-server community dell ro 10.1.1.1
```

Определение фильтров уведомлений SNMP

Страница [Notification Filter](#) (Фильтр уведомлений) разрешает фильтрацию системных прерываний на основе идентификаторов объекта (OID). Каждый идентификатор объекта (OID) связан с функцией или подфункцией устройства. С помощью страницы [Notification Filter](#) (Фильтр уведомлений) администраторы сети также могут осуществлять фильтрацию уведомлений.

Чтобы открыть страницу [Notification Filter](#) (Фильтр уведомлений), выберите **System** (Система) → **SNMP** → **Notification Filters** (Фильтры уведомлений) на панели дерева.

Рис. 6-64. Страница Notification Filter (Фильтр уведомлений)



Страница [Notification Filter](#) (Фильтр уведомлений) содержит следующие поля.

Notification Filter Name (Имя фильтра уведомлений) - содержит список фильтров уведомлений, определенных пользователем. Имя фильтра уведомлений может содержать не более 30 символов.

New Object Identifier Subtree (Новая ветвь идентификатора объекта) - идентификатор объекта, для которого отправляются или блокируются уведомления. Если к идентификатору объекта (OID) применяется фильтр, системные прерывания или сообщения генерируются и отправляются получателям системных прерываний. Идентификаторы объектов либо выбираются в окне *Select from List* (Выбор из списка), либо указываются в поле *Object ID* (Идентификатор объекта).

Notification Filter Type (Тип фильтра уведомлений) - указывает, какой вид уведомлений - сообщения или системные прерывания с учетом идентификатора объекта (OID) - отправляется получателю системных прерываний.

Excluded (Отправка исключена) - запрещает отправку системных прерываний или сообщений OID.

Included (Отправка включена) - отправляет системные прерывания или сообщения OID.

Добавление фильтров SNMP

1. Откройте страницу [Notification Filter](#) (Фильтр уведомлений).
2. Нажмите кнопку **Add** (Добавить).

Откроется страница [Add Filter](#) (Добавление фильтра)

Рис. 6-65. Страница Add Filter (Добавление фильтра)

Refresh

Add Notification Filter

Filter Name (1-255 Characters)

New Object Identifier Tree Object ID

Filter Type

Apply Changes

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

Новый фильтр будет добавлен, а устройство обновлено.

Отображение таблицы фильтров

1. Откройте страницу [Notification Filter](#) (Фильтр уведомлений).
2. Нажмите кнопку **Show All** (Показать все).

Откроется страница [Filter Table](#) (Таблица фильтров).

Рис. 6-66. Страница Filter Table (Таблица фильтров)

Filter Table

Refresh

Filter Name

Object Identifier Subtree	Filter Type	Remove
<input type="text"/>	<input type="text" value="Include"/>	<input type="checkbox"/>

Apply Changes

Удаление фильтра

1. Откройте страницу [Notification Filter](#) (Фильтр уведомлений).
2. Нажмите кнопку **Show All** (Показать все).

Откроется страница [Filter Table](#) (Таблица фильтров).

3. Выберите запись в [Filter Table](#) (Таблицу фильтров).
4. Установите флажок **Remove** (Удалить).

Запись фильтра будет удалена, а устройство обновлено.

Настройка фильтров уведомлений с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для определения полей, отображенных на странице [Notification Filter](#) (Фильтр уведомлений).

Таблица 6-44. Команды консоли для фильтров уведомлений SNMP

Команда консоли	Описание
<code>snmp-server filter имя_фильтра oid-tree {included excluded}</code>	Создает или обновляет фильтр уведомлений SNMP.
<code>show snmp filters [имя_фильтра]</code>	Отображает конфигурацию фильтров уведомлений SNMP.

Далее приведен пример команд консоли:

Console (config)# snmp-server filter user1 1 included											
Console(config)# end											
Console # show snmp filters											
<table border="1"> <thead> <tr> <th>Name</th> <th>OID Tree</th> <th>Тип</th> </tr> </thead> <tbody> <tr> <td>-----</td> <td>-----</td> <td>-----</td> </tr> <tr> <td>user1</td> <td>iso</td> <td>Included</td> </tr> </tbody> </table>			Name	OID Tree	Тип	-----	-----	-----	user1	iso	Included
Name	OID Tree	Тип									
-----	-----	-----									
user1	iso	Included									

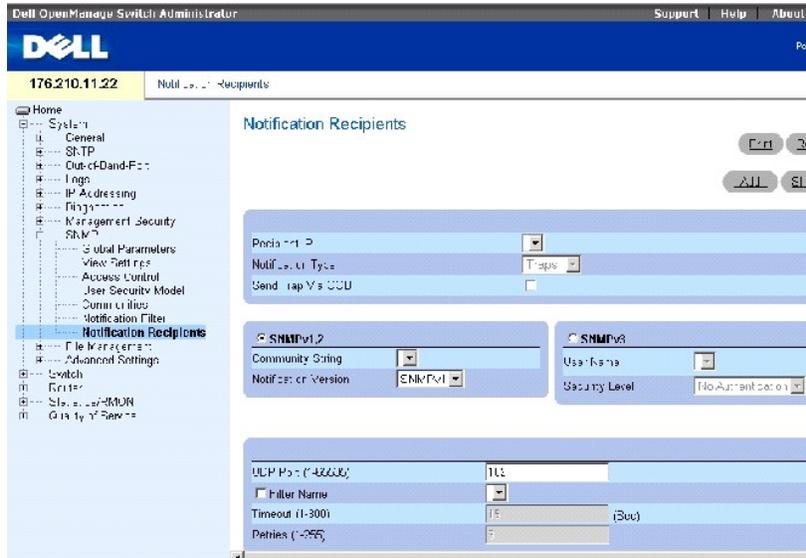
Определение получателей уведомлений SNMP

На странице [Notification Recipients](#) (Получатели уведомлений) представлена информация по настройке фильтров, которые указывают, отправляются ли системные прерывания определенным пользователям, а также тип системных прерываний. Фильтры уведомлений SNMP выполняют следующие функции.

- 1 Определение объектов системных прерываний управления
- 1 Фильтрация системных прерываний
- 1 Выбор параметров генерации системных прерываний
- 1 Обеспечение проверок контроля доступа

Чтобы открыть страницу [Notification Filter](#) (Фильтр уведомлений), выберите System (Система)→ SNMP→ Notification Recipient (Получатель уведомлений) на панели дерева.

Рис. 6-67. Страница Notification Recipients (Получатели уведомлений)



Страница [Notification Recipients](#) (Получатели уведомлений) содержит следующие поля.

Recipient IP (IP получателя) - содержит IP-адреса получателей уведомлений, определенных пользователем.

Notification Type (Тип уведомлений) - тип отправленного уведомления. Возможные значения:

Trap (Системное прерывание) - отправляются системные прерывания.

Inform (сообщение) - отправляются сообщения.

SNMPv1,2 (SNMP версия 1, 2) - для выбранного получателя включен протокол SNMP версии 1 или 2. Возможные значения:

Community String (Строка сообщества) - содержит список строк сообщества. Выберите одну строку для отправки с уведомлением.

Notification Version (Версия уведомления) - определяет версию уведомления. Возможные значения:

SNMP V1 - отправляются системные прерывания SNMP версии 1.

SNMP V2 - отправляются системные прерывания или сообщения SNMP версии 2.

SNMPv3 - для выбранного получателя включен протокол SNMP версии 3. Возможные значения:

User Name (Имя пользователя) - содержит список пользователей. Выберите одного, чтобы генерировать уведомления.

Security Level (Уровень безопасности) - уровень безопасности, применяемый к уведомлениям. Возможные значения:

No Authentication (Нет проверки подлинности) - не производится ни проверка подлинности, ни шифрование пакета.

Authentication (Проверка подлинности) - производится проверка подлинности пакета.

Privacy (Конфиденциальность) - производится и проверка подлинности и шифрование пакета.

UDP Port (1-65535) (Порт UDP) - порт UDP, используемый для отправки уведомлений. Значение по умолчанию: 162.

Filter Name (Имя фильтра) - установите этот флажок, чтобы применить к уведомлениям фильтр SNMP, определенный пользователем, и выбрать фильтр SNMP из списка.

Timeout (1-300) (Тайм-аут) - время ожидания устройства (в секундах) перед повторной отправкой сообщений. Значение по умолчанию: 15 секунд.

Retries (1-255) (Повторные попытки) - максимальное число повторных попыток отправки устройством запросов. Значение по умолчанию: 3.

Remove Notification Recipient (Удаление получателя уведомлений) - когда установлен этот флажок, удаляет выбранного получателя уведомлений.

Добавление нового получателя уведомлений

1. Откройте страницу [Notification Recipients](#) (Получатели уведомлений).
2. Нажмите кнопку **Add** (Добавить).

Откроется страница [Add Notification Recipient](#) (Добавление получателя уведомлений).

Рис. 6-68. Страница Add Notification Recipient (Добавление получателя уведомлений)

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

Получатель уведомлений будет добавлен, а устройство обновлено.

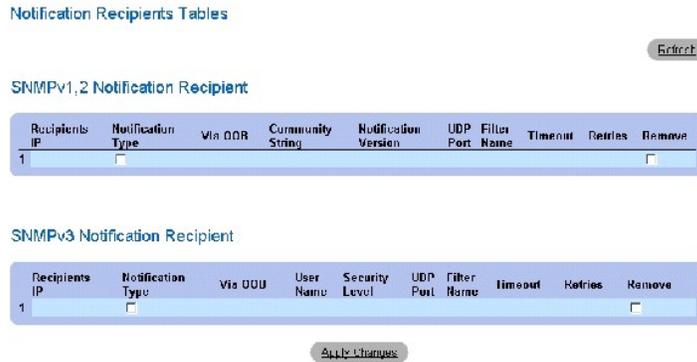
Отображение таблиц получателей уведомлений

1. Откройте страницу [Notification Recipients](#) (Получатели уведомлений).

2. Нажмите кнопку **Show All** (Показать все).

Откроется страница [Notification Recipients Table](#) (Таблица получателей уведомлений).

Рис. 6-69. Страница Notification Recipients Table (Таблица получателей уведомлений)



Удаление получателей уведомлений

1. Откройте страницу [Notification Recipients](#) (Получатели уведомлений).
2. Нажмите кнопку **Show All** (Показать все).

Откроется страница Notification Recipients Table (Таблица получателей уведомлений).

3. Выберите одного или более получателей уведомлений в таблице **SNMPV1,2 Notification Recipient** (Получатель уведомлений SNMP версии 1, 2) и/или **SNMPv3 Notification Recipient** (Получатель уведомлений SNMP версии 3).
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Получатели будут удалены, а устройство обновлено.

Определение получателей уведомлений SNMP с помощью команд консоли

В следующей таблице приведены команды консоли для определения полей, отображаемых на странице [Notification Recipients](#) (Получатели уведомлений).

Таблица 6-45. Команды консоли для определения получателей уведомлений SNMP

Команда консоли	Описание
<code>snmp-server host {ip-адрес имя_хоста} community-string [traps informs] [1 2] [udp-port номер_порта] [filter имя_фильтра] [timeout секунды] [retries число_попыток]</code>	Создает или обновляет получателя уведомлений SNMP версий 1 или 2.
<code>snmp-server v3-host {ip-адрес имя_хоста} имя_пользователя [traps informs] {noauth auth priv} [udp-port номер_порта] [filter имя_фильтра] [timeout секунды] [retries число_попыток]</code>	Создает или обновляет получателя уведомлений SNMP версии 3.

Далее приведен пример команд консоли:

```
Console (config)# snmp-server host 12.1.1.1 Dell-community
```

Console (config)# end

console# show snmp

Community-String	Community-Access	View name	IP address	Тип
-----	-----	-----	-----	----
Community-String	Group name	IP address	Тип	
-----	-----	-----	----	

OOB management stations

Community-String	Community-Access	View name	IP address	Тип
-----	-----	-----	-----	----
Community-String	Group name	IP address	Тип	
-----	-----	-----	----	

Traps are enabled.

Authentication-failure trap is enabled.

Version 1,2 notifications

Target Address	Тип	Community	Version	Udp Port	Filter name	To Sec	Retries
-----	----	-----	-----	-----	-----	---	-----
12.1.1.1	Trap	Dell_community	2	162		1500	3

OOB Notification Receivers

Target Address	Тип	Community	Version	Udp Port	Filter name	To Sec	Retries

-----	---	-----	----	----	-----	---	-----
Version 3 notifications							
Target Address	Тип	Username	Security Level	Udp Port	Filter name	To Sec	Retries
-----	---	-----	----	----	-----	---	-----
OOB Notification Receivers							
Target Address	Тип	Username	Security Level	Udp Port	Filter name	To Sec	Retries
-----	---	-----	----	----	-----	---	-----

Управление файлами

Для управления программным обеспечением устройства, файлами образов и файлами настройки используйте страницу **File Management** (Управление файлами). Файлы можно передавать или загружать через сервер TFTP.

Обзор управления файлами

Управление файловой структурой состоит из следующих элементов:

- 1 **Startup configuration file** (Файл настройки для запуска) - сохраняет полную настройку устройства при отключении или перезагрузке устройства. Файл для запуска хранит команды настройки, и в нем можно сохранить команды настройки из файла рабочей настройки.
- 1 **Running configuration file** (Файл рабочей настройки) - содержит все команды файла для запуска, а также все команды, введенные во время текущего сеанса. После отключения или перезагрузки устройства все команды, сохраненные в файле рабочей настройки, теряются. В ходе запуска все команды файла для запуска копируются в файл рабочей настройки и применяются к устройству. Во время сеанса все новые введенные команды добавляются к существующим командам файла рабочей настройки. Команды не переписываются. Чтобы изменить файл запуска, нужно перед отключением устройства скопировать файл рабочей настройки в файл настройки для запуска. Тогда при следующем запуске устройства команды копируются обратно в файл рабочей настройки из файла настройки для запуска.
- 1 **Backup Configuration File** (Резервный файл настройки) - содержит резервную копию настройки устройства. Резервный файл настройки изменяется, когда в него копируется файл рабочей настройки или файл для запуска. Копируемые в файл команды заменяют существующие команды, сохраненные в резервном файле. Содержимое резервного файла можно скопировать либо в файл рабочей настройки, либо в файл настройки запуска.
- 1 **Image Files** (Файлы образа - системные образы) - System images - сохраняются в двух секторах Flash, называемых образами (Image 1 и Image 2). Активный образ хранит активную копию, другой образ - вторую копию. Устройство загружается и запускается из активного образа. Если активный образ поврежден, система автоматически загружается из неактивного образа. Эта функция безопасности для сбоя, происходящих в процессе обновления программы загрузки.

Чтобы открыть страницу **File Management** (Управление файлами), выберите **System** (Система) → **File Management** (Управление файлами) на панели дерева.

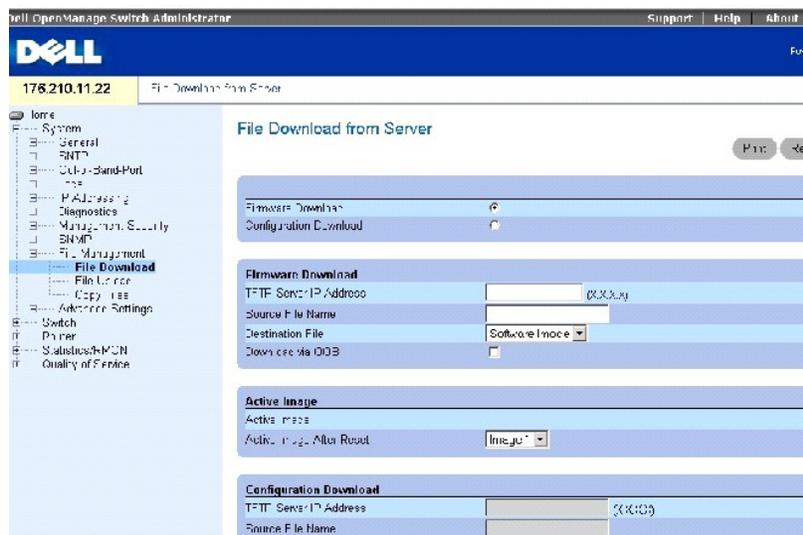
Загрузка файлов

Страница [File Download from Server](#) (Загрузка файлов с сервера) содержит поля для загрузки программного обеспечения с сервера TFTP на устройство. Файл образа, также может быть загружен со страницы **File Download from Server** (Загрузка файлов с сервера).

Чтобы открыть страницу [File Download From Server](#) (Загрузка файлов с сервера), выберите **System** (Система) → **File Management** (Управление

файлами)→ File Download (Загрузка файла) на панели дерева.

Рис. 6-70. Страница File Download from Server (Загрузка файлов с сервера)



Страница [File Download From Server](#) (Загрузка файлов с сервера) содержит следующие поля.

Firmware Download (Загрузка микропрограммы) - когда выбран этот параметр, будет загружаться файл микропрограммы. Если выбран этот параметр, поля **Configuration Download** (Загрузка настройки) недоступны.

Configuration Download (Загрузка настройки) - когда выбран этот параметр, будет загружаться файл настройки. Если выбран параметр **Configuration Download** (Загрузка настройки), поля **Firmware Download** (Загрузка микропрограммы) недоступны.

Firmware TFTP Server IP Address (IP-адрес сервера TFTP для загрузки микропрограмм) - IP-адрес сервера TFTP, с которого загружаются файлы.

Firmware Source File Name (Имя исходного файла микропрограммы) - файл микропрограммы для загрузки.

Firmware Destination File (Файл назначения для микропрограммы) - определяет, в какой файл будет загружен файл: в файл образа или загрузочный файл.

Firmware Download via OOB (Загрузка микропрограммы через OOB) - загружает микропрограмму через порт управления вне диапазона.

Active Image (Активный образ) - текущий активный файл образа.

Active Image After Reset (Активный образ после перезагрузки) - файл образа, который станет активным после перезагрузки устройства. Возможные значения:

Image 1 - файл Image 1 будет активен после перезагрузки устройства.

Image 2 - файл Image 2 будет активен после перезагрузки устройства.

Configuration File TFTP Server IP Address (IP-адрес сервера TFTP для файла настройки) - IP-адрес сервера TFTP, с которого загружаются файлы настройки.

Configuration File Source File Name (Имя файла источника для файла настройки) - файл настройки, который необходимо загрузить.

Configuration File Destination (Целевой файл настройки) - файл, в который будет загружен файл настройки. Возможные значения:

Running Configuration (Рабочая настройка) - загружает файлы рабочей настройки.

Startup Configuration (Настройка для запуска) - загружает файлы настройки запуска.

Backup Configuration (Резервная настройка) - загружает резервные файлы настройки.

Configuration Download via OOB (Загрузка настройки через OOB) - загружает файлы настройки через порт управления вне диапазона.

Загрузка файлов

1. Откройте страницу [File Download from Server](#) (Загрузка файлов с сервера).
2. Проверьте IP-адрес сервера TFTP и убедитесь, что образ программы или загрузочный файл доступны для загрузки с этого сервера TFTP.
3. Заполните поля **TFTP Server IP Address** (IP-адрес сервера TFTP), **Source File Name** (Имя файла источника) (полный путь без IP-адреса сервера TFTP) и **Destination File** (Целевой файл) (образ программы или загрузочный образ).

 **ПРИМЕЧАНИЕ.** Образ из файла заменяет неактивный образ. Рекомендуется определить неактивный образ, который станет активным после сброса, а затем выполнить сброс устройства после загрузки.

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

Программное обеспечение будет загружено на устройство.

Активизация файла образа

1. Откройте страницу [File Download from Server](#) (Загрузка файлов с сервера).
2. Выберите образ, который необходимо активизировать, в раскрывающемся меню **Active Image After Reset** (Активный образ после перезагрузки).
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Файл образа будет выбран.

 **ПРИМЕЧАНИЕ.** Для активизации выбранного файла образа перезагрузите устройство. Подробнее о перезагрузке устройства см. в разделе «[Восстановление заводских параметров устройства](#)».

Загрузка файлов с сервера с помощью команд консоли

В следующей таблице приведены команды консоли для определения полей, отображаемых на странице [File Download From Server](#) (Загрузка файлов с сервера).

Таблица 6-46. Команды консоли для загрузки

Команда консоли	Описание
<code>copy url_источника url_приемника</code>	Копирует файл из исходного местоположения в место назначения.

Firmware Upload (Передача микропрограммы) - когда параметр выбран, передается файл микропрограммы. Если выбран параметр **Firmware Upload** (Передача микропрограммы), поля **Configuration Upload** (Передача настройки) недоступны.

Configuration Upload (Передача настройки) - когда параметр выбран, передается файл настройки. Если выбран параметр **Configuration Upload** (Передача настройки), поля **Firmware Upload** (Передача микропрограммы) недоступны.

Software Image Upload TFTP Server IP Address (IP-адрес сервера TFTP для передачи образа программы) - IP-адрес сервера TFTP, на который передается образ программы.

Software Image Upload Destination (Место назначения передачи образа программы) - путь к файлу образа программы, куда передается файл.

Software Image Upload via OOB (Передача образа программы через OOB) - указывает, что образ программы будет передаваться через порт управления вне диапазона.

Configuration Upload TFTP Server IP Address (IP-адрес сервера TFTP для передачи настройки) - IP-адрес сервера TFTP, на который передается файл настройки.

Configuration Upload Destination (Место назначения передачи настройки) - определяет путь к файлу настройки, куда выполняется передача файла.

Configuration Upload Transfer File Name (Имя передаваемого файла настройки) - программный файл, в который выполняется передача настройки. Возможные значения этого поля:

Running Configuration (Рабочая настройка) - передает текущий файл настройки.

Startup Configuration (Настройка для запуска) - передает файлы настройки для запуска.

Backup Configuration (Резервная настройка) - передает файлы резервной настройки.

Configuration Upload via OOB (Выгрузка настройки через OOB) - указывает, что передача файлов настройки осуществляется через порт управления вне диапазона.

Передача файлов на сервер

1. Откройте страницу [File Upload to Server](#) (Передача файлов на сервер).
2. Определите требуемые поля на странице.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Программное обеспечение будет загружено на сервер.

Передача файлов на сервер с помощью команд консоли

В следующей таблице приведены команды консоли, для определения полей, отображенных на странице [File Upload to Server](#) (Передача файлов на сервер).

Таблица 6-47. Команды консоли для передачи файлов

Команда консоли	Описание
<code>copy url_источника url_приемника</code>	Копирует файл из исходного местоположения в место назначения.

Далее приведен пример команды консоли:

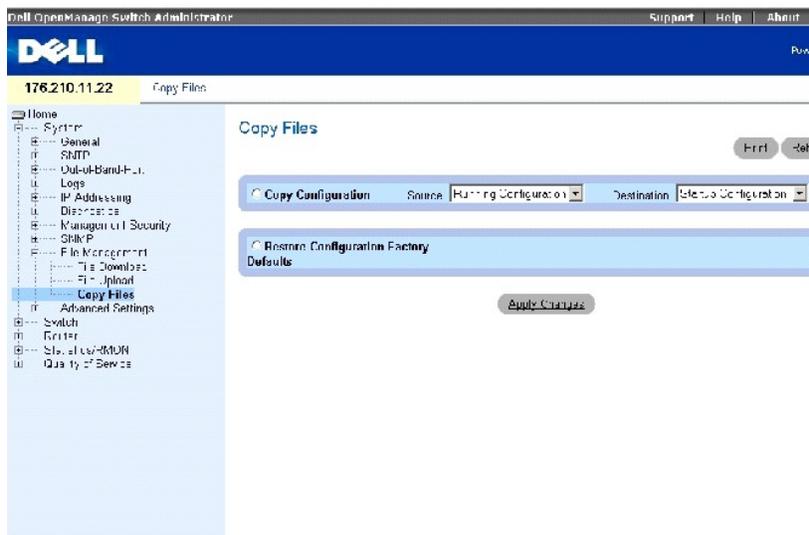
```
console#copy image tftp:16.1.1.200/file1
```

Копирование файлов

Используйте страницу [Copy Files](#) (Копировать файлы) для копирования и восстановления настроек по умолчанию.

Чтобы открыть страницу [Copy Files](#) (Копирование файлов), выберите **System** (Система) → **File Management** (Управление файлами) → **Copy** (Копирование) на панели дерева.

Рис. 6-72. Страница Copy Files (Копирование файлов)



Страница [Copy Files](#) (Копирование файлов) содержит следующие поля.

Copy Configuration (Копирование настройки) - определяет файл настройки, который должен быть скопирован.

Source (Исходный) - исходный файл, из которого копируются настройки (рабочая, запуска, резервная).

Destination (Целевой) - целевой файл, в который копируются настройки (запуска, резервная).

Restore Configuration Factory Defaults (Восстановить заводские файлы настройки) - когда выбран этот параметр, восстанавливаются заводские файлы настройки по умолчанию. Если параметр не выбран, используются текущие параметры настройки.

ПРИМЕЧАНИЕ. При копировании файлов в текущую настройку добавляются только данные настройки, сам файл не заменяется.

Копирование файлов

1. Откройте страницу [Copy Files](#) (Копирование файлов).
2. Выберите **Copy** (Копировать) или **Restore** (Восстановить) и заполните поля.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Файл будет скопирован.

Копирование файлов с помощью команд консоли

В следующей таблице приведены команды консоли для определения полей, отображаемых на странице [Copy Files](#) (Копирование файлов).

Таблица 6-48. Команды консоли для копирования файлов

Команда консоли	Описание
<code>copy url_источника url_приемника</code>	Копирует файл из исходного местоположения в место назначения.
<code>delete startup-config</code>	Удаляет файл настройки для запуска.

Далее приведен пример команд консоли.

```
console# delete startup-config
```

Определение расширенных параметров

Расширенные параметры используются для настройки прочих глобальных атрибутов устройства. Изменения для этих атрибутов применяются только после сброса устройства. Выберите **System** (Система) → **Advanced Settings** (Расширенные параметры) на панели дерева, чтобы открыть страницу **Advanced Settings** (Расширенные параметры).

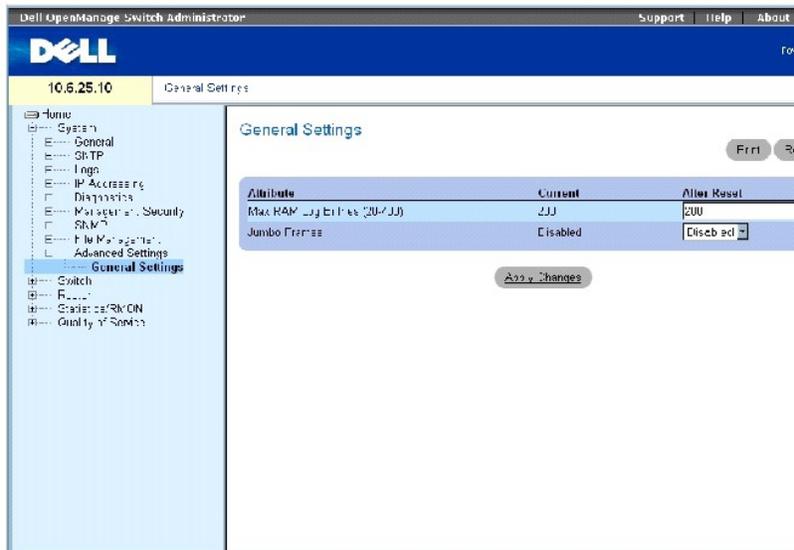
Страница **Advanced Settings** (Расширенные параметры) содержит ссылки для настройки общих параметров.

Настройка общих параметров

Используйте страницу [General Settings](#) (Общие параметры), чтобы определить общие параметры устройства.

Чтобы открыть страницу [General Settings](#) (Общие параметры), выберите **System** (Система) → **Advanced Settings** (Расширенные параметры) → **General** (Общие) на панели дерева.

Рис. 6-73. Страница General Settings (Общие параметры)



Страница [General Settings](#) (Общие параметры) содержит следующие поля.

Current (Текущее) - максимальное число записей.

After Reset (После перезагрузки) - максимальное число записей после перезагрузки устройства. При вводе значения в столбце выделяется память для поля таблицы.

Max RAM Log Entries (20-400) (Максимальное число записей журнала ОЗУ) - максимальное число записей в таблице журнала ОЗУ. Значение по умолчанию - 200 записей.

Jumbo Frames (Большие кадры) - разрешает передачу тех же данных, но меньшим числом пакетов. Это уменьшает объем служебной информации, время обработки и перерывы. Можно включить внутренние кадры, включив большие кадры.

Включение поддержки больших пакетов

1. Откройте страницу [General Settings](#) (Общие параметры).
2. Выберите значение **Enabled** (Включено) в поле **Jumbo packets** (Большие пакеты).
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Поддержка больших пакетов включена для устройства.

Просмотр общих параметров с помощью команд консоли

В следующей таблице приведены команды консоли для определения полей, отображаемых на странице [General Settings](#) (Общие параметры).

Таблица 6-49. Команды консоли для определения общих параметров

Команда консоли	Описание
logging buffered size <i>число</i>	Задаёт число системных сообщений, хранящихся во внутреннем буфере (ОЗУ).

```
port jumbo-frame
```

Включает поддержку больших кадров для устройства.

Далее приведен пример команд консоли.

```
Console (config)# logging buffered size 300
```

```
Console (config)#port jumbo-frame
```

[Назад на страницу Содержание](#)

[Назад на страницу Содержание](#)

Информация о настройке коммутатора

Системы Dell™ PowerConnect™ 6024/6024F

- [Настройка безопасности сети](#)
- [Настройка портов](#)
- [Настройка адресных таблиц](#)
- [Настройка протокола GARP](#)
- [Настройка протокола STP](#)
- [Настройка сетей VLAN](#)
- [Объединение портов](#)
- [Поддержка пересылки многоадресного трафика](#)

В этом разделе описаны все системные операции и приведены общие сведения о настройке безопасности сети, портов, адресных таблиц, протокола GARP, групп VLAN, протокола STP, объединения портов и многоадресной поддержке.

Настройка безопасности сети

Используйте страницу **Network Security** (Безопасность сети) для настройки безопасности сети с помощью списков управления доступом и заблокированных портов. Чтобы открыть страницу **Network Security** (Безопасность сети), выберите **Switch** (Коммутатор) → **Network Security** (Безопасность сети).

На странице **Network Security** (Безопасность сети) приведены ссылки, позволяющие настроить проверку подлинности на основе порта, безопасность портов, ACL, основанные на IP-адресах, ACL, основанные на MAC-адресах и привязки ACL.

Проверка подлинности на основе порта (802.1x)

Проверка подлинности на основе порта обеспечивает проверку подлинности пользователей системы на основе портов через внешний сервер. Только прошедшие проверку подлинности и одобренные пользователи системы могут передавать и принимать данные. Проверка подлинности портов выполняется с помощью сервера RADIUS, использующего протокол EAP (Extensible Authentication Protocol).

Сеть 802.1x состоит из трех компонентов, указанных ниже.

- 1 **Удостоверения** - определяет порт, для которого выполняется проверка подлинности перед разрешением доступа к системе.
- 1 **Просители** - указывает хост, подключенный к проверенному порту, запрашивающему доступ к службам системы.
- 1 **Сервер проверки подлинности** - указывает внешний сервер, например сервер RADIUS, который выполняет проверку подлинности от имени администратора, а также указывает, может ли пользователь получить доступ к службам системы.

Проверка подлинности на основе портов формирует два состояния доступа.

- 1 **Controlled Access** (Управляемый доступ) - разрешает связь между пользователем и системой, если пользователь прошел проверку.
- 1 **Uncontrolled Access** (Неконтролируемый доступ) - разрешает неконтролируемый обмен данными независимо от состояния порта.

Устройство в настоящее время поддерживает проверку подлинности на основе порта с помощью серверов RADIUS.

Расширенная проверка подлинности на основе порта

Расширенная проверка подлинности на основе порта позволяет нескольким хостам подключаться к одному порту. Расширенная проверка подлинности на основе порта требует авторизации только одного хоста, чтобы доступ к системе имели все хосты. Если порт не проходит авторизацию, всем подключенным хостам будет отказано в доступе к сети.

Расширенная проверка подлинности на основе порта позволяет использовать проверку подлинности на основе группы VLAN. Определенные группы VLAN в коммутаторе всегда являются доступными, даже если порты, подключенные к группе VLAN, не прошли авторизацию. Например, для передачи голоса по IP не требуется проверка подлинности, а для трафика передачи данных требуется. Можно определить группы VLAN, для которых не требуется проверка подлинности. Непрошедшие проверку группы VLAN доступны для пользователей, даже если порты, подключенные к группе VLAN, определены как проверенные.

Расширенная проверка подлинности на основе порта реализована в следующих режимах.

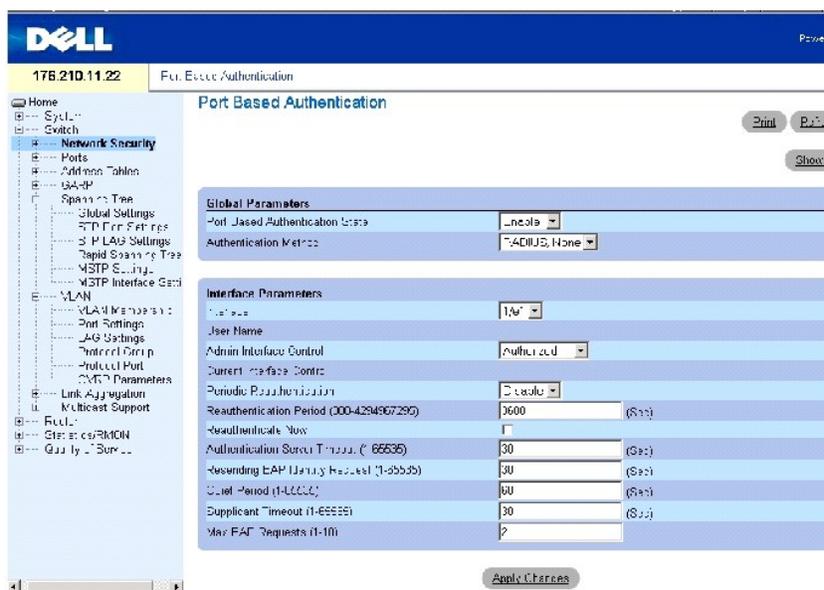
- 1 **Single Host Mode** (Режим одного хоста) - разрешает доступ к порту только проверенному хосту.
- 1 **Multiple Host Mode** (Режим нескольких хостов) - позволяет нескольким хостам подключаться к одному порту. Требуется авторизация только одного хоста, чтобы доступ к сети имели все хосты. В случае неудачной проверки подлинности хоста или появления сообщения выхода EAPOL доступ запрещается для всех подключенных клиентов.

Настройка проверки подлинности на основе порта

Страница [Port Based Authentication](#) (Проверка подлинности на основе порта) содержит поля для настройки проверки подлинности на основе порта.

Чтобы открыть страницу [Port Based Authentication](#) (Проверка подлинности на основе порта), выберите **Switch** (Коммутатор) → **Network Security** (Безопасность сети) → **Port Based Authentication** (Проверка подлинности на основе порта).

Рис. 7-1. Страница Port Based Authentication (Проверка подлинности на основе порта)



Страница [Port Based Authentication](#) (Проверка подлинности на основе порта) содержит следующие поля:

Port Based Authentication State (Состояние проверки подлинности на основе порта) - позволяет выполнять проверку подлинности на основе порта для устройства. Возможные значения:

Enable (Включено) - выполняется проверка подлинности на основе порта для устройства.

Disable (Выключено) - отключена проверка подлинности на основе порта для устройства.

Authentication Method (Метод проверки подлинности) - используемый метод проверки подлинности. Возможные значения:

RADIUS, None (RADIUS, Нет) - сообщает, что проверка подлинности на основе порта сначала выполняется на сервере RADIUS. Если сервер RADIUS недоступен, метод проверки подлинности не используется. Однако, если произойдет сбой, то порт останется неавторизованным и доступ не будет получен.

RADIUS - сообщает, что проверка подлинности выполняется на сервере RADIUS.

None (Нет) - сообщает, что метод проверки подлинности не используется.

Interface (Интерфейс) - содержит список интерфейсов для проверки подлинности.

User Name (Имя пользователя) - имя пользователя, настроенное на сервере RADIUS.

Admin Interface Control (Управление интерфейсом) - определяет состояние авторизации порта. Возможные значения:

Auto (Авто) - позволяет использовать проверку подлинности каждого порта. Авторизация интерфейса включается или выключается в зависимости от обмена данными между устройством и клиентом в ходе проверки подлинности.

Authorized (Авторизован) - устанавливает интерфейс в состояние авторизации без проверки подлинности. Интерфейс посылает и получает нормальный трафик без проверки подлинности клиента на основе порта.

Unauthorized (Неавторизован) - запрещает доступ к выбранной системе интерфейса и переводит интерфейс в неавторизованное состояние. Устройство не обеспечивает проверку подлинности клиента через интерфейс.

Current Interface Control (Текущее управление интерфейсом) - текущее состояние авторизации порта. Звездочка отображается, если порт в данный момент не работает.

Periodic Reauthentication (Периодическое повторение проверки подлинности) - для выбранного порта, если это возможно, выполняется периодическая проверка подлинности.

Reauthentication Period (300-4294967295) (Период повторения проверки подлинности) - определяет время, по истечении которого для выбранного порта будет выполнена повторная проверка подлинности. Значение этого поля указывается в секундах. Значение по умолчанию: 3600 секунд.

Reauthenticate Now (Немедленная повторная проверка подлинности) - выполняет повторную проверку подлинности выбранного порта.

Authentication Server Timeout (1-65535) (Время ответа сервера проверки подлинности) - определяет время, которое проходит, прежде чем устройство посылает повторный запрос серверу проверки подлинности. Значение этого поля указывается в секундах. Значение по умолчанию: 30 секунд.

Resending EAP Identity Request (1-65535) (Повторная отправка запроса EAP) - определяет время до повторной отправки запроса EAP. Значение этого поля указывается в секундах. Значение по умолчанию: 30 секунд.

Quiet Period (1-65535) (Период молчания) - определяет время, в течение которого устройство остается в состоянии молчания после обмена данными в ходе неудачной проверки подлинности. Возможные значения поля: 0-65535. Значение этого поля указывается в секундах. Значение по умолчанию: 60 секунд.

Supplicant Timeout (1-65535) (Тайм-аут просителя) - определяет время до повторной отправки запросов EAP пользователю. Значение этого поля указывается в секундах. Значение по умолчанию: 30 секунд.

Max EAP Requests (1-10) (Максимальное число запросов EAP) - максимальное число попыток отправки запросов EAP перед возобновлением процесса проверки подлинности, если устройство не получает ответ. Возможные значения поля: 1-10. Значение по умолчанию: 2 попытки.

Отображение таблицы проверки подлинности на основе порта

1. Откройте страницу [Port Based Authentication](#) (Проверка подлинности на основе порта).
2. Нажмите кнопку **Show All** (Показать все).

Откроется страница [Port Based Authentication Table](#) (Таблица проверки подлинности на основе порта).

Рис. 7-2. Таблица Port Based Authentication Table (Таблица проверка подлинности на основе порта)

Port Based Authentication Table Refresh

Port	User Name	Admin Port Control	Current Port Control	Periodic Reauthentication	Reauthentication Period	Reauthenticate Now <small>(select All)</small>	Authenticator State
1 g1		Authorized		Enable		<input type="checkbox"/>	
2 g2		Authorized		Enable		<input type="checkbox"/>	

Apply Changes

Таблица [Port Based Authentication Table](#) (Таблица проверки подлинности на основе порта) содержит следующие поля:

Copy Parameters From Port No. (Копировать параметры из порта №) - порт, из которого копируются параметры.

Termination Cause (Причина завершения) - причина, по которой была завершена проверка подлинности на основе порта.

Copy To (Копировать в) - копирование параметров одного порта в выбранные порты.

Select All (Все порты) - выбор всех портов в таблице [Port Based Authentication Table](#) (Таблица проверки подлинности на основе порта).

Копирование параметров в таблицу [Port Based Authentication Table](#) (Таблица проверки подлинности на основе порта)

1. Откройте страницу [Port Based Authentication](#) (Проверка подлинности на основе порта).
2. Нажмите кнопку **Show All** (Показать все).

Откроется страница [Port Based Authentication Table](#) (Таблица проверки подлинности на основе порта).

3. Выберите интерфейс в поле **Copy Parameters from** (Копировать параметры из).
4. Установите флажок **Copy to** (Копировать в), чтобы определить интерфейс, для которого будут скопированы параметры проверки подлинности на основе порта.
5. Нажмите кнопку **Apply Changes** (Применить изменения).

Параметры будут скопированы в порт выбранный в таблице [Port Based Authentication Table](#) (Таблица проверки подлинности на основе порта), а устройство обновлено.

Включение проверки подлинности на основе порта с использованием команд консоли

В следующей таблице приведены команды консоли для включения проверки подлинности на основе порта, соответствующие полям на странице [Port Based Authentication](#) (Проверка подлинности на основе порта).

Таблица 7-1. Команды консоли для проверки подлинности на основе порта

Команда консоли	Описание
<code>aaa authentication dot1x default метод1 [метод2.]</code>	Указывает один или несколько методов проверки подлинности, авторизации и учета (AAA), используемые на интерфейсах IEEE 802.1X.
<code>dot1x system-auth- control</code>	Глобальное включение 802.1X.
<code>dot1x port-control {auto force- authorized force- unauthorized}</code>	Управление состоянием авторизации порта вручную.
<code>dot1x max-req число</code>	Устанавливает максимальное число попыток отправки запросов EAP клиенту перед возобновлением процесса проверки подлинности.
<code>dot1x re-authenticate [ethernet интерфейс]</code>	Инициализирует ручную повторную проверку подлинности всех портов, поддерживающих 802.1X или указанного порта, поддерживающего 802.1X.
<code>dot1x re- authentication</code>	Включает периодические повторные проверки подлинности клиента.
<code>dot1x timeout quiet-period секунды</code>	Устанавливает число секунд, в течение которых устройство остается в состоянии молчания после обмена данными в ходе неудачной проверки подлинности.
<code>dot1x timeout re-authperiod секунды</code>	Устанавливает число секунд между попытками повторной проверки подлинности.
<code>dot1x timeout server-timeout секунды</code>	Устанавливает время повторной передачи пакетов на сервер проверки подлинности.
<code>dot1x timeout supp-timeout секунды</code>	Устанавливает время для повторной отправки кадра запроса EAP клиенту.
<code>dot1x timeout tx- period секунды</code>	Устанавливает число секунд, в течение которых устройство ожидает ответа на запрос EAP от клиента перед повторной отправкой запроса.
<code>show dot1x [ethernet интерфейс]</code>	Отображает состояние 802.1X для устройства или указанного интерфейса.
<code>show dot1x users [username имя_пользователя]</code>	Отображает пользователей 802.1X для устройства.
<code>show dot1x statistics ethernet интерфейс</code>	Отображает статистику 802.1X для указанного интерфейса.

Далее приведен пример команд консоли.

```

Console# show dot1x

```

Port	Admin Mode	Oper Mode	Reauth Control	Reauth Period	Username
----	-----	-----	-----	-----	-----
g11	Auto	Authorized	Ena	3600	Bob
g12	Auto	Authorized	Ena	3600	John
g13	Auto	Unauthorized	Ena	3600	Clark

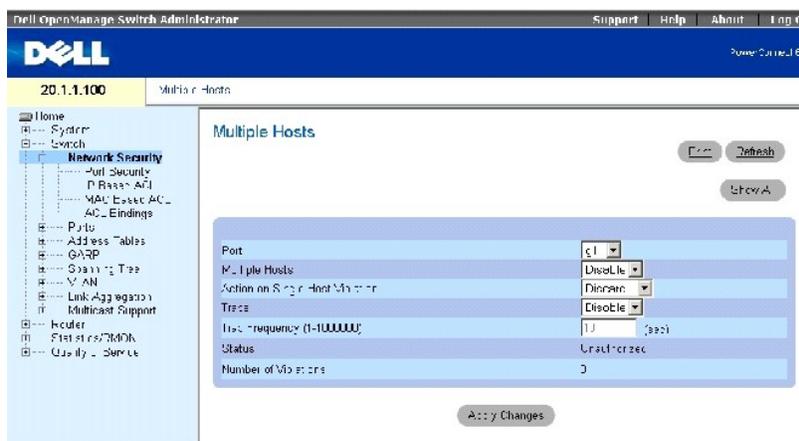
g14	Force-auth	Authorized	Dis	3600	n/a
-----	------------	------------	-----	------	-----

Настройка расширенной проверки подлинности на основе порта

Страница [Multiple Hosts](#) (Несколько хостов) содержит информацию, позволяющую определить параметры расширенной проверки подлинности на основе порта для определенных портов.

Чтобы открыть страницу [Multiple Hosts](#) (Несколько хостов), выберите **Switch** (Коммутатор) → **Network Security** (Безопасность сети) → **Multiple Hosts** (Несколько хостов).

Рис. 7-3. Страница Multiple Hosts (Несколько хостов)



Страница [Multiple Hosts](#) (Несколько хостов) содержит следующие поля:

Port (Порт) - номер порта, для которого включен режим расширенной проверки подлинности на основе порта.

Multiple Hosts (Несколько хостов) - включает или отключает один хост для авторизации нескольких хостов для доступа к системе. Этот параметр необходимо включить, чтобы отключить фильтрацию на входе или использовать защиту блокировки для выбранного порта.

Action on Single Host Violation (Действие при нарушении доступа одного хоста) - определяет действие, которое необходимо применять для пакетов, поступающих в режиме одного хоста от хоста, MAC-адрес которого отличается от MAC-адреса клиента (просителя). Возможные значения:

Forward (Переслать) - пересылает пакет от неизвестного источника, но MAC-адреса не распознаются.

Discard (Отвергнуть) - отбрасывает пакеты от любого неизвестного источника. Это значение по умолчанию.

Discard Shutdown (Игнорировать завершение работы) - отбрасывает пакеты от любого неизвестного источника и блокирует порт. Порты останутся выключенными, пока не будет выполнена их активизация или сброс устройства.

Traps (Системные прерывания) - включает или отключает отправку системных прерываний на хост в случае нарушения доступа.

Trap Frequency (1-1000000) (Частота системных прерываний) - определяет временной интервал между отправками системных прерываний на хост. Значение по умолчанию: 10 секунд.

Status (Состояние) - состояние хоста. Возможные значения:

Unauthorized (Неавторизован) - означает, что управление портом является *Force Unauthorized* (Принудительно не авторизовано), соединение порта закрыто или порт управляется автоматически (Auto), но проверка подлинности клиента не была произведена через порт.

Not in auto mode (Автоматический режим отключен) - указывает, что управление портом является *Forced Authorized* (Принудительно авторизовано) и клиенты имеют полный доступ к порту.

Single-host Lock (Блокировка одного хоста) - указывает, что портом управляется автоматически (Auto) и была произведена проверка подлинности одного клиента через порт.

No Single Host (Не один хост) - указывает, что включен параметр Multiple Host (Несколько хостов).

Number of Violations (Число нарушений) - число пакетов, поступивших на интерфейс в режиме одного хоста от хоста, MAC-адрес которого отличается от MAC-адреса клиента (просителя).

Отображение таблицы [Multiple Hosts Table](#) (Таблица нескольких хостов)

1. Откройте страницу [Multiple Hosts](#) (Несколько хостов).
2. Нажмите кнопку **Show All** (Показать все).

Откроется страница [Multiple Hosts Table](#) (Таблица нескольких хостов).

Рис. 7-4. Страница Multiple Hosts Table (Таблица нескольких хостов)

Port	Enable Multiple Hosts	Action on Violation	Enable Traps	Trap Frequency	Status	Number of Violations
1	<input type="checkbox"/>	Discard	<input type="checkbox"/>			

Включение нескольких хостов с использованием команд консоли

В следующей таблице приведены команды консоли для включения расширенной проверки подлинности на основе порта, соответствующие полям на странице [Multiple Hosts](#) (Несколько хостов).

Таблица 7-2. Команды консоли для нескольких хостов

Команда консоли	Описание
<code>dot1x multiple-hosts</code>	Разрешает наличие нескольких хостов (клиентов) на проверяемом порту 802.1X, для которых в команде настройки интерфейса <code>dot1x port-control</code> установлено значение <code>auto</code> .
<code>dot1x single-host-violation {forward discard discard- shutdown}[trap секунды]</code>	Настраивает действие, которое необходимо выполнить, когда станция, MAC-адрес которой отличается от MAC-адреса клиента (просителя), осуществляет попытку доступа к интерфейсу.

Далее приведен пример команды консоли.

```
Console(config)# interface ethernet g11  
  
Console(config-if)# dot1x multiple-hosts
```

Проверка подлинности пользователей

Страница [Authenticated Users](#) (Проверяемые пользователи) отображает список доступа пользователей к портам.

Чтобы открыть страницу [Authenticated Users](#) (Проверка подлинности пользователей), **выберите** Switch (Коммутатор)→ Network Security (Безопасность сети)→ [Authenticated Users](#) (Проверка подлинности пользователей).

Рис. 7-5. Страница Authenticated Users (Проверка подлинности пользователей)



Страница [Authenticated Users](#) (Проверка подлинности пользователей) содержит следующие поля:

User Name (Имя пользователя) - список пользователей, авторизированных с использованием сервера RADIUS.

Port (Порт) - отображает номера портов, используемых для проверки подлинности. Порты отображаются по имени пользователя.

Session Time (Время сеанса) - время с момента входа пользователя на устройство. Формат поля **дни:часы:минуты:секунды**, например 3 дня: 2 часа: 4 минуты: 39 секунд.

Authentication Method (Метод проверки подлинности) - метод, использовавшийся при последней проверке подлинности. Возможные значения:

Remote (Удаленно) - проверка подлинности пользователя выполняется на удаленном сервере.

None (Нет) - проверка подлинности пользователя не выполнялась.

MAC Address (MAC-адрес) - MAC-адрес посетителя.

Отображение таблицы проверки подлинности пользователей

1. Откройте страницу [Authenticated Users](#) (Проверка подлинности пользователей).
2. Нажмите кнопку **Show All** (Показать все).

Откроется страница [Authenticated Users Table](#) (Таблица проверки подлинности пользователей):

Рис. 7-6. Страница Authenticated Users Table (Таблица проверки подлинности пользователей)

Authenticated Users Table Refresh

User Name	Port	Session Time	Authentication Method	MAC Address
1				

Отображение проверки подлинности пользователей с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для проверки подлинности пользователей, соответствующие полям на странице [Authenticated Users](#) (Проверка подлинности пользователя).

Таблица 7-3. Команды консоли для добавления имени пользователя

Команда консоли	Описание
<code>show dot1x users [username имя_пользователя]</code>	Отображает пользователей 802.1X для устройства.

Далее приведен пример команд консоли.

Console# show dot1x users				
Port	Username	Session Time	Auth Method	MAC Address
----	-----	-----	-----	-----
g12	bob	00:09:27	Remote	00:80:c8:b9:dc:1d

Настройка безопасности портов

Безопасность сети можно повысить, если разрешить доступ к определенным портам только пользователям с определенными MAC-адресами. MAC-адреса определяются динамически в процессе подключения или настраиваются статически. Функция безопасности блокировки портов проверяет полученные пакеты и определяет, откуда был получен пакет для определенных портов. Доступ к заблокированным портам разрешается только пользователям с определенными MAC-адресами. Эти адреса вводятся вручную для порта или определяются при попытке доступа к заблокированному порту. Когда заблокированный порт получает пакет, и MAC-адрес источника пакета не связан с этим портом (определен на другом порте или неизвестен системе), активизируется механизм защиты и могут быть выполнены различные действия. Несанкционированные пакеты, поступающие на заблокированный порт, пересылаются, игнорируются без системного прерывания, игнорируются с системным прерыванием или входной порт отключается.

Функция безопасности **Locked Port** (Заблокированный порт) позволяет сохранить список MAC-адресов в файле конфигурации. Этот список MAC-адресов можно восстановить после перезагрузки устройства.

Отключенные порты можно активизировать только на странице [Port Configuration](#) (Настройка порта).

Чтобы открыть страницу [Port Security](#) (Безопасность портов), выберите **Switch** (Коммутатор)→ **Network Security** (Безопасность сети)→ **Port Security** (Безопасность портов).

Рис. 7-7. Страница Port Security (Безопасность портов)



Interface (Интерфейс) - указывает, включена ли функция безопасности блокировки портов или LAG.

Current Port Status (Текущее состояние порта) - указывает, что в настоящий момент порт заблокирован, отключен или разблокирован.

Set Port (Установка порта) - включает блокировку порта. Если порт заблокирован, все текущие адреса, которые динамически определяются коммутатором для этого порта, преобразуются в статические MAC-адреса. Если порт разблокирован, они удаляются из статического списка.

Action on Violation (Действие при нарушении) - действие, применяемое к пакетам, поступившим на порт. если порт разблокирован, поле отображается серым цветом. Возможные значения:

Discard (Отвергнуть) - отбрасывает пакеты от любого неизвестного источника. Это значение по умолчанию.

Forward (Переслать) - пересылает пакеты от неизвестного источника. MAC-адрес для них не определяется.

Shutdown (Завершить работу) - отбрасывает пакеты от любого неизвестного источника и отправляет системное прерывание. Кроме того, входной порт отключается.

Trap (Прерывание) - включает или отключает отправку системных прерываний при получении пакета на заблокированный порт.

Trap Frequency (Частота системных прерываний) - время в секундах, которое проходит между системными прерываниями.

Определение заблокированного порта

1. Откройте страницу [Port Security](#) (Безопасность портов).
2. Выберите тип и номер интерфейса.
3. В раскрывающемся меню **Set Port** (Установка порта) выберите значение **Locked** (Заблокирован).
4. Заполните необходимые поля.

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

Заблокированный порт будет добавлен в Port Security Table (Таблицу безопасности портов), а устройство обновлено.

Копирование параметров в таблицу заблокированных портов

1. Откройте страницу [Port Security](#) (Безопасность портов).
2. Нажмите кнопку **Show All** (Показать все), чтобы отобразить страницу **Port Security Table** (Таблица безопасности портов).

Поля страницы Port Security Table (Таблица безопасности портов) соответствуют полям на странице **Port Security** (Безопасность портов).

3. В поле **Copy Parameters from** (Копировать параметры из) выберите интерфейс в раскрывающемся меню **Port** (Порт) или **LAG**.

Параметры безопасности портов, определенные для этого интерфейса, будут скопированы в выбранный интерфейс, см. шаг 5.

4. Установите флажок **Copy to** (Копировать в) для выбора интерфейсов, в которые будут скопированы определения безопасности портов.

ИЛИ

Нажмите **Select All** (Выбрать все) для копирования определений во все порты или группы LAG.

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

Параметры будут скопированы в выбранные порты или группы LAG в **Port Security Table** (Таблица безопасности портов), а устройство обновлено.

Настройка безопасности заблокированных портов с помощью команд консоли

В следующей таблице приведены команды консоли для настройки функции безопасности заблокированных портов, соответствующие полям на странице [Port Security](#) (Безопасность портов).

Таблица 7-4. Команды консоли для настройки безопасности заблокированных портов

Команда консоли	Описание
<code>port security [forward discard discard-shutdown] [trap секунды]</code>	Запрещает новые адреса, определенные для интерфейса.
<code>show ports security [ethernet интерфейс port-channel номер_канала_порта]</code>	Отображает состояние блокировки для порта.

Далее приведен пример команд консоли.

```
Console(config)# interface ethernet g1

Console (config-if)# port security forward trap 100

Console (config-if)# exit
```

```
Console (config)# exit
```

```
Console# show ports security
```

Port	status	Action	Trap	Frequency	Counter
----	-----	-----	----	-----	-----
g1	Locked	Forward	Enabled	100	0
g2	Unlocked	-	-	-	-
...					
g24	Unlocked	-	-	-	-
ch1	Unlocked	-	-	-	-
...					
ch7	Unlocked	-	-	-	-

Определение списков ACL, основанных на IP-адресах

Списки управления доступом (ACL) позволяют сетевым администраторам определять классификационные действия и правила для определенных входных портов. Коммутатор поддерживает до 1024 списков ACL. Пакеты, поступающие на входной порт с активным списком ACL, пропускаются или отбрасываются и входной порт отключается. Если они отбрасываются, пользователь может отключить порт.

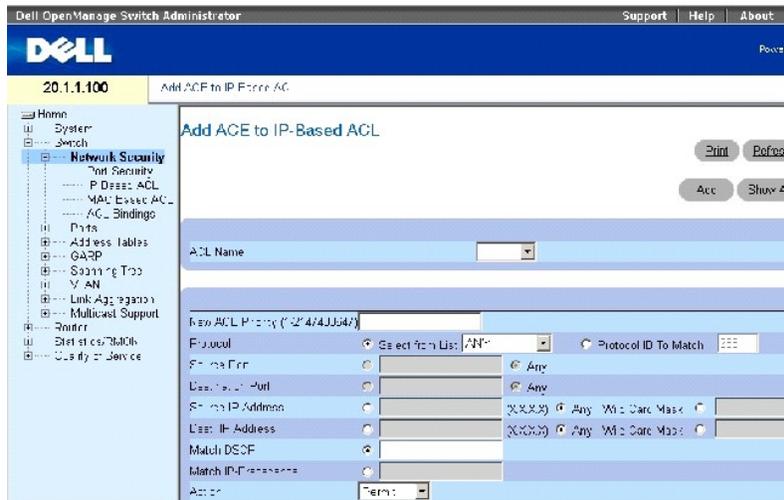
Например, администратор сети может определить правило ACL, которое устанавливает, что порт с номером 20 может получать пакеты TCP, но если будет получен пакет UDP, этот пакет будет отброшен.

Списки ACL состоят из элементов управления доступом (ACE), которые создают фильтры, определяющие классификации трафиков. Во всех списках ACL может быть определено 1024 записи ACE.

Используйте страницу [Add ACE to IP Based ACL](#) (Добавление ACE в ACL, основанный на IP-адресах) для определения записи ACE основанной на IP-адресе.

Чтобы открыть страницу [Add ACE to IP Based ACL](#) (Добавление ACE в ACL, основанный на IP-адресах), выберите **Switch** (Коммутатор) → **Network Security** (Безопасность сети) → **IP Based ACL** (ACL на основе IP).

Рис. 7-8. Добавление ACE в ACL, основанный на IP-адресах



Страница [Add ACE to IP Based ACL](#) (Добавление ACE в ACL, основанный на IP-адресах) содержит следующие поля:

ACL Name (Имя ACL) - определенный пользователем список ACL.

New ACE Priority (Новый приоритет ACE) - приоритет ACE, определяющий, какая запись ACE соответствует пакету на основе схемы первого совпадения.

Protocol (Протокол) - включает создание новой записи ACE, основанной на определенном протоколе.

Select from List (Выбор из списка) - щелкните, чтобы выбрать из списка протокол, на котором может быть основана запись ACE.

Protocol ID To Match (Идентификатор протокола для сопоставления) - щелкните, чтобы добавить определенный пользователем протокол, пакеты которого будут сопоставляться с записью ACE.

 **ПРИМЕЧАНИЕ.** Для выбора всех протоколов используйте значение «any».

Source Port (Порт-источник) - исходный порт TCP/UDP. Это поле активно только в том случае, если выбрано значение 800/6-TCP или 800/17-UDP в раскрывающемся меню **Select from List** (Выбор из списка).

Destination Port (Порт-приемник) - порт назначения TCP/UDP. Это поле активно только в том случае, если выбрано значение 800/6-TCP или 800/17-UDP в раскрывающемся меню **Select from List** (Выбор из списка).

Source IP Address (IP-адрес источника) - сопоставляет IP-адрес исходного порта, на который адресованы пакеты, с записью ACE.

Wild Card Mask (Маски ввода) - маска ввода IP-адреса источника. Маски ввода указывают, какие биты используются, а какие игнорируются. Маска ввода 255.255.255.255 указывает, что никакие биты не важны. Маска ввода 0.0.0.0 указывает, что все биты важны.

Dest. IP Address (IP-адрес назначения) - сопоставляет IP-адрес порта назначения, на который адресованы пакеты, с записью ACE.

Wild Card Mask (Маска ввода) - маска ввода для IP-адреса назначения. Выберите **Match DSCP** (Соответствие DSCP) или **Match IP Precedence** (Соответствие приоритету IP):

Match DSCP (Соответствие DSCP) - сопоставляет значение пакетов DSCP с записью ACE. При сравнении пакетов с записями ACL используется значение DSCP или значение приоритета пакета IP.

Match IP Precedence (Соответствие приоритета IP) - сопоставляет значение приоритета IP-пакетов с записью ACE. При сравнении пакетов с записями ACL используется значение DSCP или значение приоритета пакета IP.

Action (Действие) - операция передачи для ACL. Возможные значения:

Permit (Разрешить) - пересылает пакеты, отвечающие критериям ACL.

Deny (Запретить) - отбрасывает пакеты, отвечающие критериям ACL.

Shutdown (Завершение работы) - отбрасывает пакет, отвечающий критериям ACL, и отключает порт, на который он был адресован. Порты можно снова активизировать на странице **Ports Configuration** (Настройка портов), см. раздел [«Определение настройки портов»](#).

Чтобы просмотреть все ACE, связанные с ACL, нажмите **Show All** (Показать все).

Добавление в ACL, основанный на IP-адресах

1. Откройте страницу [Add ACE to IP Based ACL](#) (Добавление ACE в ACL, основанный на IP-адресах).
2. Щелкните **Add** (Добавить), чтобы отобразить страницу [Add IP Based ACL](#) (Добавление ACL, основанного на IP-адресах).

Рис. 7-9. Добавление ACL, основанного на IP-адресах

The screenshot shows the 'Add IP Based ACL' configuration interface. It includes a title bar, an 'ACL Name' field, a 'New ACE Priority' checkbox and input field, a 'Protocol' dropdown menu (set to 'Any') and a 'Protocol ID To Match' input field, 'Source Port' and 'Destination Port' input fields, 'Source IP Address' and 'Dest IP Address' input fields with 'Wild Card Mask' input fields, 'Match DSCP' and 'Match IP Precedence' input fields, and an 'Action' dropdown menu (set to 'Permit'). An 'Apply Changes' button is located at the bottom of the form.

3. Введите значение в поле **ACL Name** (Имя ACL).
4. Установите флажок **New ACE Priority** (Новый приоритет ACE) и введите значения во все поля на странице.
5. Нажмите кнопку **Apply Changes** (Применить изменения).

Список ACL, основанный на IP-адресах, будет определен, а устройство обновлено.

Изменение записи ACE, основанной на IP-адресах

ПРИМЕЧАНИЕ. Запись ACE может быть изменена, только когда список ACL, в котором она находится, не связан с интерфейсом.

1. Откройте страницу [Add ACE to IP Based ACL](#) (Добавление ACE в ACL, основанный на IP-адресах).
2. Нажмите кнопку **Show All** (Показать все) для отображения всех записей ACE в списке ACL.
3. Выберите нужный список ACL в поле **ACL Name** (Имя ACL).
4. Выполните необходимые изменения в полях.
5. Нажмите кнопку **Apply Changes** (Применить изменения).

Запись ACE, основанная на IP-адресах, будет изменена, а устройство обновлено.

Добавление новой записи ACE в список ACL, основанный на IP-адресах

1. Откройте страницу [Add ACE to IP Based ACL](#) (Добавление ACE в ACL, основанный на IP-адресах).
2. Выберите нужный список ACL в поле **ACL Name** (Имя ACL).
3. Определите поля в диалоговом окне.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Запись ACE будет присвоена списку ACL, основанному на IP-адресах.

5. Нажмите кнопку **Apply Changes** (Применить изменения) и укажите новые параметры для дополнительных записей ACE в существующем списке ACL.

Изменение порядка записей ACE в ACL

1. Откройте страницу [Add ACE to IP Based ACL](#) (Добавление ACE в ACL, основанный на IP-адресах) и выберите необходимый список ACL в раскрывающемся меню **ACL Name** (Имя ACL).
2. Нажмите кнопку **Show All** (Показать все).

Откроется страница **ACEs Associated with IP-ACL** (Записи ACE, связанные с ACL, основанным на IP-адресах).

3. Введите значение приоритета для необходимой сортировки записей ACE.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Порядок записей ACE будет изменен, а устройство обновлено.

Удаление списков ACL

1. Откройте страницу [Add ACE to IP Based ACL](#) (Добавление ACE в ACL, основанный на IP-адресах) и выберите необходимый список ACL в раскрывающемся меню **ACL Name** (Имя ACL).
2. Нажмите кнопку **Show All** (Показать все).

Откроется страница **ACEs Associated with IP-ACL** (Записи ACE, связанные с ACL, основанным на IP-адресах).

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

Список ACL, основанный на IP-адресах, будет удален, а устройство обновлено.

Назначение записей ACE, основанных на IP-адресах, для списков ACL с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли, позволяющие назначить записи ACE, основанные на IP-адресах, спискам ACL, как показано на странице [Add ACE to IP Based ACL](#) (Добавление ACE в ACL, основанный на IP-адресах).

Таблица 7-5. Команды консоли для назначения записей ACE, основанных на IP-адресах, для списков ACL

Команда консоли	Описание
<code>ip access-list ИМЯ</code>	Создает списки ACL, основанные на IP-адресах, и включает режим настройки списка доступа, основанного на IP-адресах.
	Разрешает трафик, если соблюдены условия,

<code>permit {any протокол} {any source маска_ввода_источника} {any destination маска_ввода_назначения} [dscp dscp номер ip-precedence приоритет_ip_пакета]</code>	определенные в операторе permit.
<code>deny [disable-port] {any протокол} {any source маска_ввода_источника} {any destination маска_ввода_назначения} [dscp dscp номер ip-precedence приоритет_ip_пакета]</code>	Запрещает трафик, если соблюдены условия, определенные в операторе deny.
<code>show access-lists [имя]</code>	Отображает списки управления доступом, определенные на коммутаторе.

Далее приведен пример команд консоли.

```
Console (config)# ip access-list Dell
```

```
Console (config-ip-al)# permit rsvp 12.1.1.1 0.0.0.0 any dscp 56
```

```
Console (config-ip-al)# deny any 192.1.1.10 0.0.0.255 any
```

```
Console# show access-lists
```

```
IP access list one
```

```
permit ip host 12.1.1.1 any
```

```
permit rsvp host 176.30.40.1 any
```

```
Console# show access-lists
```

```
IP access list Dell
```

```
permit rsvp 12.1.1.1 0.0.0.0 any dscp 56
```

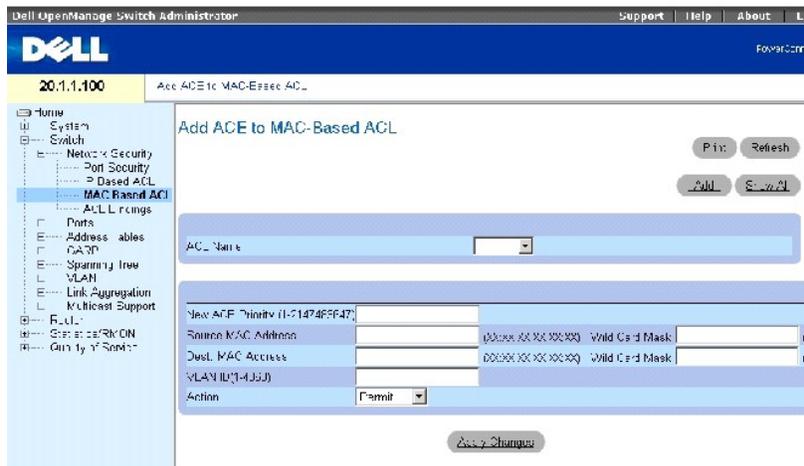
```
deny any 192.1.1.10 0.0.0.255 any
```

Определение списков ACL, основанных на MAC-адресах

На странице [Add ACE to MAC Based ACL](#) (Добавление ACE в ACL, основанный на MAC-адресах) администраторы сети могут определить список ACL, основанный на MAC-адресах. Описание списков ACL см. в разделе «[Определение списков ACL, основанных на IP-адресах](#)».

Чтобы открыть страницу [Add ACE to MAC Based ACL](#) (Добавление ACE в ACL, основанный на MAC-адресах), выберите Switch (Коммутатор) → Network Security (Безопасность сети) → MAC based ACL (ACL, основанный на MAC-адресах).

Рис. 7-10. Добавление ACE в ACL, основанный на MAC-адресах



Страница [Add ACE to MAC Based ACL](#) (Добавление ACE в ACL, основанный на MAC-адресах) содержит следующие поля:

ACL Name (Имя ACL) - список ACL, определенный пользователем.

New ACE Priority (Новый приоритет ACE) - приоритет ACE, определяющий, какой ACE соответствует пакету на основе схемы первого совпадения.

Source MAC Address (MAC-адрес источника) - сопоставляет MAC-адрес источника, с которого адресованы пакеты, с записью ACE.

Wild Card Mask (Маска ввода) - маска ввода для MAC-адреса источника. Подстановочные символы используются для замены всего MAC-адреса источника или его части. Маски ввода указывают, какие биты используются, а какие игнорируются. Маска ввода FF:FF:FF:FF:FF:FF показывает, что нет важных битов. Маска ввода 00:00:00:00:00:00 указывает, что все биты важны. Например, если MAC-адрес источника - E0:3B:4A:C2:CA:E2, а маска ввода - 00:3B:4A:C2:CA:FF, то используются первые два бита MAC-адреса, а последние два игнорируются.

Destination MAC Address (MAC-адрес назначения) - сопоставляет MAC-адрес назначения, куда адресованы пакеты, с записью ACE.

Wild Card Mask (Маска ввода) - маска ввода для MAC-адреса назначения. Подстановочные символы используются для замены всего MAC-адреса назначения или его части.

VLAN ID (Идентификатор сети VLAN) - сопоставляет идентификатор сети VLAN пакета с записью ACE. Возможные значения: 1-4094.

Action (Действие) - указывает операцию передачи для ACL. Возможные значения этого поля:

Permit (Разрешить) - пересылает пакеты, отвечающие критериям ACL.

Deny (Запретить) - отбрасывает пакеты, отвечающие критериям ACL.

Shutdown (Завершение работы) - отбрасывает пакет, отвечающий критериям ACL, и отключает порт, на который он был адресован. Порты можно снова активизировать на странице [Ports Configuration](#) (Настройка портов), см. раздел «[Определение настройки портов](#)».

Добавление ACL, основанного на MAC-адресах

1. Откройте страницу [Add ACE to MAC Based ACL](#) (Добавление ACE в ACL, основанный на MAC-адресах).

- Щелкните **Add** (Добавить), чтобы открыть страницу [Add MAC Based ACL](#) (Добавление ACL, основанного на MAC-адресах).

Рис. 7-11. Добавление ACL, основанного на MAC-адресах

Add MAC Based ACL Refresh

ACL Name

New ACE Priority [1-214/4096] ▾

Source MAC Address [XXXXXXXXXX] Wild Card Mask [XXXXXXXXXX]

Dest MAC Address [XXXXXXXXXX] Wild Card Mask [XXXXXXXXXX]

VLAN ID [4093/4095]

Action [Permit ▾]

- Введите значение в поле **ACL Name** (Имя ACL).
- Для добавления записи ACE в созданный список ACL установите флажок **New ACE Priority** (Новый приоритет ACE) и определите поля **Source MAC addresses** (MAC-адрес источника), **Destination MAC addresses** (MAC-адрес назначения), **VLAN ID** (Идентификатор VLAN) и **Action** (Действие).
- Нажмите кнопку **Apply Changes** (Применить изменения).

Список ACL, основанный на MAC-адресах, будет определен, а устройство обновлено.

Изменение записи ACE, основанной на MAC-адресах

- Откройте страницу [Add ACE to MAC Based ACL](#) (Добавление ACE в ACL, основанный на MAC-адресах).
- Выберите нужный список ACL в поле **ACL Name** (Имя ACL).
- Измените необходимые поля.
- Нажмите кнопку **Apply Changes** (Применить изменения).

Поля будут изменены, а устройство обновлено.

Добавление ACE в список ACL, основанный на MAC-адресах

ПРИМЕЧАНИЕ. Запись ACE может быть добавлена только в том случае, если список ACL не связан с интерфейсом.

- Откройте страницу [Add ACE to MAC Based ACL](#) (Добавление ACE в ACL, основанный на MAC-адресах).
- Выберите нужный список ACL в поле **ACL Name** (Имя ACL).
- Определите поля **New ACE Priority** (Новый приоритет ACE), **Source MAC addresses** (MAC-адрес источника), **Destination MAC addresses** (MAC-адрес назначения), **VLAN ID** (Идентификатор VLAN) и **Action** (Действие).
- Нажмите кнопку **Apply Changes** (Применить изменения).

Запись ACE будет присвоена списку ACL, основанному на MAC-адресах.

ПРИМЕЧАНИЕ. Для добавления записи ACE в существующий список ACL нажмите кнопку **Apply Changes** (Применить изменения) и укажите новые параметры записи ACE.

Отображение записей ACE из списка ACL

- Откройте страницу [Add ACE to MAC Based ACL](#) (Добавление ACE в ACL, основанный на MAC-адресах).
- Нажмите кнопку **Show All** (Показать все) для отображения страницы **ACEs Associated with MAC ACL** (Записи ACE, связанные с ACL, основанным на MAC-адресах).

Удаление списков ACL

 **ПРИМЕЧАНИЕ.** Список ACL может быть удален только в том случае, если он не связан с интерфейсом.

1. Выберите ACL.
2. Откройте страницу [Add ACE to MAC Based ACL](#) (Добавление ACE в ACL, основанный на MAC-адресах).
3. Нажмите кнопку **Show All** (Показать все) для отображения страницы **ACEs Associated with MAC ACL** (Записи ACE, связанные с ACL, основанным на MAC-адресах).
4. Установите флажок **Remove ACL** (Удалить ACL).
5. Нажмите кнопку **Apply Changes** (Применить изменения).

Список ACL, основанный на MAC- адресах, будет удален, а устройство обновлено.

Удаление записи ACE из списка ACL

1. Выберите ACL.
2. Откройте страницу [Add ACE to MAC Based ACL](#) (Добавление ACE в ACL, основанный на MAC-адресах).
3. Нажмите кнопку **Show All** (Показать все) для отображения страницы **ACEs Associated with MAC ACL** (Записи ACE, связанные с ACL, основанным на MAC-адресах).
4. Установите флажок **Remove ACE** (Удалить ACE) в строке ACE, которую необходимо удалить.
5. Нажмите кнопку **Apply Changes** (Применить изменения).

Список ACL, основанный на MAC- адресах, будет удален, а устройство обновлено.

Назначение записей ACE, основанных на MAC-адресах, для списков ACL с помощью команд консоли

В следующей таблице приведены команды консоли, позволяющие назначить записи ACE, основанные на MAC-адресах, спискам ACL, как показано на странице [Add ACE to MAC Based ACL](#) (Добавление ACE в ACL, основанный на MAC-адресах).

Таблица 7-6. Команды консоли для записей ACE, основанных на MAC-адресах

Команда консоли	Описание
<code>mac access-list имя</code>	Создает списки ACL, основанные на MAC-адресах, на уровне 2 и включает режим настройки списка доступа, основанного на MAC-адресах.
<code>permit {any host source маска_ввода_источника} {any destination маска_ввода_назначения}[vlan идентификатор-vlan]</code>	Разрешает трафик, если соблюдены условия, определенные в операторе permit.
<code>deny [disable-port] {any source маска_ввода_источника} {any destination маска_ввода_назначения}[vlan идентификатор-vlan]</code>	Запрещает трафик, если соблюдены условия, определенные в операторе deny.
<code>show access-lists [имя]</code>	Отображает списки управления доступом, настроенные на коммутаторе.

Далее приведен пример команд консоли.

```
Console (config)# mac access-list dell
```

```
Console (config-mac-a1)# permit 6:6:6:6:6:6 0:0:0:0:0:0 any vlan 4
```

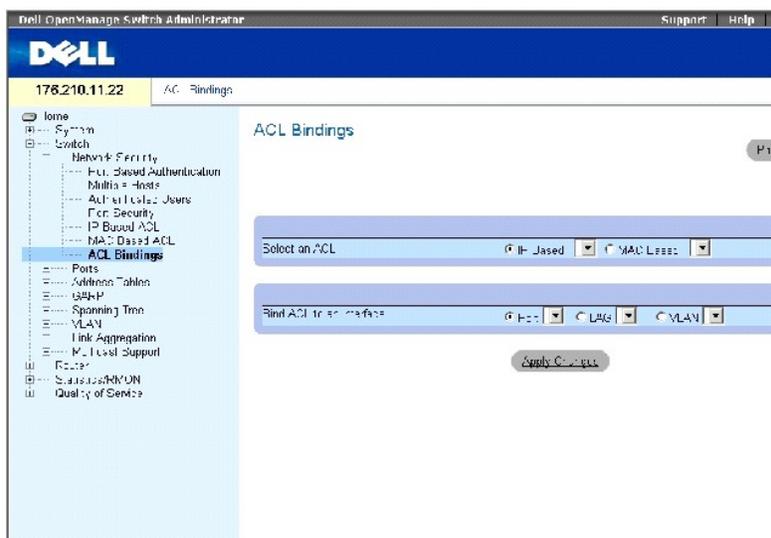
```
Console (config-mac-a1)# deny 6:6:6:6:6:6 0:0:255:255:255:255
```

Настройка привязки списков ACL

Когда выполняется связь списка ACL с интерфейсом, все правила, определенные в записях ACE, применяются для выбранного интерфейса. Используйте страницу [ACL Bindings](#) (Привязки ACL) для назначения списков ACL методам классификации и интерфейсам.

Чтобы открыть страницу [ACL Bindings](#) (Привязки ACL), выберите **Switch** (Коммутатор)→ **Network Security** (Безопасность сети)→ **ACL Binding** (Привязки ACL).

Рис. 7-12. Привязки ACL



Страница [ACL Bindings](#) (Привязки ACL) содержит следующие поля:

Select an ACL (Выбрать ACL) - тип списка ACL, с которым сравниваются входящие пакеты. Пакеты могут сравниваться со списком ACL, основанным на IP-адресах или на MAC-адресах.

Bind ACL to Interface (Привязать список ACL к интерфейсу) - показывает интерфейс и его тип, к которому привязан список ACL. Можно подключить список ACL к порту, LAG или VLAN.

Назначение списка ACL для интерфейса

1. Откройте страницу [ACL Bindings](#) (Привязки ACL).
2. Выберите тип ACL в поле **Select ACL** (Выберите ACL).
3. Выберите в поле **Bind ACL to an Interface** (Привязать интерфейс к списку ACL) интерфейс, с которым связан ACL.

ПРИМЕЧАНИЕ. Каждый раз, когда список ACL назначается для порта, группы LAG или VLAN, потоки с этого входящего интерфейса, которые не соответствуют списку ACL, сравниваются с правилом по умолчанию (опускание несоответствующих пакетов).

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

Список ACL будет привязан к интерфейсу.

Удаление записи из таблицы привязки ACL

1. Откройте страницу [ACL Bindings](#) (Привязки ACL).
2. Нажмите кнопку **Show All** (Показать все), чтобы отобразить страницу **ACL Bindings Table** (Таблица привязки ACL).
3. Установите флажок **Remove** (Удалить) для записи, которую необходимо удалить.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Выбранная запись будет удалена из таблицы, а устройство обновлено.

Отображение таблицы привязки ACL

1. Откройте страницу [ACL Bindings](#) (Привязки ACL).
2. Нажмите кнопку **Show All** (Показать все), чтобы отобразить страницу **ACL Bindings Table** (Таблица привязки ACL).

Поля страницы **ACL Bindings Table** (Таблица привязки ACL) такие же, как на странице [ACL Bindings](#) (Привязки ACL).

Скопируйте параметры в таблицу привязки ACL

1. Откройте страницу [ACL Bindings](#) (Привязки ACL).
2. Нажмите кнопку **Show All** (Показать все), чтобы отобразить страницу **ACL Bindings Table** (Таблица привязки ACL).
3. Выберите интерфейс в поле **Copy from** (Копировать из).
4. Выберите порт/транк в раскрывающемся меню **Port/LAG** или **VLAN**.

Определения для интерфейса будут скопированы в выбранный порт/транк.

5. Установите флажок **Copy to** (Копировать в) для записи, которую необходимо изменить, или нажмите **Select All** (Выбрать все) для копирования определений для всех возможных портов/транков.
6. Нажмите кнопку **Apply Changes** (Применить изменения).

Параметры будут скопированы в выбранные порты/транки в *ACL Bindings Table* (Таблица привязки ACL), а устройство обновлено.

Назначение принадлежности к списку ACL с помощью команд консоли

В следующей таблице приведены команды консоли, соответствующие действиям по назначению членства в ACL страницы [ACL Bindings](#) (Привязки ACL).

Таблица 7-7. Команды консоли привязки ACL

Команда консоли	Описание
<code>class-map имя_таблицы_классов [match-all match-any]</code>	Создает таблицу классов и включает режим ее настройки.
<code>match access-group имя_acl</code>	Определяет критерии соответствия для классификации трафика.
<code>show class-map [имя_таблицы_классов]</code>	Отображает все таблицы классов, настроенные на устройстве.

Далее приведен пример команд консоли.

```
Console (config)# class-map class1 match-all
```

```
Console (config-cmap)# match access-group dell
```

```
Console (config-cmap)# exit
```

```
Console(config)# exit
```

```
Console> exit
```

```
Console> show class-map class1
```

```
Class Map match-all class1 (id4)
```

Настройка портов

На странице [Ports \(Порты\)](#) находятся ссылки для настройки работы портов, в том числе таких функций, как контроль «лавины», зеркалирование портов и виртуальное тестирование портов.

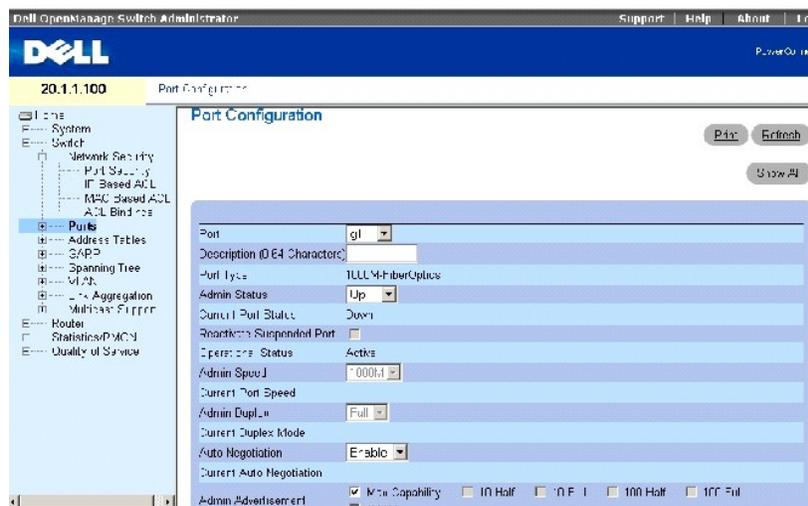
Чтобы открыть страницу [Ports \(Порты\)](#), выберите [Switch \(Коммутатор\)](#) → [Ports \(Порты\)](#).

Определение настройки портов

Используйте страницу [Port Configuration](#) (Настройка портов) для определения параметров портов.

Чтобы открыть страницу [Port Configuration](#) (Настройка портов), выберите [Switch \(Коммутатор\)](#) → [Ports \(Порты\)](#) → [Port Configuration](#) (Настройка портов) на панели дерева.

Рис. 7-13. Страница Port Configuration (Настройка портов)



Страница [Port Configuration](#) (Настройка портов) содержит следующие поля:

Port (Порт) - номер порта, для которого определяются параметры.

Description (Описание) (0-64 символов) - краткое описание интерфейса, например Ethernet.

Port Type (Тип порта) - тип порта.

Admin Status (Состояние администрирования) - включает или отключает пересылку трафика через порт.

Current Port Status (Текущее состояние порта) - показывает, в работоспособном ли состоянии находится в настоящий момент порт.

Reactivate Suspended Port (Возврат отключенного порта к работе) - заново активизирует порт, если он был отключен системой безопасности.

Operational Status (Рабочее состояние) - показывает рабочее состояние порта. Возможные значения этого поля:

Suspended (Приостановлен) - порт активен и в настоящий момент не получает и не передает трафик.

Active (Активен) - порт активен и в настоящий момент получает и передает трафик.

Disable (Отключен) - порт отключен и в настоящий момент не получает и не передает трафик.

Admin Speed (Администрирование скорости) - настроенная скорость порта. Тип порта определяет доступные параметры скорости. Значение скорости порта может быть изменено только в том случае, если порт отключен.

Current Port Speed (Текущая скорость порта) - показывает скорость синхронизации порта (в битах в секунду).

Admin Duplex (Администрирование дуплексного режима) - скорость порта в дуплексном режиме (в битах в секунду). Значение **Full** (Дуплексный) указывает, что интерфейс поддерживает передачу между устройством и клиентом одновременно в обоих направлениях. Значение **Half** (Полудуплексный) указывает, что интерфейс поддерживает передачу между устройством и клиентом только в одном направлении в каждый момент времени.

Current Duplex Mode (Дуплексный режим) - показывает дуплексный режим синхронизации порта.

Auto Negotiation (Автоматическое согласование) - включает автоматическое согласование 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 (Текущее автоматическое согласование) - показывает текущую настройку автоматического согласования.

Admin Advertisement (Объявление администрирования) - указывает возможности, объявляемые портом. Возможные значения:

Max Capability (Максимальная производительность) - указывает все параметры скорости портов и дуплексного режима, которые можно использовать.

10 Half (10 полудуплексный) - указывает, что порт объявляет параметры скорости 10 Мбит/с и полудуплексного режима.

10 Full (10 дуплексный) - указывает, что порт объявляет параметры скорости 10 Мбит/с и дуплексного режима.

100 Half (100 полудуплексный) - указывает, что порт объявляет параметры скорости 100 Мбит/с и полудуплексного режима.

100 Full (100 дуплексный) - указывает, что порт объявляет параметры скорости 100 Мбит/с и дуплексного режима.

1000 Full (1000 дуплексный) - указывает, что порт объявляет параметры скорости 1000 Мбит/с и дуплексного режима.

Current Advertisement (Текущее объявление) - порт объявляет скорость соседнему порту для начала согласования. Возможные значения полей указаны в поле Admin Advertisement (Объявление администрирования).

Neighbor Advertisement (Объявление соседнего порта) - соседний порт (тот, к которому подключается выбранный интерфейс) объявляет возможности для начала согласования. Возможные значения указаны в поле Admin Advertisement (Объявление администрирования).

Back Pressure (Обратное давление) - включает режим обратного давления для порта. Режим обратного давления используется с полудуплексным режимом, чтобы отключить получение сообщений на порты. Функция обратного давления не поддерживается для портов вне диапазона.

Current Back Pressure (Текущий режим обратного давления) - текущая настройка режима обратного давления.

Flow Control (Управление потоком) - включает или отключает управление потоком или включает автоматическое согласование управления потоком для порта.

Current Flow Control (Текущее управление потоком) - текущая настройка управления потоком.

MDI/MDIX - позволяет устройству определять, какой используется кабель - перекрестный и неперекрестный.

В концентраторах и коммутаторах специально используется противоположная схема подключения проводов, чем на конечных станциях. Поэтому при подключении концентратора или коммутатора к конечной станции можно использовать соединение напрямую кабелем Ethernet, так как провода совпадают. При соединении между собой двух концентраторов/коммутаторов или двух конечных станций используют перекрестный кабель, который соединяет правильные пары. Функция автоматического выбора MDIX не работает на портах FE, если автоматическое согласование отключено. MDIX не поддерживается для портов вне диапазона.

Возможные значения:

Media Dependent Interface with Crossover (MDIX) - используется для концентраторов и коммутаторов.

Media Dependent Interface (MDI) - используется для конечных станций.

Current MDI/MDIX (Текущий MDI/MDIX) - указывает текущие настройки устройства MDIX. Возможные значения этого поля:

MDI - для параметра MDI установлено значение MDI.

MDIX - для параметра MDI установлено значение MDIX.

Auto (Авто) - значение задается автоматически.

LAG - показывает, что порт входит в группу LAG.

PVE - включает порт как Private VLAN Edge (PVE). Если порт определен как PVE, он обходит базу данных пересылки (FDB) и пересылает весь одноадресный, многоадресный и широковещательный трафик на групповое соединение (за исключением пакетов MAC-to-me). Групповые соединения могут быть портом или LAG. Трафик групповых соединений распределяется на все интерфейсы.

Определение параметров порта

1. Откройте страницу [Port Configuration](#) (Настройка портов).
2. Выберите порт в поле **Port** (Порт).
3. Заполните доступные поля в диалоговом окне.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Параметры порта будут сохранены для этого устройства.

Отображение таблицы портов

1. Откройте страницу [Port Configuration](#) (Настройка портов).
2. Нажмите кнопку **Show All** (Показать все), чтобы отобразить страницу **Port Configuration Table** (Таблица настройки портов).

Настройка портов с помощью команд консоли

В следующей таблице приведены команды консоли для настройки портов, как показано на странице [Port Configuration](#) (Настройка портов).

Таблица 7-8. Команды консоли для настройки портов

Команда консоли	Описание
<code>interface ethernet <i>интерфейс</i></code>	Включает режим настройки интерфейса для настройки типа интерфейса Ethernet.
<code>description <i>строка</i></code>	Добавляет описание в конфигурацию интерфейса.
<code>shutdown</code>	Выключает интерфейсы, которые входят в состав текущего заданного контекста.
<code>set interface active {ethernet <i>интерфейс</i> port-channel <i>номер_канала_порта</i>}</code>	Вновь активизирует интерфейс, отключенный по причинам безопасности.
<code>speed {10 100 1000}</code>	Настраивает скорость заданного интерфейса Ethernet, если не используется автоматическое согласование.
<code>duplex {half full}</code>	Настраивает дуплексный или полудуплексный режим для заданного интерфейса Ethernet, если не используется автоматическое согласование.
<code>negotiation</code>	Включает автоматическое согласование для параметров скорости и дуплексного режима данного интерфейса.
<code>back-pressure</code>	Включает режим обратного давления для заданного интерфейса.
<code>flowcontrol {auto on off}</code>	Настраивает управление потоком для заданного интерфейса.
<code>mdix {on auto}</code>	Включает автоматическое использование перекрестного кабеля для заданного интерфейса или канала порта.
<code>show interfaces configuration [ethernet <i>интерфейс</i> port-channel <i>номер_канала_порта</i> oob- eth <i>интерфейс</i>]</code>	Отображает конфигурацию для всех настроенных интерфейсов.

<pre>show interfaces status [ethernet интерфейс port- channel номер_канала_порта oob-eth интерфейс]</pre>	Отображает состояние для всех настроенных интерфейсов.
<pre>show interfaces description [ethernet интерфейс port-channel номер_канала_порта oob- eth интерфейс]</pre>	Отображает описание для всех настроенных интерфейсов.

Далее приведен пример команд консоли.

```
Console (config)# interface ethernet g18
```

```
Console (config-if)# description RD_SW#3
```

```
Console (config-if)# speed 100
```

```
Console (config-if)# shutdown
```

```
Console (config-if)# no shutdown
```

```
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)# exit
```

```
Console(config)# exit
```

```
Console> set interface active ethernet g9
```

```
Console> show interfaces status
```

Port	Тип	Duplex	Speed	Neg	Flow ctrl	Link State	Back Pressure	Mdix Mode
---	-----	----	---	---	-----	-----	-----	-----
g1	1G-Copper	Full	1000	Enabled	Off	Up	Disabled	Off

g2	1G-Copper	Full	1000	Enabled	Off	Up	Disabled	Off
g3	1G-Copper	Full	1000	Enabled	Off	Up	Disabled	Off

Ch	Тип	Duplex	Speed	Neg	control	State	Pressure
---	-----	-----	-----	-----	-----	-----	-----
ch1	Unknown	Unknown		Unknown	Off	Not Present	Unknown
ch2	Unknown	Unknown		Unknown	Off	Not Present	Unknown
ch3	Unknown	Unknown		Unknown	Off	Not Present	Unknown
ch4	Unknown	Unknown		Unknown	Off	Not Present	Unknown

Console# show interfaces configuration

Ch	Тип	Duplex	Speed	Neg	control	State	Pressure
---	-----	---	---	---	-----	-----	-----
ch1	Unknown			Включен	Off	Up	Disabled
ch2	Unknown			Включен	Off	Up	Disabled
ch3	Unknown			Включен	Off	Up	Disabled

Console# show interfaces description ethernet 1

Port	Description
---	-----
g1	connect_to_server

Определение настройки LAG

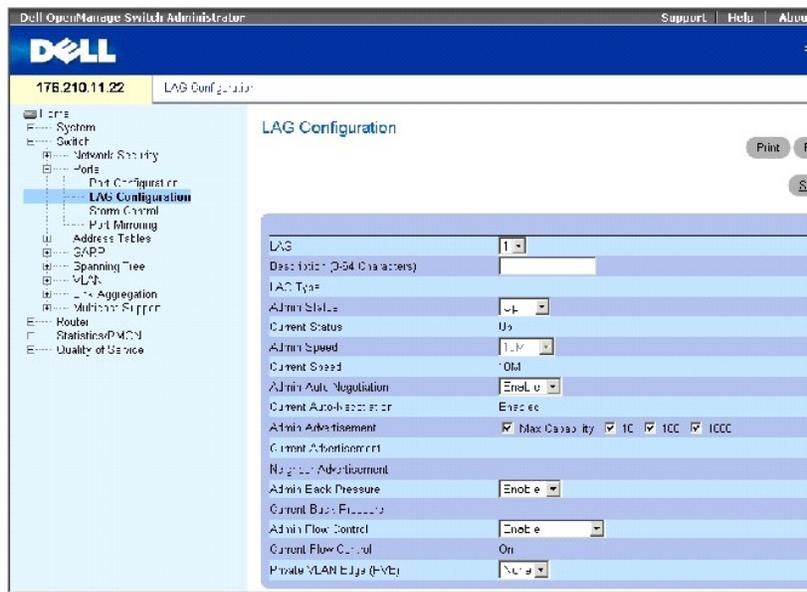
Многоуровневые коммутаторы поддерживают объединение нескольких каналов в один логический канал с суммарной пропускной способностью, который называется группой объединенных каналов (LAG). LAG также называют транками или объединенными каналами.

Для настройки параметров LAG используйте страницу [LAG Configuration](#) (Настройка LAG). Коммутатор поддерживает в каждой системе до семи портов на группу LAG и семь групп LAG. Если конфигурация порта изменяется, пока он является членом группы LAG, изменения вступают в действие только после удаления порта из этой группы.

Дополнительную информацию об объединении портов и назначении портов в группы LAG см. в разделе «[Объединение портов](#)».

Чтобы открыть страницу [LAG Configuration](#) (Настройка LAG), выберите Switch (Коммутатор)→ Ports (Порты)→ LAG Configuration (Настройка LAG) на панели дерева.

Рис. 7-14. Страница LAG Configuration (Настройка LAG)



Страница [LAG Configuration](#) (Настройка LAG) содержит следующие поля.

LAG - содержит список номеров LAG.

Description (0-64 Characters) (Описание (0-64 символов)) - описание порта.

LAG Type (Тип LAG) - типы портов, входящих в состав LAG.

Admin Status (Состояние администрирования) - включает или отключает пересылку трафика через выбранную группу LAG.

Current Status (Текущее состояние) - показывает, работает ли в данный момент группа LAG.

Admin Speed (Администрирование скорости) - скорость, на которой работает LAG.

Current Speed (Текущая скорость) - текущая скорость, на которой работает LAG.

Admin Auto Negotiation (Администрирование автоматического согласования) - включает или отключает автоматическое согласование для группы LAG. Автоматическое согласование - это протокол между двумя партнерами по связи, который позволяет группе LAG оповестить партнера канала связи о

своей скорости передачи, возможности работы в дуплексном режиме и управлении потоком (управление потоком по умолчанию выключено).

Current Auto Negotiation (Текущее автоматическое согласование) - показывает текущую настройку автоматического согласования.

Admin Advertisement - (Объявление администрирования) - указывает возможности, объявляемые LAG. Возможные значения:

Max Capability (Максимальная производительность) - указывает все параметры скорости LAG и дуплексного режима, которые можно использовать.

10 - указывает, что LAG объявляет параметры скорости 10 Мбит/с и дуплексного режима.

100 - указывает, что LAG объявляет параметры скорости 100 Мбит/с и дуплексного режима.

1000 - указывает, что LAG объявляет параметры скорости 1000 Мбит/с и дуплексного режима.

Current Advertisement (Текущее объявление) - LAG объявляет возможности соседней LAG для начала согласования. Возможные значения полей указаны в поле Admin Advertisement (Объявление администрирования).

Neighbor Advertisement (Объявление соседней LAG) - соседняя LAG (та, к которой подключается выбранный интерфейс) объявляет возможности для начала согласования. Возможные значения указаны в поле Admin Advertisement (Объявление администрирования).

Admin Back Pressure (Обратное значение) - включает или отключает режим обратного давления на устройстве. Режим обратного давления используется с полудуплексным режимом, чтобы отключить получение сообщений на порты.

Current Back Pressure (Текущий режим обратного давления) - указывает, включен или выключен режим обратного давления.

Admin Flow Control (Управление потоком) - включает или отключает управление потоком или включает автоматическое согласование управления потоком для LAG.

Current Flow Control (Текущее управление потоком) - определяемая пользователем настройка управления потоком.

Определение параметров LAG

1. Откройте страницу [LAG Configuration](#) (Настройка LAG).
2. Выберите группу LAG в поле **LAG**.
3. Введите значения в имеющиеся поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Параметры группы LAG будут сохранены для этого устройства.

Отображение таблицы настройки LAG

1. Откройте страницу [LAG Configuration](#) (Настройка LAG).
2. Нажмите кнопку **Show All** (Показать все), чтобы отобразить страницу **LAG Configuration Table** (Таблица настройки LAG).

Настройка групп LAG с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для настройки групп LAG, как показано на странице [LAG Configuration](#) (Настройка LAG).

Таблица 7-9. Команды консоли для настройки LAG

Команда консоли	Описание
<code>interface port-channel номер_канала_порта</code>	Включает режим настройки интерфейса для указанного канала-порта.
<code>channel-group номер_канала_порта mode {on auto}</code>	Связывает порт с каналом порта.
<code>show interfaces port- channel [номер_канала_порта]</code>	Выводит сведения о канале порта (какие порты входят в канал порта, активны они на данный момент или нет).

Далее приведен пример команд консоли.

```
Console (config)# interface ethernet g5
```

```
Console (config-if)# channel-group 1 mode on
```

```
Console(config-if)# exit
```

```
Console# show interfaces port-channel
```

```
Channel Port
```

```
-----
```

```
Ch 1 Active g1, g2, g5 Inactive g3
```

```
Ch 2 Active g2
```

```
Ch 3 Inactive g8
```

Включение контроля «лавины»

Широковещательная «лавина» - это результат чрезмерного количества широковещательных сообщений, одновременно переданных по сети на один порт. Ответы на пересылаемые сообщения перегружают сеть, уменьшая ее ресурсы или вызывая задержки в сети.

Коммутатор измеряет скорость входящих широковещательных многоадресных пакетов для каждого порта и отбрасывает пакеты при превышении установленного значения скорости. Контроль «лавины» включается для каждого устройства путем определения типа пакета и скорости передачи пакетов. Группы портов обеспечивают защиту от «лавины» для целой группы.

Чтобы включить и настроить контроль «лавины», используйте страницу **Storm Control** (Контроль «лавины»). Чтобы открыть страницу **Storm Control** (Контроль «лавины»), выберите **Switch** (Коммутатор)→ **Ports** (Порты)→ **Storm Control** (Контроль «лавины») на панели дерева.

Рис. 7-15. Страница Storm Control (Контроль «лавины»)



Count Multicast with Broadcast (Подсчитывать многоадресные и широковещательные) - **Enable** (Включено) выполняется подсчет широковещательного и многоадресного трафика; **Disable** (Отключено) выполняется подсчет только широковещательного трафика.

Port (Порт) - порт, для которого включен контроль «лавины».

Broadcast Control (Управление широковещательными передачами) - включает или отключает пересылку пакетов неизвестного типа на устройство.

Broadcast Rate Threshold (Порог скорости широковещательных пакетов) - максимальная скорость (в килобайтах в секунду), при которой пересылаются неизвестные пакеты. Диапазон значений от 0 до 148800. Значение по умолчанию: 12000. Все значения округляются до 64 Кбит/с. Если значение поля меньше 64 Кбит/с, значение округляется до 64 Кбит/с.

Изменение параметров контроля «лавины» порта

1. Откройте страницу **Storm Control** (Контроль «лавины»).
2. Заполните поля на этой странице.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Параметры контроля «лавины» порта будут сохранены для этого устройства.

Копирование параметров в таблицу параметров контроля «лавины»

1. Откройте страницу **Storm Control** (Контроль «лавины»).
2. Нажмите кнопку **Show All** (Показать все), чтобы отобразить страницу **Storm Control Settings Table** (Таблица параметров контроля «лавины»).
3. В поле **Copy Parameters from Port** (Копировать параметры из порта) выберите порт, из которого необходимо скопировать параметры.
4. Установите флажок **Copy to** (Копировать в), чтобы определить интерфейсы, в которые будут скопированы параметры контроля «лавины», или нажмите кнопку **Select All** (Выбрать все) для копирования определений во все порты.
5. Нажмите кнопку **Apply Changes** (Применить изменения).

Параметры будут скопированы в выбранные порты в **Storm Control Settings Table** (Таблице параметров контроля «лавины»), а устройство обновлено.

Настройка контроля «лавины» с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для настройки контроля «лавины», как показано на странице Storm Control (Контроль «лавины»).

Таблица 7-10. Команды консоли для настройки контроля «лавины»

Команда консоли	Описание
<code>port storm-control include-multicast</code>	Позволяет устройству подсчитывать многоадресные пакеты вместе с широковещательными пакетами.
<code>port storm-control broadcast enable</code>	Включает контроль широковещательной «лавины».
<code>port storm-control broadcast rate <i>скорость</i></code>	Настраивает максимальную скорость для широковещательных пакетов.
<code>show ports storm-control <i>порт</i></code>	Отображает конфигурацию контроля «лавины».

Далее приведен пример команд консоли.

```
Console(config)# port storm-control include-multicast
```

```
Console (config)# interface ethernet g1
```

```
Console(config-if)# port storm-control broadcast enable
```

```
Console(config-if)# port storm-control broadcast rate 100000
```

```
Console (config-if) # exit
```

Port	Защита от «лавины» широковещательной и многоадресной передачи [Кбайт/сек]	
---	-----	
g1		100000
g2		Disabled
...		
g24		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 (контролирующий). Зеркалирование портов можно использовать как средство диагностики и отладки. Зеркалирование портов также позволяет контролировать работу коммутатора.

Администраторы сети настраивают зеркалирование портов, выбирая определенный порт для копирования всех пакетов и разные порты, с которых

копируются пакеты. Перед настройкой зеркалирования портов учтите следующее.

- 1 Контролируемые порты не могут работать быстрее, чем контролируемые.
- 1 Допустимое максимальное количество исходных портов - восемь.
- 1 За один раз может быть настроен только один сеанс зеркалирования.

К портам, настроенным как порты назначения, применяются следующие ограничения.

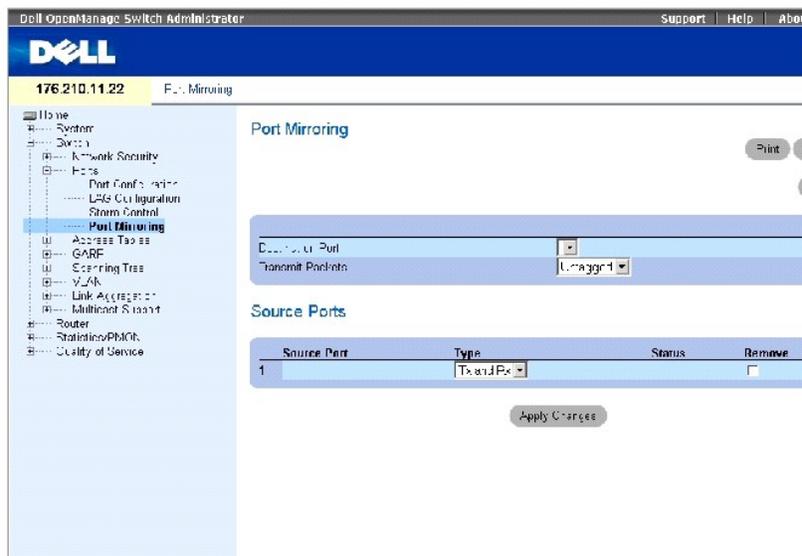
- 1 Порты нельзя настроить в качестве портов-источников.
- 1 Порты не могут входить в группу LAG.
- 1 Для этого порта не настроены интерфейсы IP.
- 1 Для этого порта не включен протокол GVRP.
- 1 Порт не входит в сеть VLAN.
- 1 Можно определить только один порт назначения.

К портам, настроенным как порты-источники, применяются следующие ограничения.

- 1 Порты-источники не могут входить в группу LAG.
- 1 Порты нельзя настроить в качестве портов назначения.
- 1 Все пакеты помечаются при их передаче из порта назначения.
- 1 Все пакеты TX должны контролироваться на одном порте.

Чтобы открыть страницу [Port Mirroring](#) (Зеркалирование портов), выберите Switch (Коммутатор)→ Ports (Порты)→ Port Mirroring (Зеркалирование портов) на панели дерева.

Рис. 7-16. Страница Port Mirroring (Зеркалирование портов)



Страница [Port Mirroring](#) (Зеркалирование портов) содержит следующие поля:

Destination Port (Порт назначения) - содержит список номеров портов, из которых можно копировать трафик.

Transmit Packets (Передача пакетов) - указывает, помечаются или не помечаются пакеты при их передаче из порта назначения.

Source Port (Порт-источник) - номер порта, в который копируется трафик.

Type (Тип) - определяет тип контролируемого трафика. Возможные значения этого поля:

TX - контролирует только переданные пакеты.

RX - контролирует только полученные пакеты.

TX and RX (TX и RX) - контролирует переданные и полученные пакеты.

Status (Состояние) - показывает, выполняется ли в настоящий момент контроль порта (**Active**) или не выполняется (**Not Ready**).

Remove (Удалить) - если этот флажок установлен, удаляется сеанс зеркалирования портов.

Добавление сеанса с зеркалирования портов

1. Откройте страницу **Port Mirroring** (Зеркалирование портов).
2. Щелкните **Add** (Добавить), чтобы отобразить страницу **Add Source Port** (Добавление порта-источника).
3. В раскрывающемся списке **Source Port** (Порт-источник) выберите исходный порт.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Новый сеанс зеркалирования включен для порта, а устройство обновлено.

Изменение сеанса с зеркалирования портов

1. Откройте страницу **Port Mirroring** (Зеркалирование портов).
2. Измените поля.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Поля для сеанса зеркалирования портов будут изменены, а устройство обновлено.

Удаление сеанса с зеркалирования портов

1. Откройте страницу **Port Mirroring** (Зеркалирование портов).
2. Установите флажок **Remove** (Удалить).
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Сеанс с зеркалированием портов будет удален, а устройство обновлено.

Настройка сеанса с зеркалированием портов с помощью команд консоли

В следующей таблице приведены команды консоли, соответствующие полям страницы [Port Mirroring](#) (Зеркалирование портов) для настройки сеанса с зеркалированием портов.

Таблица 7-11. Команды консоли для настройки сеанса зеркалирования портов

Команда консоли	Описание
-----------------	----------

port monitor <i>интерфейс_src</i> [rx tx]	Запускает сеанс с зеркалированием портов.
show ports monitor	Отображает состояние контроля портов.

Далее приведен пример команд консоли.

```
Console(config-if)# port monitor g2
```

Настройка адресных таблиц

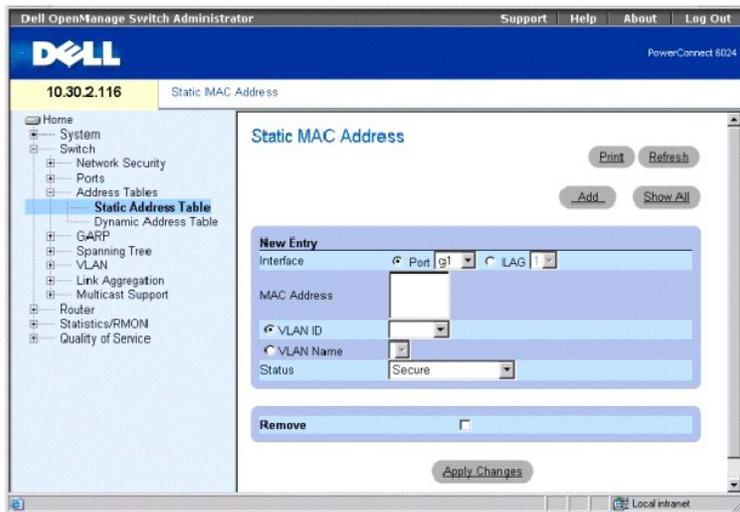
MAC-адреса хранятся в базе данных статических или динамических адресов. Статические адреса определяются пользователем. Динамические адреса распознаются системой и удаляются по истечении времени ожидания. Пакет, адресованный приемнику, хранящемуся в одной из баз данных, немедленно пересылается на порт. Таблицы статических и динамических адресов могут быть отсортированы по интерфейсу, VLAN и типу интерфейса. Кроме того, адреса можно добавить в таблицы статических и динамических адресов.

Чтобы открыть страницу Address Tables (Таблицы адресов), выберите Switch (Коммутатор) → Address Table (Таблицы адресов) на панели дерева.

Определение статических адресов

На странице Static Address (Статические адреса) приведен список всех статических MAC-адресов. Статические адреса можно добавлять и удалять со страницы Static MAC Address Table (Таблица статических MAC-адресов). Чтобы открыть страницу Static Address (Статические адреса), выберите Switch (Коммутатор) → Address Table (Таблицы адресов) → Static Address (Статические адреса) на панели дерева.

Рис. 7-17. Страница Static MAC Address (Статические MAC-адреса)



Interface (Интерфейс) - порт или группа LAG, для которых назначены статические MAC-адреса.

MAC Address (MAC-адрес) - список MAC-адрес в текущем списке статических адресов.

 **ПРИМЕЧАНИЕ.** Отображаются только MAC-адреса, назначенные для указанного интерфейса и VLAN. Чтобы просмотреть MAC-адреса, назначенные другой группе VLAN, выберите VLAN в окне выбора VLAN.

VLAN ID (Идентификатор сети VLAN) - номер группы VLAN, связанной с MAC-адресом.

VLAN Name (Имя сети VLAN) - имя сети VLAN, задаваемое пользователем.

Status (Состояние) - состояние MAC-адреса. Возможные значения:

Secure (Защищенный) - гарантирует, что MAC-адрес заблокированного порта не будет удален.

Permanent (Постоянный) - показывает, что MAC-адрес является постоянным.

Delete on Reset (Удаляется при перезагрузке) - показывает, что MAC-адрес удаляется при перезагрузке устройства.

Delete on Timeout (Удаляется по истечении времени ожидания) - показывает, что MAC-адрес удаляется по истечении времени ожидания.

Добавление статического MAC-адреса

1. Откройте страницу **Static MAC Address** (Статические MAC-адреса).
2. Щелкните **Add** (Добавить), чтобы отобразить страницу **Add Static MAC Address** (Добавление статического MAC-адреса).
3. Заполните поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Новый статический адрес будет добавлен в **Static MAC Address Table** (Таблицу статических MAC-адресов), а устройство обновлено.

Изменение статического MAC-адреса в таблице статических адресов

1. Откройте страницу **Static MAC Address** (Статические MAC-адреса).
2. Измените поля.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Статический MAC-адрес будет изменен, а устройство обновлено.

Удаление статического адреса из таблицы статических адресов

1. Откройте страницу **Static MAC Address** (Статические MAC-адреса).
2. Нажмите кнопку **Show All** (Показать все), чтобы открыть страницу **Static MAC Address Table** (Таблица статических MAC-адресов).
3. Выберите запись таблицы.
4. Установите флажок **Remove** (Удалить).
5. Нажмите кнопку **Apply Changes** (Применить изменения).

Статический адрес будет удален, а устройство обновлено.

Настройка параметров статических адресов с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для настройки параметров статических адресов, как показано на странице [Static MAC Address](#) (Статические MAC-адреса).

Таблица 7-12. Команды консоли настройки статических адресов

Команда консоли	Описание
<pre>bridge address mac-address {ethernet <i>интерфейс</i> port- channel <i>номер_канала_порта</i>} [permanent delete-on-reset delete- on-timeout secure]</pre>	Добавляет статический MAC-адрес станции-источника в таблицу связей.
<pre>show bridge address-table static [vlan <i>vlan</i>] [ethernet <i>интерфейс</i> port- channel <i>номер_канала_порта</i>]</pre>	Отображает статически созданные записи базы данных, содержащей сведения о пересылке данных через мосты.

Далее приведен пример команд консоли.

```
console (config)# interface vlan 1 console

(config-vlan)# bridge address 3aa2.64b3.a245 ethernet g8 permanent....

Console (config-vlan)# exit

Console(config)# exit

Console> show bridge address-table static

Aging time is 300 sec

Vlan Mac Address Port Type
-----
1 3a:a2:64:b3:a2:45 g8 permanent
```

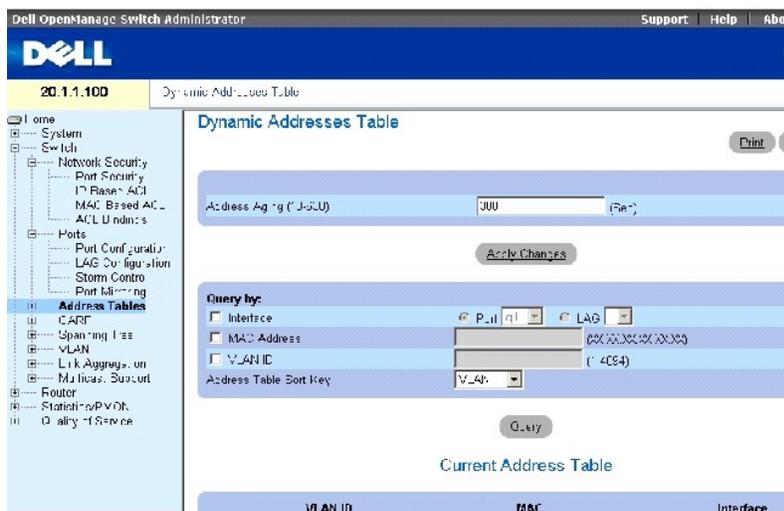
Просмотр динамических адресов

На странице [Dynamic Addresses Table](#) (Таблица динамических адресов) приведены сведения по запросу данных в таблице динамических адресов, в том числе типа интерфейса, MAC-адреса, VLAN и ключа для сортировки таблицы. Пакеты, которые пересылаются по адресам, хранящимся в таблице адресов, пересылаются непосредственно на эти порты.

[Dynamic Address Table](#) (Таблица динамических адресов) содержит информацию о сроке хранения, после которого динамические MAC-адреса удаляются из таблицы.

Чтобы открыть страницу [Dynamic Address Table](#) (Таблица динамических адресов), выберите Switch (Коммутатор) → Address Tables (Таблицы адресов) → Dynamic Addresses Table (Таблица динамических адресов) на панели дерева.

Рис. 7-18. Страница Dynamic Address Table (Таблица динамических адресов)



Страница [Dynamic Address table](#) (Таблица динамических адресов) содержит следующие поля:

Address Aging (10-630) (Срок хранения адреса) - определяет срок хранения (в секундах) перед удалением MAC-адреса. Значение по умолчанию: 300 секунд.

[Dynamic Address Table](#) (Таблица динамических адресов) может работать со следующими запросами:

Port (Порт) - интерфейс, запрошенный для адреса.

MAC Address (MAC-адрес) - MAC-адрес, запрошенный для адреса.

VLAN ID (Идентификатор сети VLAN) - номер VLAN (для которой назначен MAC-адрес), запрошенный для адреса.

Address Table Sort Key (Ключ для сортировки таблицы адресов) - определяет, сортируется ли таблица динамических адресов по адресу, VLAN или интерфейсу.

Определение срока хранения

1. Откройте страницу [Dynamic Address Table](#) (Таблица динамических адресов).
2. Определите поле **Address Aging** (Срок хранения).
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Срок хранения будет изменен, а устройство обновлено.

Опрос таблицы динамических адресов

1. Откройте страницу [Dynamic Address Table](#) (Таблица динамических адресов).
2. Определите, по какому параметру нужно выполнить запрос таблицы **Dynamic Address Table** (Таблица динамических адресов).

Записи можно запрашивать по полю **Port** (Порт), **MAC Address** (MAC-адрес) или **VLAN ID** (Идентификатор сети VLAN).

3. Нажмите кнопку **Query** (Запрос).

Будет выполнен запрос по таблице динамических адресов.

Сортировка таблицы динамических адресов

1. Откройте страницу [Dynamic Address Table](#) (Таблица динамических адресов).
2. В раскрывающемся меню **Address Table Sort Key** (Ключ сортировки таблицы адресов) выберите поле, по которому будут отсортированы адреса - по адресу, идентификатору VLAN или интерфейсу.
3. Нажмите кнопку **Query** (Запрос).

Таблица динамических адресов отсортирована.

Таблица текущих адресов

Таблица текущих адресов содержит параметры динамических адресов, по которым пакеты передаются непосредственно на порты. Таблица текущих адресов содержит следующие поля:

- 1 **VLAN ID** (Идентификатор сети VLAN) - указывает значение метки VLAN.
- 1 **MAC** (MAC-адрес) - указывает MAC-адрес.
- 1 **Port** (Порт) - указывает номер порта.

Опрос и сортировка динамических адресов с помощью команд консоли

В следующей таблице приведены команды консоли, соответствующие полям для опроса и сортировки динамических адресов на странице [Dynamic Address Table](#) (Таблица динамических адресов).

Таблица 7-13. Команды консоли для опроса и сортировки динамических адресов

Команда консоли	Описание
<code>bridge aging-time секунды</code>	Задаёт срок хранения для таблиц адресов.
<code>show bridge address-table [vlan vlan] [ethernet интерфейс port-channel номер_канала_порта]</code>	Отображает классы динамически созданных записей базы данных, содержащей сведения о пересылке данных через мосты.

Далее приведен пример команд консоли.

```
Console (config)# bridge aging-time 300
```

```
Console(config)# exit
```

```
Console# show bridge address-table
```

```
Aging time is 300 sec
```

```
vlan mac address port type
```

1 0060.704C.73FF g8 dynamic

1 0060.708C.73FF g8 dynamic

200 0010.0D48.37FF g9 static

Настройка протокола GARP

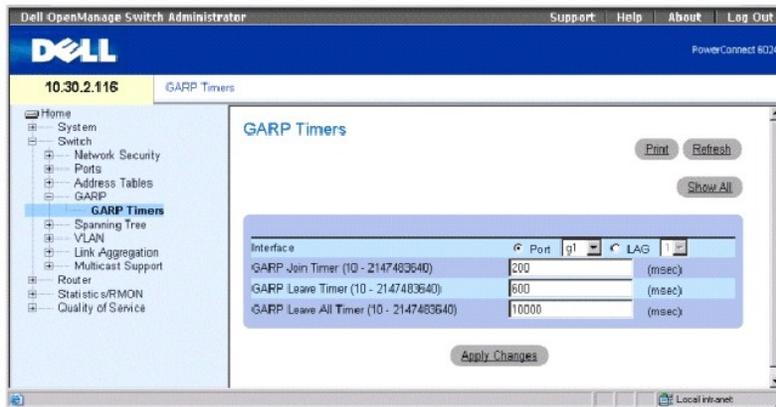
Протокол GARP (Generic Attribute Registration Protocol) - это протокол общего назначения, регистрирующий любые возможности связи в сети или сведения о принадлежности. Протокол GARP определяет набор устройств, заинтересованных в данном атрибуте сети, например VLAN или адрес многоадресной передачи.

Чтобы открыть страницу GARP, выберите Switch (Коммутатор) → GARP на панели дерева.

Определение таймеров GARP

На странице GARP Timers (Таймеры GARP) приведены параметры для включения протокола GARP на устройстве. Чтобы открыть страницу GARP Timers (Таймеры GARP), выберите Switch (Коммутатор) → GARP → GARP Timers (Таймеры GARP) на панели дерева.

Рис. 7-19. Страница GARP Timers (Таймеры GARP)



Страница [GARP Timers](#) (Таймеры GARP) содержит следующие поля:

Interface (Интерфейс) - определяет, где включен таймер - для порта или группы LAG.

GARP Join Timer (10 - 2147483640) (Таймер соединения GARP) - показывает время в миллисекундах, когда передаются модули PDU. Возможные значения поля: 10-2147483640. Значение по умолчанию: 200 мсек.

GARP Leave Timer (10 - 2147483640) (Таймер отключения GARP) - время (в миллисекундах), в течение которого устройство ожидает, прежде чем

выйти из состояния GARP. Отсчет времени Leave Time (Время отключения) активируется при отправке/получении сообщения Leave All Time (Время полного отключения) и отменяется при получении сообщения Join (Соединение). Время отключения должно быть больше или равно трехкратному времени соединения. Возможные значения поля: 0-2147483640. Значение по умолчанию: 600 мсек.

GARP Leave All Timer (10 - 2147483640) (Таймер полного отключения GARP) - время (в миллисекундах), в течение которого все устройства ожидают, прежде чем выйти из состояния GARP. Время полного отключения должно быть больше времени отключения. Возможные значения поля: 0-2147483640. Значение по умолчанию: 10000 мсек.

Определение таймеров GARP

1. Откройте страницу **GARP Timers** (Таймеры GARP).
2. Заполните поля.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Параметры GARP будут сохранены на устройстве.

Копирование параметров в таблицу таймеров GARP

1. Откройте страницу **GARP Timers** (Таймеры GARP).
2. Нажмите кнопку **Show All** (Показать все), чтобы отобразить страницу **GARP Timers Table** (Таблица таймеров GARP).
3. Выберите интерфейс в поле **Copy Parameters from** (Копировать параметры из).
4. Выберите интерфейс в раскрывающемся меню **Port** (Порт) или **LAG**.
5. Определения для интерфейса будут скопированы в выбранный интерфейс. См. шаг 6.
6. Установите флажок **Copy to** (Копировать в), чтобы определить интерфейс, для которого будут скопированы параметры таймера GARP, или нажмите **Select All** (Выбрать все) для копирования определений во все порты или группы LAG.
7. Нажмите кнопку **Apply Changes** (Применить изменения).

Параметры будут скопированы в выбранные порты или группы LAG в **GARP Timers Table** (Таблица таймеров GARP), а устройство обновлено.

Определение таймеров GARP с помощью команд консоли

[В таблице 7-14](#) приведены команды консоли для определения таймеров GARP, как показано на странице **Garp Timers** (Таймеры GARP).

Таблица 7-14. Команды консоли для определения таймеров GARP

Команда консоли	Описание
<code>garp timer {join leave leaveall} время</code>	Задаёт значения таймеров GARP для времени соединения, отключения и полного отключения приложений GARP.

Далее приведен пример команд консоли.

```
Console (config)# interface ethernet g8
```

```
Console (config-if)# garp timer leave 900
```

Настройка протокола STP

Протокол STP (Spanning Tree Protocol) предоставляет древовидную топологию для любого расположения мостов. STP обеспечивает также единственный путь между конечными станциями сети и исключает циклы.

Циклы появляются, когда между хостами существует несколько альтернативных маршрутов. Циклы в расширенной сети могут привести к тому, что мосты будут пересылать трафик неограниченно, в результате чего увеличится трафик и снизится производительность сети.

Устройство поддерживает следующие версии протоколов STP: **Classic STP** (Классический STP), **Rapid STP** (Быстрый STP) и **Multiple STP** (Множественный STP).

Classic STP (Классический STP) - обеспечивает единственный путь между конечными станциями сети и исключает циклы. Дополнительную информацию о настройке классического STP см. в разделе «[Определение общих параметров STP](#)».

Быстрый STP (RSTP) выявляет и использует топологию сети, обеспечивая лучшую сходимость для протокола STP без образования циклов пересылки. Дополнительную информацию о настройке RSTP см. в разделе «[Определение протокола RSTP](#)».

Множественный STP (MSTP) предоставляет полную связность для пакетов, назначаемых любым VLAN. MSTP основан на протоколе RSTP. Кроме того, по протоколу MSTP передаются пакеты, назначенные разным VLAN через разные области MST. Области MST действуют как один мост. Протокол MSTP повышает системную отказоустойчивость и обеспечивает выравнивание нагрузки. Дополнительную информацию о настройке MSTP см. в разделе [Определение протокола MST](#).

Чтобы открыть страницу **Spanning Tree**, выберите **Switch (Коммутатор)** → **Spanning Tree** на панели дерева.

Определение общих параметров STP

На странице [Spanning Tree Global Settings](#) (Общие параметры STP) приведены параметры для включения протокола STP на устройстве.

Чтобы открыть страницу [Spanning Tree Global Settings](#) (Общие параметры STP), выберите **Switch (Коммутатор)** → **Spanning Tree (Протокол STP)** → **Global Settings (Общие параметры)** на панели дерева.

Рис. 7-20. Общие параметры STP

The screenshot shows the Dell OpenManage Switch Administrator interface. The main window is titled "Spanning Tree Global Settings" and displays various configuration options for STP. The left sidebar shows a tree view with "Spanning Tree" selected. The main content area is divided into sections: "Spanning Tree State", "Bridge Settings", and "Designated Root".

Section	Parameter	Value	Unit/Label
Spanning Tree State	Spanning Tree State	Enable	
	STP Operation Mode	Classic STP	
	Pct Cost Weight	Long	
	BPDU Flooding	Filtering	
Bridge Settings	Priority (0-5140, in steps of 4096)	32768	(Dec) ms
	Hello Time (1-10)	2	(Sec)
	Max Age (6-40)	20	(Sec)
	Forward Delay (4-30)	15	(Sec)
Designated Root	Bridge ID	32768-0C:00:60:23:12:12	
	Root Bridge ID	32768-0C:00:60:23:12:12	

Страница [Spanning Tree Global Settings](#) (Общие параметры STP) содержит следующие поля:

Spanning Tree State (Состояние Spanning Tree) - включает или отключает протоколы STP, RSTP или MSTP для устройства.

STP Operation Mode (Режим работы STP) - режим включения протокола STP на устройстве. Возможные значения этого поля: **Classic STP** (Классический STP), **Rapid STP** (Быстрый STP) и **Multiple STP** (Множественный STP).

Path Cost Method (Метод определения стоимости пути) - определяет метод, используемый для назначения стоимости пути по умолчанию для портов STP. Возможные значения:

Long (Длинный) - метод определения стоимости пути с диапазоном 1-200000000.

Short (Короткий) - метод определения стоимости пути с диапазоном 1-65535. Этот метод используется по умолчанию.

Стоимость пути по умолчанию назначается для разных интерфейсов в зависимости от выбранного метода.

Интерфейс	Длинный	Короткий
LAG	20000	4
1000 Мбит/с	20000	4
100 Мбит/с	200000	19
10 Мбит/с	2000000	100

BPDU Handling (Обработка BPDU) - определяет обработку пакетов BPDU, когда протокол Spanning Tree отключен для интерфейса. Допустимые значения: **Filtering** (Фильтр) и **Flooding** (Лавина). Значение по умолчанию: **Flooding** (Лавина).

Priority (0-65535) (Приоритет от 0 до 65535) - значение приоритета для моста. Когда коммутаторы или мосты работают по протоколу STP, каждому из них назначается приоритет. После обмена пакетами BPDU коммутатор с низким значением приоритета становится корневым мостом. Значение по умолчанию: 32768.

Hello Time (1-10) (Интервал отправки) - интервал отправки конфигурационных сообщений с корневого моста (в секундах). Значение по умолчанию: 2.

Max Age (6-40) (Максимальное время) - максимальное время, которое мост ожидает перед выполнением изменения топологии (в секундах). Значение по умолчанию: 20.

Forward Delay (4-30) (Задержка пересылки) - время, в течение которого мост находится в состоянии распознавания и прослушивания перед пересылкой пакетов (в секундах). Значение по умолчанию: 5.

Bridge ID (Идентификатор моста) - идентификатор моста.

Root Bridge ID (Идентификатор корневого моста) - идентификатор корневого моста.

Root Port (Корневой порт) - номер порта, предлагающего путь от данного моста к корневому с наименьшими затратами. Этот параметр имеет значение, если мост не является корневым. Значение по умолчанию: 0.

Root Path Cost (Стоимость пути к корню) - стоимость пути от данного моста к корню.

Topology Changes Counts (Количество изменений топологии) - общее количество изменений состояния STP.

Last Topology Change (Последнее изменение топологии) - общее время, прошедшее с момента последнего изменения топологии. Выводится в формате «часы-минуты-секунды», например: 5 часов 10 минут и 4 секунды.

Определение общих параметров STP

1. Откройте страницу [Spanning Tree Global Settings](#) (Общие параметры STP).
2. Выберите порт в раскрывающемся списке **Select a Port** (Выбор порта).
3. Выберите значение **Enable** (Включить) в поле **Spanning Tree State** (Состояние Spanning Tree).
4. Выберите режим STP в поле **STP Operation Mode** (Режим работы STP) и определите настройки моста.
5. Нажмите кнопку **Apply Changes** (Применить изменения).

STP включен для этого устройства.

Изменение общих параметров STP:

1. Откройте страницу [Spanning Tree Global Settings](#) (Общие параметры STP).
2. Определите поля в диалоговом окне.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Параметры протокола STP будут изменены, а устройство обновлено.

Определение общих параметров протокола STP с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для определения общих параметров STP, как отображается на странице [Spanning Tree Global Settings](#) (Общие параметры STP).

Таблица 7-15. Команды консоли для определения общих параметров STP

Команда консоли	Описание
<code>spanning-tree</code>	Включает функциональные возможности протокола STP.
<code>spanning-tree mode {stp rstp}</code>	Настраивает режим работы протокола STP.
<code>spanning-tree pathcost method {long short}</code>	Настраивает метод определения стоимости пути STP.
<code>spanning-tree bpdu {filtering flooding}</code>	Настраивает обработку пакетов BPDU, когда протокол Spanning Tree отключен для интерфейса.
<code>spanning-tree priority <i>приоритет</i></code>	Настраивает приоритет протокола STP.
<code>spanning-tree hello-time <i>секунды</i></code>	Настраивает время Hello Time для моста протокола STP, определяющее, как часто коммутатор выполняет широковещательную передачу сообщений «Hello» другим коммутаторам.
<code>spanning-tree max-age <i>секунды</i></code>	Настраивает максимальное время для моста протокола STP.
<code>spanning-tree forward-time <i>секунды</i></code>	Настраивает время пересылки для моста протокола STP, определяющее, как долго порт находится в состоянии прослушивания и распознавания перед переключением в состояние пересылки.
<code>show spanning-tree [ethernet <i>интерфейс</i> port-channel <i>номер_канала_порта</i>]</code>	Отображение конфигурации протокола STP.

Далее приведен пример команд консоли.

Console(config)# **spanning-tree**

Console(config)# **spanning-tree mode rstp**

Console(config)# **spanning-tree priority 12288**

Console(config)# **spanning-tree hello-time 5**

Console(config)# **spanning-tree max-age 10**

Console(config)# **spanning-tree forward-time 25**

Console (config)# **exit**

Console# **show spanning-tree**

Spanning tree enabled mode RSTP

Root ID Priority 32768

Address 0001.4297.e000

Cost 57

Port g1

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769

Address 0002.4b29.7a00

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Number of topology changes 8 last change occurred 00:37:24 ago

Times: hold 1, topology change 35, notification 2

hello 2, max age 20, forward delay 15



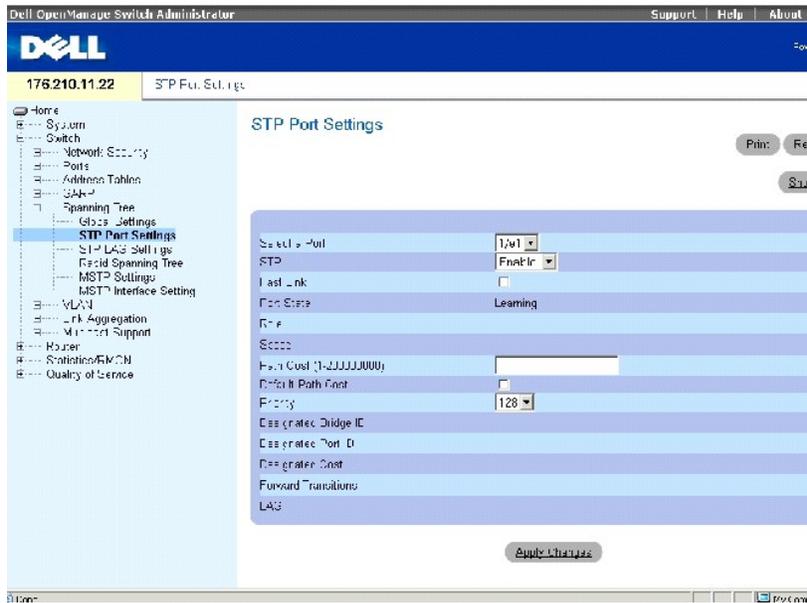
Inter face	Port ID				Designated			Port ID
Name	Prio	Sts	Enb	Cost	Cost	Bridge Id		Prio.Nbr
----	----	----	---	----	----	-----		---
g1	128	DSBL	FALSE	100	0	8000 00:00:b0:70:09:00		80 001
g2	128	DSBL	FALSE	100	0	8000 00:00:b0:70:09:00		80 002
g3	128	DSBL	FALSE	100	0	8000 00:00:b0:70:09:00		80 003
ch1	128	DSBL	TRUE	4	0	8000 00:00:b0:70:09:00		80 019
ch2	128	DSBL	TRUE	4	0	8000 00:00:b0:70:09:00		80 01a
ch3	128	DSBL	TRUE	4	0	8000 00:00:b0:70:09:00		80 01b

Определение параметров STP для порта

Чтобы назначить свойства STP для отдельных портов, используйте страницу [STP Port Settings](#) (Параметры STP для порта).

Чтобы открыть страницу [STP Port Settings](#) (Параметры STP для порта), выберите **Switch** (Коммутатор) → **Spanning Tree** (Протокол STP) → **Port Settings** (Параметры порта) на панели дерева.

Рис. 7-21. Страница STP Port Settings (Параметры STP для порта)



Страница [STP Port Settings](#) (Параметры порта STP) содержит следующие поля:

Select a Port (Выбор порта) - порт, для которого включен протокол STP.

STP (Протокол STP) - включает или отключает протокол STP для порта.

Fast Link (Быстрая связь) - при установке этого флажка включается режим быстрой связи для порта. Если режим быстрой связи для порта включен, то для параметра **Port State** (Состояние порта) автоматически устанавливается состояние **Forwarding** (Пересылка) сразу после появления связи. Режим **Fast Link** (Быстрая связь) оптимизирует время, которое требуется протоколу STP для сходимости. Для сходимости протокола STP в больших сетях может потребоваться от 30 до 60 секунд.

Port State (Состояние порта) - показывает текущее состояние протокола STP для порта. Если этот параметр включен, он определяет, какое действие пересылки выполняется для трафика. Ниже перечислены возможные состояния порта.

Disabled (Отключено) - протокол STP отключен на этом порте. Порт будет передавать весь трафик при распознавании MAC-адреса.

Blocking (Блокирование) - порт в данный момент заблокирован, и его нельзя использовать для передачи трафика или распознавания MAC-адресов.

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.

Speed (Скорость) - скорость, на которой работает порт.

Path Cost (1-200,000,000) (Стоимость пути) - доля, которую этот порт вносит в стоимость пути к корню. Стоимость пути может иметь большее или меньшее значение и используется для пересылки трафика в случае переопределения маршрута пути.

Default Path Cost (Стандартная стоимость пути) - указывает, что назначена стандартная стоимость пути в соответствии с методом, выбранным на странице [Spanning Tree Global Settings](#) (Общие параметры STP).

Priority (0-240) (Приоритет от 0 до 240) - значение приоритета для порта. Значение приоритета влияет на выбор порта, когда мост имеет два порта, соединенных в петлю.

Designated Bridge ID (Идентификатор назначенного моста) - идентификатор назначенного моста.

Designated Port ID (Идентификатор назначенного порта) - идентификатор выбранного порта.

Designated Cost (Назначенная стоимость) - стоимость порта, участвующего в топологии STP. Порты с меньшей стоимостью блокируются с меньшей вероятностью, когда STP определяет циклы.

Forward Transitions (Передача при пересылке) - показывает, сколько раз порт изменял свое состояние с **Forwarding** (Пересылка) на **Disabled** (Отключено).

LAG - группа LAG, с которой связан порт.

Включение STP для порта

1. Откройте страницу [STP Port Settings](#) (Параметры STP для порта).
2. Выберите значение **Enabled** (Включено) в поле **STP Port Status** (Состояние STP для порта).
3. Определите поля **Fast Link** (Быстрая связь), **Path Cost** (Стоимость пути) и **Priority** (Приоритет).
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Протокол STP будет включен на этом порте.

Изменение параметров STP для порта

1. Откройте страницу [STP Port Settings](#) (Параметры STP для порта).
2. Измените поля **Priority** (Приоритет), **Fast Link** (Быстрая связь), **Path Cost** (Стоимость пути) и **Fast Link** (Быстрая связь).
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Параметры STP для порта будут изменены, а устройство обновлено.

Отображение таблицы STP для порта

1. Откройте страницу [STP Port Settings](#) (Параметры STP для порта).
2. Нажмите кнопку **Show All** (Показать все).

Откроется страница **STP Port Table** (Таблица STP для порта).

Определение параметров STP для порта с помощью команд консоли

В следующей таблице приведены команды консоли, соответствующие полям для определения параметров STP для порта на странице [STP Port Settings](#) (Параметры STP для порта).

Таблица 7-16. Команды консоли для определения параметров STP для порта

Команда консоли	Описание
<code>spanning-tree disable</code>	Отключение протокола STP на определенном порте.
<code>spanning-tree cost стоимость</code>	Настраивает стоимость пути STP для порта.
<code>spanning-tree port-priority приоритет</code>	Настройка приоритета порта.
<code>show spanning-tree [ethernet интерфейс port-channel номер_канала_порта]</code>	Отображение конфигурации протокола STP.
<code>spanning-tree portfast</code>	Включение режима PortFast.

Далее приведен пример команд консоли.

```
Console (config)# interface ethernet g5
```

```
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 g1
```

Interface	Port ID	Designated				Port ID
Name	Prio.Nbr	Cost	Sts	Cost Bridge ID	Prio.Nbr	
-----	-----	---	--	-----	-----	
g1	128.1	19	FWD	38 32768 0030.9441.62c1	128.25	

```
Spanning tree enabled
```

```
Type: point-to-point (configured
```

```
: auto)
```

```
Port Fast: no (configured: no)
```

Определение параметров STP для LAG

Чтобы назначить параметры STP для объединенных портов, используйте страницу [STP LAG Settings](#) (Параметры STP для LAG). Чтобы открыть страницу [STP LAG Settings](#) (Параметры STP для LAG), выберите **Switch** (Коммутатор) → **Spanning Tree** (Протокол STP) → **LAG Settings** (Параметры LAG) на панели дерева.

Рис. 7-22. Страница STP LAG Settings (Параметры STP для LAG)



Страница [STP LAG Settings](#) (Параметры STP для LAG) содержит следующие поля:

Select a LAG (Выбор LAG) - номер LAG, для которого необходимо изменить параметры STP.

STP (Протокол STP) - включает или отключает протокол STP для группы LAG.

Fast Link (Быстрая связь) - включает режим быстрой связи для LAG. Если режим быстрой связи для группы LAG включен, то **LAG State** (Состояние LAG) автоматически переводится в состояние **Forwarding** (Пересылка) сразу после появления связи. Режим Fast Link (Быстрая связь) оптимизирует время, которое требуется протоколу STP для сходимости. Для сходимости протокола STP в больших сетях может потребоваться от 30 до 60 секунд.

LAG State (Состояние LAG) - текущее состояние протокола STP для группы LAG. Если этот параметр включен, действие пересылки, которое выполняется с трафиком, определяется по состоянию LAG. Если мост выявляет неполадки в работе группы LAG, то она переводится в состояние **Broken** (Оборвано). Ниже указаны возможные состояния LAG.

Disabled (Отключено) - протокол STP отключен для LAG. LAG будет передавать весь трафик при распознавании MAC-адресов.

Blocking (Блокирование) - группа LAG в данный момент заблокирована и не может использоваться для передачи трафика или распознавания MAC-адресов.

Listening (Прослушивание) - LAG находится в режиме прослушивания и не может использоваться для передачи трафика или распознавания MAC-адресов.

Learning (Распознавание) - LAG находится в режиме распознавания и не может пересылать трафик, но может распознавать новые MAC-адреса.

Forwarding (Пересылка) - LAG находится в режиме передачи и может пересылать трафик и распознавать новые MAC-адреса.

Broken (Оборвано) - LAG функционирует не правильно, и ее нельзя использовать для пересылки трафика.

Path Cost (1-200000000) (Стоимость пути) - доля, которую эта группа LAG вносит в стоимость пути к корню. Стоимость пути может иметь большее или меньшее значение и используется для пересылки трафика в случае переопределения маршрута пути.

Default Path Cost (Стандартная стоимость пути) - указывает, что назначена стандартная стоимость пути в соответствии с методом, выбранным на странице [Spanning Tree Global Settings](#) (Общие параметры STP).

Priority (0-240) (Приоритет) - значение приоритета для LAG. Значение приоритета влияет на выбор LAG, когда на мосту два порта соединены в петлю. Значения приоритета находятся в диапазоне 0-240 с шагом 16.

Designated Bridge ID (Идентификатор назначенного моста) - идентификатор назначенного моста.

Designated Port ID (Идентификатор назначенного порта) - идентификатор назначенного порта.

Designated Cost (Назначенная стоимость) - стоимость порта, участвующего в топологии STP. Порты с меньшей стоимостью блокируются с меньшей вероятностью, когда STP определяет циклы.

Forward Transitions (Передача при пересылке) - показывает, сколько раз **LAG State** (Состояние LAG) изменялось с **Forwarding** (Пересылка) на **Disabled** (Отключено).

Изменение параметров STP для группы LAG

1. Откройте страницу **STP LAG Settings** (Параметры STP для LAG).
2. Выберите LAG в раскрывающемся меню **Select a LAG** (Выбор LAG).
3. Выполните необходимые изменения в полях.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Параметры STP для группы LAG будут изменены, а устройство обновлено.

Определение параметров STP для LAG с помощью команд консоли

В следующей таблице приведены команды консоли для определения параметров STP для LAG.

Таблица 7-17. Команды консоли для определения параметров STP для LAG

Команда консоли	Описание
<code>spanning-tree</code>	Включает STP.
<code>spanning-tree cost стоимость</code>	Настраивает стоимость пути STP для порта.
<code>spanning-tree port-priority приоритет</code>	Настройка приоритета порта.
<code>show spanning-tree [ethernet интерфейс port-channel номер_канала_порта]</code>	Отображение конфигурации протокола STP.
<code>spanning-tree portfast</code>	Включает режим Port Fast.

Далее приведен пример команд консоли.

```
Console(config)# interface port-channel 1
```

```

Console(config-if)# spanning-tree disable

Console(config-if)# spanning-tree cost 35000

Console(config-if)# spanning-tree port-priority 96

Console(config-if)# spanning-tree portfast

Console(config-if)# exit

Console(config)# exit

Console# show spanning-tree port-channel 1

Interface Port ID Designated Port ID

Name Prio Sts Enb Cost Cost Bridge Id Prio.Nbr

-----

----- ch1 96 DSBL FALSE 35000 0 32768 00:00:b0:11:00:00 96 25

Spanning tree disabled

Port Fast: yes (configured: yes)

Type: point-to-point (configured: auto)

Number of transitions to forwarding state: 0

```

Определение протокола RSTP

Если классический протокол spanning tree не позволяет выполнить пересылку циклов Layer 2 в общей топологии сети, период сходимости может достигать 30-60 секунд. Эта задержка позволяет определить возможные циклы, а также распространить данные об изменениях состояния.

Протокол RSTP (Rapid Spanning Tree Protocol) выявляет и использует топологию сети, обеспечивая лучшую сходимость для протокола STP без образования циклов пересылки. Чтобы открыть страницу Rapid Spanning Tree (RSTP), выберите **Switch** (Коммутатор) → **Spanning Tree** (Протокол STP) → **Rapid Spanning Tree** (Протокол RSTP) на панели дерева.

Рис. 7-23. Страница Rapid Spanning Tree (RSTP)



Interface (Интерфейс) - порт или LAG, для которого включен протокол RSTP.

Fast Link Operational Status (Рабочее состояние быстрой связи) - указывает, включен или выключен режим быстрой связи для порта или LAG. Если для порта включен режим быстрой связи, то он автоматически переводится в состояние пересылки.

Point-to-Point Admin Status (Состояние администрирования соединения «точка-точка») - включает или отключает для устройства возможность установки соединения «точка-точка» или определяет возможность автоматического соединения «точка-точка».

Чтобы установить связь через соединение «точка-точка», PPP сначала посылает пакеты LCP (Link Control Protocol) и настройки для проверки соединения канала передачи данных. После установки соединения согласовывается дополнительное оборудование в соответствии с требованиями протокола LCP, PPP источника посылает пакеты Network Control Protocols (NCP) для выбора и настройки одного или нескольких уровней протокола уровня сети. После настройки каждого из выбранных протоколов уровня сети пакеты с каждого протокола уровня сети могут посылаться по каналу связи. Канал остается настроенным для связи до тех пор, пока он не будет закрыт с помощью пакетов LCP или NCP или не произойдет некоторое внешнее событие. Это реальный тип соединения порта коммутатора. Он может отличаться от административного состояния.

Point-to-Point Operational Status (Рабочее состояние соединения «точка-точка») - показывает рабочее состояние соединения «точка-точка».

Activate Protocol Migration Test (Активизировать тест миграции протокола) - если установлен этот флажок, то PPP разрешено посылать пакеты LCP (Link Control Protocol) для проверки и настройки соединения для передачи данных.

Включение RSTP

1. Откройте страницу Rapid Spanning Tree (RSTP).
2. Определите поля **Point-to-Point Admin**, **Point-to-Point Oper** и **Activate Protocol Migration**.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Протокол Rapid STP будет включен, а устройство обновлено.

Отображение таблицы Rapid Spanning Tree (RSTP)

1. Откройте страницу Rapid Spanning Tree (RSTP).
2. Нажмите кнопку **Show All** (Показать все).

Откроется страница **Rapid Spanning Tree (RSTP) Table** (Таблица Rapid Spanning Tree (RSTP)).

Определение параметров Rapid STP с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для определения параметров Rapid RSTP, как показано на странице **RSTP**.

Таблица 7-18. Команды консоли для определения параметров Rapid STP

Команда консоли	Описание
<code>spanning-tree link-type {point-to-point shared}</code>	Переопределяет тип связи по умолчанию.

Далее приведен пример команд консоли.

```
Console (config)# interface ethernet g5
```

```
Console(config-if)# spanning-tree link-type shared
```

Определение протокола MST

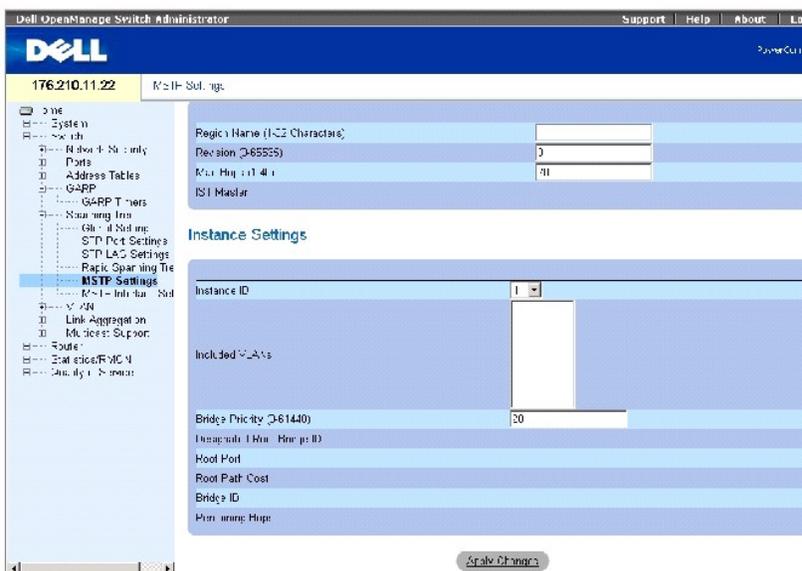
Протокол MSTP (Multiple Spanning Tree Protocol) сопоставляет сети VLAN в экземплярах STP.

Протокол MSTP обеспечивает другой сценарий выравнивания нагрузки. Например, при блокировке порта А в одном экземпляре STP этот порт переходит в состояние пересылки в другом экземпляре STP. На странице [MSTP Settings](#) (Параметры MSTP) можно определить до шестнадцати экземпляров MSTP для устройства.

Кроме того, пакеты, назначенные разным VLAN, передаются через разные пути в областях MST. Области являются один или несколько мостов Multiple Spanning Tree с одинаковой настройкой MSTP. В настройке MST определяется область MST, к которой принадлежит устройство. В настройке содержится имя, версия и область, к которой принадлежит устройство.

Чтобы открыть страницу [MSTP Settings](#) (Параметры MSTP), выберите Switch (Коммутатор)→ Spanning Tree (Протокол STP)→ MSTP Region Configuration (Настройка области MSTP) на панели дерева.

Рис. 7-24. Страница MSTP Settings (Параметры MSTP)



Страница [MSTP Settings](#) (Параметры MSTP) содержит следующие поля:

Region Name (1-32) (Имя области) - указывает имя области MST, определяемое пользователем.

Revision (0-65535) (Версия) - указывает 16-битное число без знака, определяющее версию текущей настройки MST. Номер версии необходим для настройки MST.

Max Hops (1-40) (Максимальное число узлов) - указывает общее число узлов, возникающих в определенной области, перед тем как пакеты BPDU будут отброшены. После того как пакеты BPDU будут отброшены, срок хранения информации о порте истечет. Значение поля по умолчанию: 20.

IST Master (Мастер IST) - указывает идентификатор мастера Internal Spanning Tree. IST Master (Мастер IST) - корень указанной реализации (реализация - 0).

Instance ID (Идентификатор экземпляра) - указывает идентификатор экземпляра протокола STP. Диапазон значений поля: 1-15.

Included VLANs (Включаемые VLAN) - привязка выбранных VLAN к выбранному экземпляру. Каждая группа VLAN принадлежит только одному экземпляру.

Bridge Priority (0-61440) (Приоритет моста) - указывает приоритет устройства для выбора экземпляра протокола STP.

Designated Root Bridge ID (Идентификатор назначенного корневого моста) - указывает идентификатор моста с самой низкой стоимостью пути к корню экземпляра.

Root Port (Корневой порт) - указывает корневой порт выбранного экземпляра.

Root Path Cost (Стоимость пути к корню) - указывает стоимость пути выбранного экземпляра к корню области.

Bridge ID (Идентификатор моста) - указывает идентификатор моста выбранного экземпляра.

Remaining Hops (Осталось узлов) - указывает оставшееся число узлов до следующей сети назначения.

Отображение страницы MSTP VLAN to Instance Mapping Table (Таблица привязки экземпляра к MSTP VLAN)

1. Откройте страницу [MSTP Settings](#) (Параметры MSTP).
2. Нажмите кнопку **Show All** (Показать все).

Откроется страница [MSTP VLAN to Instance Mapping Table](#) (Таблица привязки экземпляра к MSTP VLAN):

Рис. 7-25. Страница MSTP VLAN to Instance Mapping Table (Таблица привязки экземпляра к MSTP VLAN)

Refresh

MSTP VLAN to Instance Mapping Table

VLAN	Instance ID	Имя
1 VLAN1	0	
2 VLAN2	0	
3 VLAN3	11	
4 VLAN4	0	

Apply Changes

Определение экземпляров MST с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для определения групп экземпляров MST, как отображается на странице [MSTP Settings](#) (Параметры MSTP).

Таблица 7-19. Команды консоли для экземпляров MSTP

Команда консоли	Описание
<code>spanning-tree mst configuration</code>	Включает режим настройки MST.
<code>instance instance-id {add remove} vlan vlan-range</code>	Привязывает VLAN к экземпляру MST.
<code>name string</code>	Задаёт имя настройки.
<code>revision value</code>	Задаёт номер версии настройки
<code>spanning-tree mst instance-id port-priority приоритет</code>	Устанавливает приоритет порта.
<code>spanning-tree mst instance-id priority приоритет</code>	Устанавливает приоритет устройства для указанного экземпляра протокола STP.
<code>spanning-tree mst max-hops hop-count</code>	Устанавливает число узлов в области MST, перед тем как пакеты BPDU будут отброшены и срок хранения информации о порте истечёт.
<code>spanning-tree mst instance-id cost cost</code>	Устанавливает стоимость пути порта для вычислений MST
<code>exit</code>	Выход из режима настройки MST с сохранением изменений.
<code>abort</code>	Выход из режима настройки MST без сохранения изменений.
<code>show {current pending}</code>	Отображает текущую или незаконченную настройку области MST.

Далее приведен пример команд консоли.

```
Console(config)# spanning-tree mst configuration
```

```
Console(config-mst)# instance 1 add vlan 10-20
```

```
Console(config-mst)# name region1
```

```
Console(config-mst)# revision 1
```

```
Console(config)# spanning-tree mst configuration
```

```
Console(config-mst)# instance 2 add vlan 21-30
```

```
Console(config-mst)# name region1
```

```
Console(config-mst)# revision 1
```

```
Console(config-mst)# show pending
```

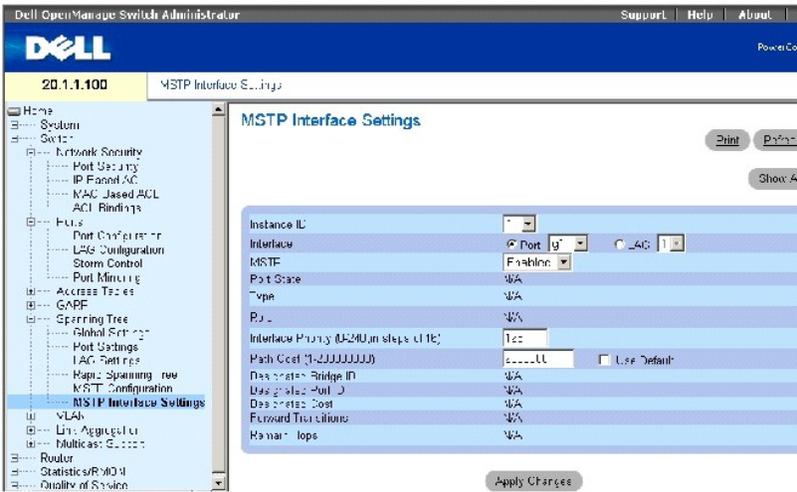
Pending MST configuration	
Имя: Region1	
Revision: 1	
Instance	Vlans Mapped
-----	-----
0	1-9,31-4094
1	10-20
2	21-30

Определение параметров интерфейса MSTP

Страница [MSTP Interface Setting](#) (Параметры интерфейса MSTP) позволяет назначить параметры MSTP для определенных интерфейсов.

Чтобы открыть страницу [MSTP Interface Setting](#) (Параметры интерфейса MSTP), выберите Switch (Коммутатор) → Spanning Tree (Протокол STP) → MSTP Interface Setting (Параметры интерфейса MSTP) на панели дерева.

Рис. 7-26. Страница MSTP Interface Setting (Параметры интерфейса MSTP)



Страница [MSTP Interface Setting](#) (Параметры интерфейса MSTP) содержит следующие параметры:

Instance ID (Идентификатор экземпляра) - перечисляет экземпляры MSTP, настроенные на устройстве. Возможные значения поля: 0-15.

Interface (Интерфейс) - назначает порты или LAG для выбранного экземпляра MSTP.

Port State (Состояние порта) - указывает, включен или выключен порт в определенном экземпляре.

Type (Тип) - указывает, является ли порт для MSTP двухточечным или он подключен к концентратору, а также является ли порт внутренним для области MST или граничным. Если порт является граничным, параметр также указывает, работает ли устройство на другом конце линии в режиме RSTP или STP.

Role (Роль) - указывает роль порта, назначаемого алгоритмом STP для указания для путей STP. Возможные значения:

Root (Корневой) - предоставляет путь с наименьшими затратами для пересылки пакетов в корневое устройство.

Designated (Назначенный) - указывает порт или группу LAG, с помощью которых назначенное устройство подключено к LAN.

Alternate (Альтернативный) - предлагает альтернативный путь к корневому устройству из интерфейса.

Backup (Резервный) - предлагает резервный путь к указанной LAN. Резервные порты требуются только в том случае, когда два порта соединены в петлю с помощью соединения «точка-точка». Резервные порты также необходимы, когда LAN имеет два или более соединений к сегменту с общим доступом.

Disabled (Отключено) - указывает, что порт не участвует в соединении по протоколу STP.

Interface Priority (Приоритет интерфейса) - определяет приоритет интерфейса для указанного экземпляра. Значения приоритета находятся в диапазоне 0-240 с шагом 16. Значение по умолчанию: 128.

Path Cost (Стоимость пути) - указывает долю, которую порт вносит в экземпляр протокола STP. Значение должно всегда быть в диапазоне: 1-200000000.

Default Path Cost (Стандартная стоимость пути) - указывает, что назначена стандартная стоимость пути в соответствии с методом, выбранным на странице [Spanning Tree Global Settings](#) (Общие параметры STP).

Designated Bridge ID (Идентификатор назначенного моста) - номер идентификатора моста, связывающего соединение или общую LAN с корнем.

Designated Port ID (Идентификатор назначенного порта) - номер идентификатора порта на назначенном мосту, связывающем соединение или общую LAN с корнем.

Designated Cost (Назначенная стоимость) - стоимость пути от соединения или общей LAN к корню.

Forward Transitions (Передача при пересылке) - показывает, сколько раз порт изменял свое состояние на **forwarding** (пересылка).

Remain Hops (Осталось узлов) - указывает оставшееся число узлов до следующей сети назначения.

Просмотр страницы MSTP Interface Table (Таблица интерфейса MSTP)

1. Откройте страницу [MSTP Interface Setting](#) (Параметры интерфейса MSTP).
2. Нажмите кнопку **Show All** (Показать все).

Откроется страница [MSTP Interface Table](#) (Таблица интерфейса MSTP):

Рис. 7-27. Страница MSTP Interface Table (Таблица интерфейса MSTP)



Определение интерфейса MSTP с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для определения интерфейсов MSTP, как отображается на странице [MSTP Interface Setting](#) (Параметры интерфейса MSTP).

Таблица 7-20. Команды консоли для интерфейса MSTP

Команда консоли	Описание
<code>spanning-tree mst instance-id cost cost</code>	Устанавливает стоимость пути порта для вычислений MST.
<code>spanning-tree mst instance-id priority приоритет</code>	Устанавливает приоритет устройства для указанного экземпляра протокола STP.
<code>show spanning-tree mst- configuration</code>	Отображает настройку MST.

Далее приведен пример команд консоли.

```
Console (config)# interface ethernet g9
```

```
Console (config-if) # spanning-tree mst 1 cost 4
```

```
Console (config-if)# spanning-tree mst 1 port-priority 142
```

```
Console (config-if)# end
```

```
Console# show spanning-tree
```

```
Spanning tree enabled mode MSTP
```

```
Default port cost method: long
```

```
##### MST 0 Vlans Mapped: 1-9, 21-4094
```

```
CST Root ID Priority 32768
```

```
Address 00:01:42:97:e0:00
```

```
Path Cost 20000
```

```
Root Port 1 (ig)
```

```
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
IST Master ID Priority 32768
```

```
Address 00:02:4b:19:7a:00
```

```
Path Cost 10000
```

```
Rem hops 19
```

```
Bridge ID Priority 32768
```

```
Address 00:02:4b:29:7a:00
```

```
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Max hops 20
```

Настройка сетей VLAN

VLAN - это логические подгруппы сети, созданные программным, а не аппаратным путем. Группы VLAN объединяют пользовательские станции и сетевые устройства в одну группу независимо от того, к какому физическому сегменту LAN они подключены. Сети VLAN позволяют сделать более эффективным поток сетевого трафика в пределах подгрупп. Группы VLAN, управляемые с помощью программы, уменьшают время реализации изменений, добавлений и перемещений в сети.

Минимальное число портов в VLAN не ограничено. Группы VLAN могут объединяться по модулям, по устройствам, по стеку или любым другим логическим соединениям, поскольку группы VLAN определяются на уровне программы, а не с помощью физических атрибутов.

Сети VLAN работают на уровне Layer 2. Поскольку они изолируют трафик внутри себя, для обеспечения трафика между группами VLAN необходим маршрутизатор уровня Layer 3, поддерживающий соответствующий уровень протокола. Маршрутизаторы уровня Layer 3 идентифицируют сегменты и координируют их с сетями VLAN. Группы VLAN - это широковещательные и многоадресные домены. Широковещательный и многоадресный трафик передается только в той сети VLAN, где он создается.

Маркировка сетей VLAN обеспечивает способ передачи информации VLAN между группами VLAN. При маркировке VLAN к заголовкам пакета присоединяется метка размером 4 байта. Метка VLAN указывает, к какой сети VLAN принадлежит пакет. Метки VLAN присоединяются к пакету на конечной станции или сетевом устройстве. Метки VLAN также содержат сведения о приоритете сетей VLAN.

Совместное использование сетей VLAN и протокола GVRP позволяет менеджерам сети объединять узлы сети в широковещательные домены. Широковещательный и многоадресный трафик ограничивается только передающей группой.

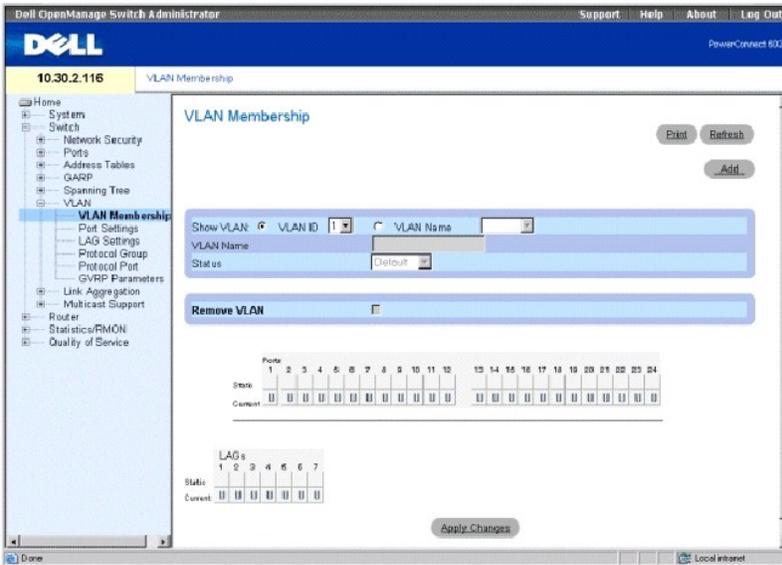
Чтобы отобразить страницу VLAN, выберите Switch (Коммутатор) → VLAN на панели дерева.

Определение принадлежности к группе VLAN

Используйте страницу VLAN Membership (Принадлежность к VLAN), чтобы определить группы VLAN.

Чтобы открыть страницу VLAN Membership (Принадлежность к VLAN), выберите Switch (Коммутатор) → VLAN → VLAN Membership (Принадлежность к VLAN) на панели дерева.

Рис. 7-28. Страница VLAN Membership (Принадлежность VLAN)



Страница **VLAN Membership** (Принадлежность VLAN) содержит [VLAN Membership Table](#) (Таблица принадлежности VLAN) и [VLAN Port Membership Table](#) (Таблица принадлежности портов VLAN).

Таблица принадлежности VLAN

Страница **VLAN Membership Table** (Таблица принадлежности VLAN) содержит параметры для включения портов в состав VLAN. Коммутатор поддерживает одновременно до 4095 групп VLAN. Однако в действительности можно создать только 4062 группы VLAN, поскольку:

- 1 Группы VLAN с номерами от 4064 до 4094 зарезервированы устройством для внутреннего использования.
- 1 VLAN 1 - это группа VLAN по умолчанию, все порты которой по умолчанию принадлежат этой группе.
- 1 VLAN 4095 определена как «Игнорируемая VLAN».

Show VLAN (Отобразить VLAN) - выводит информацию по конкретной группе VLAN в соответствии с идентификатором VLAN или именем VLAN.

VLAN Name (Имя сети VLAN) - показывает имя сети VLAN, задаваемое пользователем.

Status (Состояние) - указывает тип VLAN. Возможные значения:

Dynamic (Динамическая) - показывает, что VLAN была динамически создана при использовании протокола GVRP.

Static (Статическая) - показывает, что VLAN определена пользователем.

Remove VLAN (Удалить VLAN) - когда установлен этот параметр, VLAN удаляется из таблицы принадлежности VLAN.

Добавление новых сетей VLAN

- 1 Откройте страницу **VLAN Membership** (Принадлежность VLAN).
- 2 Щелкните **Add** (Добавить), чтобы отобразить страницу **Create New VLAN** (Создание новой VLAN).
- 3 Введите идентификатор и имя VLAN.
- 4 Нажмите кнопку **Apply Changes** (Применить изменения).

Новая группа VLAN будет добавлена, а устройство обновлено.

Изменение групп принадлежности VLAN

1. Откройте страницу **VLAN Membership** (Принадлежность VLAN).
2. Выберите сеть VLAN в раскрывающемся списке **Show VLAN** (Отобразить VLAN).
3. Выполните необходимые изменения в полях.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Информация о принадлежности VLAN будет изменена, а устройство обновлено.

Удаление групп принадлежности VLAN

1. Откройте страницу **VLAN Membership** (Принадлежность VLAN).
2. Выберите сеть VLAN в поле **Show VLAN** (Отобразить VLAN).
3. Установите флажок **Remove VLAN** (Удалить VLAN).
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Группа VLAN будет удалена, а устройство обновлено.

Определение групп принадлежности VLAN с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для определения принадлежности групп VLAN, как показано на странице **VLAN Membership** (Принадлежность VLAN).

Таблица 7-21. Команды консоли для определения принадлежности VLAN

Команда консоли	Описание
vlan database	Включает режим настройки интерфейса (VLAN).
vlan {диапазон_vlan}	Создает VLAN.
name строка	Добавляет имя в VLAN.

Далее приведен пример команд консоли.

```
console (config)#interface vlan 1972
```

```
console (config-if)#name Marketing
```

Таблица принадлежности портов VLAN

Таблица портов VLAN содержит таблицу портов для назначения портов в группы VLAN. Принадлежность портов к VLAN определяется путем переключения параметров **Port Control** (Управление портом). Порты могут иметь следующие значения:

Таблица 7-22. Таблица принадлежности портов VLAN

Управление портом	Описание
T	Интерфейс входит в VLAN. Все пакеты, пересылаемые интерфейсом, помечаются. Пакеты содержат информацию о VLAN.
U	Интерфейс входит в VLAN. Пакеты, пересылаемые интерфейсом, не помечаются.
F	Интерфейсу отказано в принадлежности VLAN.
Пусто	Интерфейс не входит в VLAN. Пакеты, связанные с интерфейсом, не пересылаются.

В VLAN Port Membership Table (Таблица принадлежности портов VLAN) отображаются порты и состояния портов, а также группы LAG.

Назначение портов в группу VLAN

1. Откройте страницу **VLAN Membership** (Принадлежность VLAN).
2. Нажмите кнопку **VLAN ID** (Идентификатор VLAN) или **VLAN Name** (Имя VLAN) и выберите VLAN в раскрывающемся меню.
3. Выберите порт в **Port Membership Table** (Таблица принадлежности портов) и назначьте значение для порта.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Порт будет назначен в группу VLAN, а устройство будет обновлено.

Удаление VLAN

1. Откройте страницу **VLAN Membership** (Принадлежность VLAN).
2. Нажмите кнопку **VLAN ID** (Идентификатор VLAN) или **VLAN Name** (Имя VLAN) и выберите VLAN в раскрывающемся меню.
3. Установите флажок **Remove VLAN** (Удалить VLAN).
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Группа VLAN будет удалена, а устройство обновлено.

Назначение портов в VLAN с помощью команд консоли

Следующая таблица содержит команды консоли для назначения портов в группы VLAN.

Таблица 7-23. Команды консоли для назначения портов в группы VLAN

Команда консоли	Описание
<code>switchport general acceptable-frame-types tagged-only</code>	Отбрасывает входящие непомеченные кадры.
<code>switchport forbidden vlan {add список_сетей_vlan remove список_сетей_vlan}</code>	Запрещает добавление указанных VLAN для порта.

Примеры команд консоли:

```
Console (config)# interface ethernet g1
```

```
Console(config-if)#switchport general acceptable-frame-types tagged-only
```

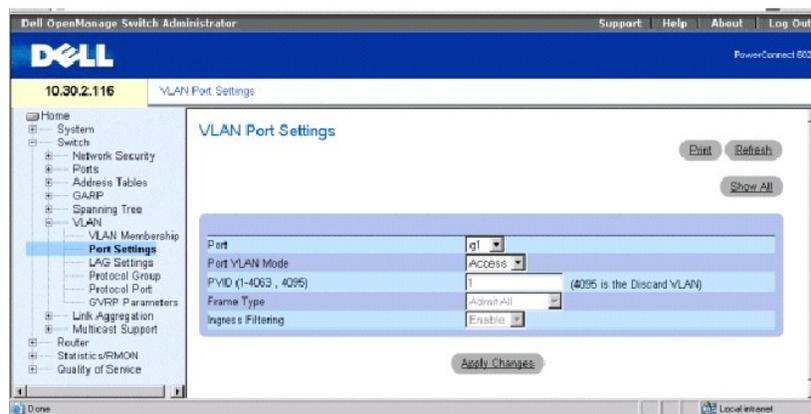
```
Console (config-if)#switchport forbidden vlan add 234-256
```

Определение параметров VLAN для порта

Для изменения параметров управления портами, входящими в состав сети VLAN, используйте страницу **VLAN Port Settings** (Параметры VLAN для порта). Идентификатор по умолчанию VLAN (PVID) для порта настраивается на странице **VLAN Port Settings** (Параметры VLAN для порта). Все непомеченные пакеты, поступающие на устройство, маркируются идентификатором PVID портов.

Чтобы открыть страницу **VLAN Port Settings** (Параметры VLAN для порта), выберите **Switch** (Коммутатор) → **VLAN** → **Port Settings** (Параметры порта) на панели дерева.

Рис. 7-29. Страница VLAN Port Settings (Параметры VLAN для порта)



Port (Порт) - номер порта, входящего в VLAN.

Port VLAN Mode (Режим порта VLAN) - показывает режим работы порта. Возможные значения:

General (Общий) - порт принадлежит нескольким группам VLAN, каждая из них определена пользователем как помеченная или непомеченная (дуплексный режим 802.1Q).

Access (Доступен) - порт принадлежит к одной непомеченной группе VLAN. Когда порт находится в режиме доступа (Access), типы пакетов, которые принимаются на порт (packet type), нельзя назначить. Кроме того, невозможно включить или отключить входящий фильтр на порте доступа.

Trunk (Транк) - порт принадлежит VLAN, в которой помечаются все порты (кроме необязательной одной «родной» VLAN).

PVID (1-4063, 4095) - присваивает идентификатор VLAN непомеченным пакетам. Допустимые значения поля: 1-4063 и 4095. VLAN 4095 определяется в соответствии со стандартом и принятой практикой в отрасли, как «discard VLAN». Пакеты, определенные в эту группу VLAN, опускаются.

Frame Type (Тип кадра) - тип кадров, принимаемый портом. Возможные значения:

Admit Tag Only (Разрешить только помеченные) - показывает, что порт принимает только помеченные кадры.

Admit All (Разрешить все) - показывает, что порт принимает и помеченные, и немеченные кадры.

Ingress Filtering (Фильтрация на входе) - включает или отключает фильтрацию на входе для порта. При фильтрации на входе отклоняются кадры, метка VLAN которых не совпадает с портом VLAN.

Назначение параметров порта

1. Откройте страницу **VLAN Port Settings** (Параметры VLAN для порта).
2. Выберите порт, для которого необходимо назначить параметры, в раскрывающемся списке **Port** (Порт).
3. Введите значения в необходимые поля и нажмите кнопку **Apply Changes** (Применить изменения).

Параметры порта VLAN будут определены, а устройство будет обновлено.

Отображение таблицы портов VLAN

1. Откройте страницу **VLAN Port Settings** (Параметры VLAN для порта).
2. Нажмите кнопку **Show All** (Показать все), чтобы отобразить страницу **VLAN Port Table** (Таблица портов VLAN).

 **ПРИМЕЧАНИЕ.** Если выбран порт **Access** (Доступ), типы пакетов, которые принимаются на порт (packet type), нельзя назначить. Кроме того, невозможно включить или отключить входящий фильтр на порте доступа.

Назначение портов в VLAN с помощью команд консоли

Следующая таблица содержит команды консоли для назначения портов в группы VLAN.

Таблица 7-24. Команды консоли для назначения портов в группы VLAN

Команда консоли	Описание
<code>switchport mode { access trunk general }</code>	Настраивает режим принадлежности VLAN для порта.
<code>switchport trunk native vlan идентификатор_vlan</code>	Определяет принадлежность порта к указанной группе VLAN, а также определяет идентификатор VLAN как «идентификатор VLAN по умолчанию для порта (PVID)».
<code>switchport general pvid идентификатор_vlan</code>	Настраивает идентификатор VLAN (PVID) для порта, если интерфейс работает в общем режиме.
<code>switchport general allowed vlan add список_vlan [tagged untagged]</code>	Добавляет или удаляет группы VLAN из порта, работающего в общем режиме.
<code>switchport general acceptable-packet- types tagged-only</code>	Отбрасывает немеченные входящие пакеты.
<code>switchport general ingress-filtering disable</code>	Отключает фильтрацию на входе для порта.
<code>shutdown</code>	Отключает интерфейсы.
<code>set interface active {ethernet интерфейс port-channel номер_канала_порта}</code>	Вновь активизирует интерфейс, отключенный по причинам безопасности.

Далее приведен пример команд консоли.

```
Console (config)# interface ethernet g8
```

```
Console (config-if)# switchport mode access
```

```
console (config-if)# switchport trunk native vlan 123
```

```
Console (config-if)# switchport general pvid 234
```

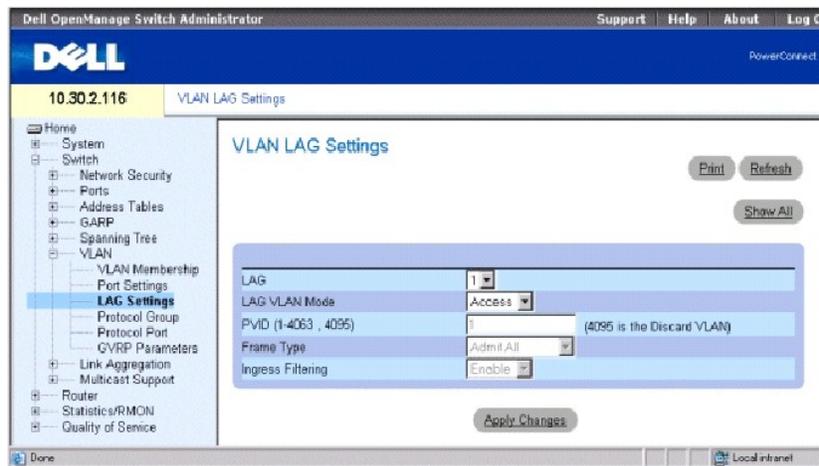
```
Console (config-if)# switchport general allowed vlan add 1,2,5,6 tagged
```

```
Console (config-if)# switchport general acceptable-packet-types tagged-only
```

Определение параметров группы LAG группы VLAN

На странице **VLAN LAG Settings** (Параметры группы LAG сети VLAN) приведены параметры для управления группами LAG, входящими в состав VLAN. Сети VLAN состоят из отдельных портов или групп LAG. Непомеченные пакеты, поступающие на коммутатор, помечаются с помощью идентификатора групп LAG в соответствии с идентификатором PVID. Чтобы открыть страницу **VLAN LAG Settings** (Параметры группы LAG сети VLAN), выберите **Switch** (Коммутатор) → **VLAN** → **LAG Settings** (Параметры LAG) на панели дерева.

Рис. 7-30. Страница VLAN LAG Settings (Параметры группы LAG сети VLAN)



LAG - номер LAG, входящей в сеть VLAN.

LAG VLAN Mode (Режим LAG VLAN) - указывает режим VLAN LAG. Возможные значения:

General (Общий) - порт принадлежит нескольким группам VLAN, каждая из них определена пользователем как помеченная или непомеченная (дуплексный режим 802.1Q).

Access (Доступна) - группа LAG принадлежит одной непомеченной группе VLAN.

Trunk (Транк) - LAG принадлежит группе VLAN, в которой все порты помечаются (кроме необязательной «родной» VLAN).

PVID (1-4063, 4095) - присваивает идентификатор VLAN непомеченным пакетам. Допустимые значения поля: 1-4063 и 4095. VLAN 4095 определяется в соответствии со стандартом и принятой практикой в отрасли, как «discard VLAN». Пакеты, определенные в эту группу VLAN, опускаются.

Frame Type (Тип кадра) - тип пакетов, принимаемый группой LAG. Возможные значения:

Admit Tag Only (Разрешить только помеченные) - группа LAG принимает только помеченные пакеты.

Admit All (Разрешить все) - группа LAG принимает и помеченные, и непомеченные пакеты.

Ingress Filtering (Фильтрация на входе) - включает или отключает фильтрацию на входе для LAG. При фильтрации на входе отклоняются пакеты, метка VLAN которых не совпадает с LAG VLAN.

Назначение параметров VLAG

1. Откройте страницу **VLAN LAG Settings** (Параметры группы LAG сети VLAN).
2. Выберите LAG в раскрывающемся меню **LAG** и заполните поля на странице.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Параметры группы LAG сети VLAN будут определены, а устройство обновлено.

Отображение таблицы групп LAG для VLAN

1. Откройте страницу **VLAN LAG Settings** (Параметры группы LAG сети VLAN).
2. Нажмите кнопку **Show All** (Показать все), чтобы отобразить страницу **VLAN LAG Table** (Таблица VLAN LAG).

Назначение групп LAG в сети VLAN с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для назначения групп LAG группам VLAN, как показано на странице **VLAN LAG Settings** (Параметры группы LAG сети VLAN).

Таблица 7-25. Команды консоли для назначения групп LAG VLAN

Команда консоли	Описание
<code>switchport mode {access trunk general}</code>	Настраивает режим принадлежности VLAN для порта.
<code>switchport trunk native vlan идентификатор_vlan</code>	Определяет принадлежность порта к указанной группе VLAN, а также определяет идентификатор VLAN как «идентификатор VLAN по умолчанию для порта (PVID)».
<code>switchport general pvid идентификатор_vlan</code>	Настраивает идентификатор VLAN (PVID) для порта, если интерфейс работает в общем режиме.
<code>switchport general allowed vlan add список_ vlan [tagged untagged]</code>	Добавляет или удаляет группы VLAN из порта, работающего в общем режиме.
<code>switchport general acceptable-frame-type tagged-only</code>	Отбрасывает непомеченные входящие пакеты.
	Отключает фильтрацию на входе для порта.

```
switchport general ingress-filtering disable
```

Далее приведен пример команд консоли.

```
Console (config-if)# switchport mode access
```

```
Console (config-if)# switchport trunk native vlan 123
```

```
Console (config-if)# switchport general pvid 234
```

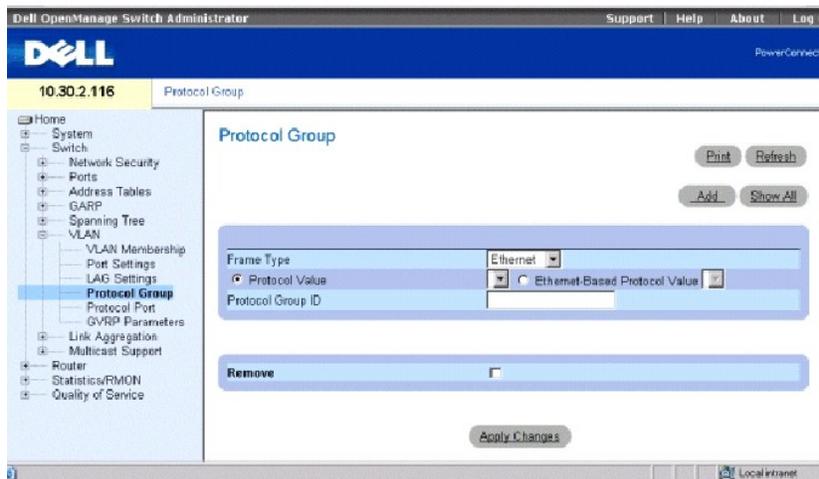
```
Console (config-if)# switchport general allowed vlan add 1,2,5,6 tagged
```

```
Console (config-if)# switchport general acceptable-frame-type tagged-only
```

Определение групп протоколов VLAN

Страница Protocol Group (Группа протоколов) содержит информацию об именах протоколов и типе Ethernet группы VLAN. Интерфейсы можно классифицировать как интерфейс на основе определенного протокола. При классификации интерфейс помещается в группу протоколов. Чтобы открыть страницу Protocol Group (Группа протоколов), выберите Switch (Коммутатор) → VLAN → Protocol Group (Группа протоколов) на панели дерева.

Рис. 7-31. Таблица Protocol Group (Группа протоколов)



Frame Type (Тип кадра) - тип пакетов. Возможные значения поля: Ethernet, RFC1042 и LLC Other.

Protocol Value (Значение протокола) - определенное пользователем имя протокола.

Ethernet-Based Protocol Value - тип группы протокола Ethernet.

Protocol Group ID (Идентификатор группы протоколов) - номер идентификатора группы VLAN.

Добавление группы протоколов

1. Откройте страницу **Protocol Group** (Группа протоколов).
2. Щелкните **Add** (Добавить), чтобы отобразить страницу **Assign Protocol to Group** (Назначить протокол группе).
3. Введите значения в поля и нажмите кнопку **Apply Changes** (Применить изменения).

Будет назначена группа протоколов, а устройство обновлено.

Назначение параметров группе протоколов VLAN

1. Откройте страницу **Protocol Group** (Группа протоколов).
2. Введите значения в поля и нажмите кнопку **Apply Changes** (Применить изменения).

Параметры группы протоколов VLAN будут определены, а устройство обновлено.

Удаление протоколов из таблицы группы протоколов

1. Откройте страницу **Protocol Group** (Группа протоколов).
2. Нажмите кнопку **Show All** (Показать все), чтобы отобразить страницу **Protocol Group Table** (Таблица группы протоколов).
3. Установите флажок **Remove** (Удалить) для группы протоколов, которую необходимо удалить.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Протокол будет удален, а устройство обновлено.

Определение групп протоколов VLAN с помощью команд консоли

В следующей таблице приведены команды консоли для настройки групп протоколов.

Таблица 7-26. Команды консоли для определения групп протоколов VLAN

Команда консоли	Описание
<code>map protocol протокол [инкапсуляция] protocols -group группа</code>	Добавляет специальный протокол в именованную группу протоколов, которую можно использовать для назначения группы VLAN, основанной на протоколах.

Следующий пример протокол ip-arp назначается для группы «213»:

```
Console (config)# vlan database
```

```
Console (config-vlan)# map protocol ip-arp protocols-group 213
```

Добавление портов в протокол

Страница **Protocol Port** (Порт протокола) используется для добавления интерфейса в группу протоколов.

Чтобы открыть страницу Protocol Port (Порт протокола), выберите Switch (Коммутатор)→ VLAN→ Protocol Port (Порт протокола) на панели дерева.

Рис. 7-32. Страница Protocol Port (Порт протокола)



Interface (Интерфейс) - номер порта или группы LAG добавляемых в группу протоколов.

Protocol Group ID (Идентификатор группы протоколов) - идентификатор группы протоколов, в которую добавляется интерфейс. Идентификатор группы протоколов определяется в таблице группы протоколов.

VLAN ID (Идентификатор сети VLAN) - связывает интерфейс с идентификатором VLAN, определенным пользователем. Идентификатор VLAN определяется на странице **Create a New VLAN (Создание новой VLAN)**. Порт протокола может быть добавлен с использованием идентификатора VLAN или имени VLAN.

VLAN Name (Имя сети VLAN) - связывает интерфейс с именем VLAN, определенным пользователем. Имя VLAN определяется на странице **Create a New VLAN (Создание новой VLAN)**. Это поле доступно только на странице **Add Protocol Port (Добавление порта в протокол)**.

Remove (Удалить) - когда установлен этот флажок, порт, назначенный для VLAN или группы протоколов, удаляется.

Добавление нового порта протокола

1. Откройте страницу **Protocol Port Table (Таблица группы протоколов)**.
2. Щелкните **Add (Добавить)**, чтобы отобразить страницу **Add Protocol Port (Добавление порта протокола)**.
3. Введите значения в полях диалогового окна и нажмите кнопку **Apply Changes (Применить изменения)**.

Новая группа протоколов VLAN будет добавлена в **Protocol Port Table (Таблица группы протоколов)**, а устройство обновлено.

Определение портов протокола с помощью команд консоли

Следующая таблица содержит команды консоли для определения портов протокола.

Таблица 7-27. Команды консоли для определения портов протокола

Команда консоли	Описание
	Определяет правило классификации на основе протокола.

```
switchport general map protocols-group группа_vlan идентификатор_vlan
```

В следующем примере определяется правило классификации на основе протокола группы протоколов 1 для VLAN 8:

```
Console (config-if)# switchport general map protocols-group 1 vlan 8
```

Настройка протокола GVRP

Протокол GVRP (GARP VLAN Registration Protocol) специально предусмотрен для автоматического распределения информации о принадлежности VLAN между мостами, поддерживающими VLAN. Протокол GVRP позволяет таким мостам автоматически определять группы VLAN для назначения портов мостам, не настраивая отдельно каждый мост, и регистрировать принадлежность к VLAN.

Чтобы минимизировать требования к памяти при работе протокола GVRP, нужно добавить к стандартным переменным две специальные настраиваемые переменные:

- 1 **Maximum number of GVRP VLANs** (Максимальное количество сетей VLAN с GVRP) - количество сетей VLAN с протоколом GVRP, которые могут участвовать в работе протокола GVRP.
- 1 **Maximum number of GVRP VLANs after Reset** (Максимальное количество сетей VLAN с GVRP после сброса) - для настройки используется максимальное количество сетей VLAN с GVRP после сброса. Это значение становится действительным только после сброса параметров.

В максимальное количество VLAN с протоколом GVRP входят все группы VLAN, участвующие в работе GVRP, независимо от того, статические они или динамические.

При определении максимального количества сетей VLAN, участвующих в GVRP, путем настройки максимального количества сетей VLAN с протоколом GVRP после сброса, нужно учитывать следующее.

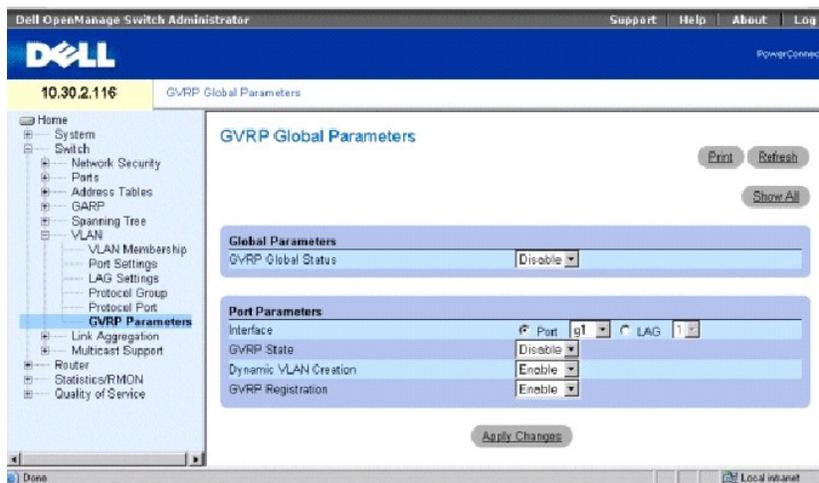
- 1 Максимальное количество сетей VLAN с протоколом GVRP по умолчанию равно 255.
- 1 Максимальное количество VLAN ограничивает (через управляющую переменную Max VLANs MIB) максимальное количество VLAN с протоколом GVRP.

Чтобы гарантировать правильную работу протокола GVRP, установите для максимального количества групп VLAN с протоколом GVRP значение, которое существенно больше суммы.

- 1 количества всех статических групп VLAN, настроенных на данный момент или ожидающих настройки;
- 1 количества всех динамических VLAN, входящих в протокол GVRP, настроенных на данный момент (начальное количество динамических сетей VLAN с протоколом GVRP равно 255) или ожидающих настройки.

Страница **GVRP Global Parameters** (Общие параметры GVRP) позволяет глобально включить GVRP. Протокол GVRP можно также включить для отдельных интерфейсов. Чтобы открыть страницу **GVRP Global Parameters** (Общие параметры GVRP), выберите **Switch** (Коммутатор) → **VLAN** → **GVRP Parameters** (Параметры GVRP) на панели дерева.

Рис. 7-33. Страница GVRP Global Parameters (Общие параметры GVRP)



GVRP Global Status (Общее состояние GVRP) - включает или отключает использование протокола GVRP на устройстве. GVRP по умолчанию отключен.

Interface (Интерфейс) - порт или группа LAG, для которой включен протокол GVRP.

GVRP State (Состояние GVRP) - включает или отключает использование протокола GVRP для интерфейса.

Dynamic VLAN Creation (Динамическое создание VLAN) - позволяет или запрещает создавать VLAN по протоколу GVRP.

GVRP Registration (Регистрация GVRP) - отображает состояние регистрации GVRP.

Включение GVRP на устройстве

1. Откройте страницу **GVRP Global Parameters** (Общие параметры GVRP).
2. Выберите значение **Enable** (Включить) в поле **GVRP Global Status** (Общее состояние GVRP).
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Протокол GVRP будет включен на этом устройстве.

Включение регистрации группы VLAN по протоколу GVRP

1. Откройте страницу **GVRP Global Parameters** (Общие параметры GVRP).
2. Для необходимого интерфейса выберите значение **Enable** (Включить) в поле **GVRP Global Status** (Общее состояние GVRP).
3. Выберите значение **Enable** (Включить) в поле **GVRP Registration** (Регистрация GVRP).
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Регистрация сети VLAN по протоколу GVRP будет включена для порта, а устройство будет обновлено.

Настройка протокола GVRP с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для настройки GVRP, как показано на странице **GVRP Global Parameters** (Общие параметры GVRP).

Таблица 7-28. Команды консоли для настройки общих параметров протокола GVRP

Команда консоли	Описание
<code>gvrp enable (global)</code>	Включает протокол GVRP для системы в целом.
<code>gvrp enable (interface)</code>	Включает протокол GVRP для интерфейса.
<code>gvrp vlan-creation-forbid</code>	Включает или отключает динамическое создание VLAN.
<code>gvrp registration-forbid</code>	Отменяет регистрацию всех динамических сетей VLAN и предотвращает динамическую регистрацию VLAN для порта.
<code>show gvrp configuration [ethernet интерфейс port- channel номер_канала_ порта]</code>	Отображает сведения о настройке протокола GVRP, в том числе значения таймеров, разрешен ли протокол GVRP или динамическое создание сети VLAN, а также какие порты работают по протоколу GVRP.
<code>show gvrp error-statistics [ethernet интерфейс port -channel номер_канала_ порта]</code>	Отображает статистику ошибок протокола GVRP.
<code>show gvrp statistics [ethernet интерфейс port- channel номер_канала_ порта]</code>	Отображает статистику протокола GVRP.
<code>clear gvrp statistics [ethernet интерфейс port- channel номер_канала_ порта]</code>	Сбрасывает всю статистику протокола GVRP.

Далее приведен пример команд консоли.

```
Console (config)# gvrp enable
```

```
Console (config)# interface ethernet g8
```

```
Console (config-if)# gvrp enable
```

```
Console (config-if)# gvrp vlan-creation-forbid
```

```
Console (config-if)# gvrp registration-forbid
```

```
Console> show gvrp configuration
```

```
GVRP Feature is currently Enabled on the device.
```

```
Maximum VLANs: 4063, Maximum VLANs after reset: 4063.
```

```
Port(s) GVRP-Status Registration Dynamic VLAN Timers(milliseconds)
```

Creation Join Leave Leave All

g1 Disabled Normal Enabled 200 600 10000

...

g7 Disabled Normal Enabled 200 600 10000

g8 Enabled Forbidden Disabled 200 600 10000

g9 Disabled Normal Enabled 200 600 10000

...

g24 Disabled Normal Enabled 200 600 10000

chl Disabled Normal Enabled 200 600 10000

...

ch7 Disabled Normal Enabled 200 600 10000

...

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
---	---	----	----	----	---	---	---	---	---	----	---	---
g1	0	0	0	0	0	0	0	0	0	0	0	0
g2	0	0	0	0	0	0	0	0	0	0	0	0
g3	0	0	0	0	0	0	0	0	0	0	0	0
g4	0	0	0	0	0	0	0	0	0	0	0	0
g5	0	0	0	0	0	0	0	0	0	0	0	0
g6	0	0	0	0	0	0	0	0	0	0	0	0
g7	0	0	0	0	0	0	0	0	0	0	0	0
g8	0	0	0	0	0	0	0	0	0	0	0	0

Console# clear gvrp statistics ethernet g8

Объединение портов

Объединение каналов оптимизирует использование портов, связывая между собой группу портов и формируя одну объединенную группу каналов LAG. Объединение портов увеличивает пропускную способность между устройствами, увеличивает гибкость портов и обеспечивает избыточность каналов.

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 формируют из них группу LAG.

При настройке объединения портов выполняйте следующие инструкции.

- 1 Все порты в группе LAG должны быть одинакового типа.
- 1 VLAN не должна быть настроена для этого порта.
- 1 Порт не должен быть назначен для другой группы LAG.
- 1 Существует MAC-адрес, который можно назначить для порта.
- 1 Режим автоматического согласования не должен быть настроен для этого порта.
- 1 Порт должен работать в дуплексном режиме.
- 1 Все порты в группе LAG должны иметь одинаковые режимы входного фильтра и пометки.
- 1 Все порты в группе LAG должны иметь одинаковые режимы обратного давления и управления потоком.

- 1 Все порты в группе LAG должны иметь одинаковые приоритеты.
- 1 Все порты в группе LAG должны иметь одинаковые типы трансивера.
- 1 PowerConnect 6024/6024F поддерживает до семи групп LAG.
- 1 Порты могут быть сконфигурированы как LACP только в том случае, если они не являются частью предварительно настроенной группы LAG.

Порты, добавляемые в группу LAG, теряют индивидуальные настройки. Когда порты удаляются из группы LAG, для них применяются первоначальные настройки.

Коммутатор использует функцию хеширования, чтобы определить, какие передаются пакеты и по какой части объединенного канала. Функция хеширования выравнивает статическую загрузку на компоненты объединенного канала. Коммутатор рассматривает объединенный канал как один логический порт.

Чтобы открыть страницу **Link Aggregation (Объединение каналов)**, выберите **Switch (Коммутатор) → Link Aggregation (Объединение каналов)** на панели дерева.

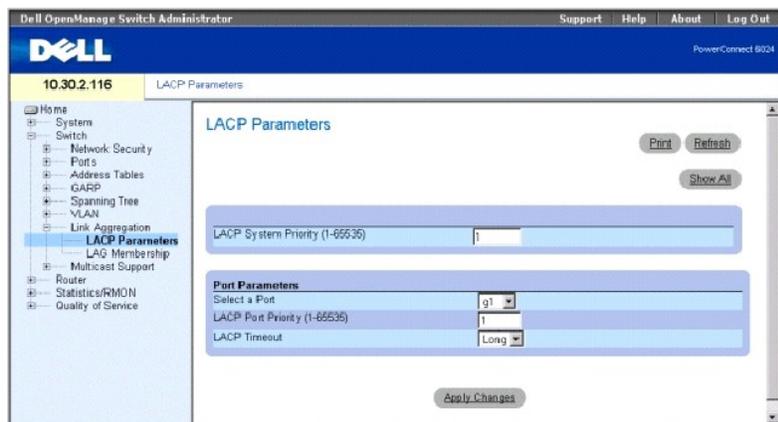
Определение параметров протокола LACP

Объединенные порты можно связать в группы портов объединенного канала. Каждая группа состоит из портов с одинаковой скоростью, работающих в дуплексном режиме.

Порты в группе LAG могут содержать разные типы носителей, если порты работают с одной скоростью. Объединенные каналы можно настроить вручную или автоматически, включив протокол LACP (Link Aggregation Control Protocol) на соответствующих каналах.

Используйте страницу **LACP Parameters (Настройка LACP)** для настройки групп LAG протокола LACP. Чтобы открыть страницу **LACP Parameters (Параметры LACP)**, выберите **Switch (Коммутатор) → Link Aggregation (Объединение каналов) → LACP Parameters (Параметры LACP)** на панели дерева.

Рис. 7-34. Страница LACP Parameters (Параметры LACP)



Страница **LACP Parameters (Параметры LACP)** содержит разделы для определения глобальных параметров и параметров порта.

LACP System Priority (1-65535) (Приоритет системы LACP) - значение приоритета LACP для общих параметров. Значение по умолчанию: 1.

Select a Port (Выбор порта) - номер порта, для которого назначены значения времени ожидания и приоритета.

LACP Port Priority (1-65535) (Приоритет порта LACP) - значение приоритета LACP для порта.

LACP Timeout (Тайм-аут LACP) - административный тайм-аут LACP. Возможные значения:

Short (Короткая) - определяет малое время ожидания.

Long (Длинная) - определяет большое время ожидания.

Определение общих параметров объединенных каналов

1. Откройте страницу **LACP Parameters** (Параметры LACP).
2. Укажите значение полей **LACP System Priority** (Приоритет системы LACP) и **LACP Timeout** (Тайм-аут LACP).
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Параметры будут определены, а устройство обновлено.

Определение параметров портов объединенного канала

1. Откройте страницу **LACP Parameters** (Параметры LACP).
2. Перейдите к таблице **Port Parameters** (Параметры портов).
3. Выберите порт, для которого необходимо определить параметры.
4. Укажите значение полей **LACP System Priority** (Приоритет LACP-системы) и **LACP Timeout** (Пауза LACP).
5. Нажмите кнопку **Apply Changes** (Применить изменения).

Параметры будут определены, а устройство обновлено.

Отображение таблицы параметров LACP

1. Откройте страницу **LACP Parameters** (Параметры LACP).
2. Нажмите кнопку **Show All** (Показать все), чтобы отобразить страницу **LACP Parameters Table** (Таблица параметров LACP).

Настройка параметров LACP с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для настройки параметров LACP, как показано на странице **Link Aggregation** (Объединение канала).

Таблица 7-29. Команды консоли для настройки параметров LACP

Команда консоли	Описание
<code>lACP system-priority значение</code>	Настраивает приоритет системы.
<code>lACP port-priority значение</code>	Настраивает приоритет физических портов.
<code>lACP timeout {long short}</code>	Задаёт административный тайм-аут LACP.
<code>show lACP ethernet интерфейс [parameters statistics protocol- state]</code>	Отображает информацию о протоколе LACP для портов Ethernet.

Далее приведен пример команд консоли.

```
Console (config)# lacp system-priority 120
```

```
Console (config)# interface ethernet g8
```

```
Console (config-if)# lacp port-priority 247
```

```
Console (config-if)# lacp timeout long
```

```
Console(config-if)# exit
```

```
Console# show lacp ethernet g1 statistics
```

```
Port 1 LACP Statistics:
```

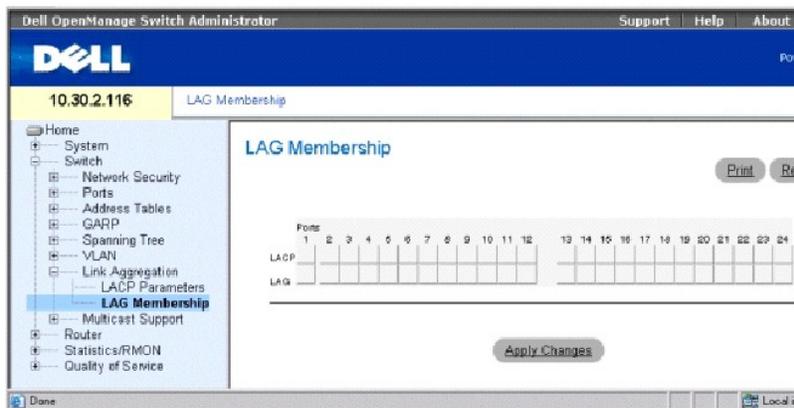
```
LACP PDUs sent:2
```

```
LACP PDUs received:2
```

Определение принадлежности к группе LAG

Коммутатор поддерживает семь групп LAG и семь портов на каждую группу LAG. Используйте страницу **LAG Membership** (Членство в LAG) для назначения портов для группы LAG. Чтобы открыть страницу **LAG Membership** (Членство в LAG), выберите **Switch** (Коммутатор) → **Link Aggregation** (Объединение каналов) → **LAG Membership** (Членство в LAG) на панели дерева.

Рис. 7-35. Страница LAG Membership Page (Принадлежность LAG)



LACP - добавляет порт в группу LAG, используя протокол LACP.

LAG - добавляет порт в группу LAG и указывает LAG, к которой принадлежит порт.

Добавление порта в группу LAG

1. Откройте страницу **LAG Membership** (Принадлежность в LAG).
2. Переключите кнопку под номером порта, чтобы присвоить статическую настройку и номер LAG.
3. Переключите кнопку в строке LACP, выбрав значение L, чтобы добавить порт в группу LAG с помощью LACP
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Порт будет добавлен в группу LAG, а устройство обновлено.

Включение портов в группы LAG с помощью команд консоли

В следующей таблице приведены команды консоли, соответствующие полям для включения портов в группы LAG на странице **LAG Membership** (Членство в LAG).

Таблица 7-30. Команды консоли для определения принадлежности LAG

Команда консоли	Описание
<code>interface port-channel номер_канала_порта</code>	Включает режим настройки интерфейса для указанного канала-порта.
<code>channel-group номер_канала_порта mode {on auto}</code>	Связывает порт с каналом порта. Для удаления конфигурации группы канала из интерфейса используйте форму по этой команды
<code>show interfaces port- channel [номер_канала_ порта]</code>	Отображает информацию о канале порта.

```
Console(config)# interface port-channel 1
```

```
Console (config-if)# channel-group 1 mode on
```

```
Console# show interfaces port-channel
```

```
Channel Port
```

```
-----
```

```
Ch 1 Active g1, g2 Inactive g3
```

```
Ch 2 Active g2
```

```
Ch 3 Inactive g8
```

Поддержка пересылки многоадресного трафика

Пересылка многоадресного трафика позволяет пересылать один пакет по нескольким адресам. Служба многоадресной пересылки уровня L2 основана

на коммутаторе L2, который получает один пакет, адресованный определенным адресам. Она создает копии пакета и передает их на соответствующие порты.

Это устройство поддерживает следующие функции.

- 1 **Forwarding L2 Multicast Packets** (Пересылка многоадресных пакетов L2) - включает пересылку многоадресных пакетов Layer 2. Фильтрация многоадресной рассылки Layer 2 включена по умолчанию и не настраивается пользователем.

 **ПРИМЕЧАНИЕ.** Система поддерживает фильтр многоадресной рассылки для 256 групп многоадресной рассылки.

- 1 **Filtering L2 Multicast Packets** (Фильтрация многоадресных пакетов L2) - включает пересылку пакетов Layer 2 на интерфейсы. Если фильтрация многоадресного трафика отключена, многоадресные пакеты «лавиной» рассылаются на все соответствующие порты.

Чтобы открыть страницу **Multicast Support** (Поддержка многоадресного трафика), выберите **Switch** (Коммутатор) → **Multicast Support** (Поддержка многоадресного трафика) на панели дерева.

Определение общих параметров многоадресной передачи

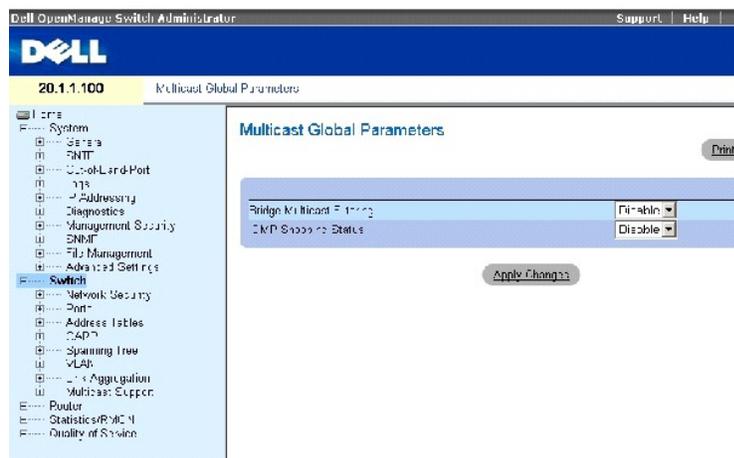
Переключение Layer 2 пересылает многоадресные пакеты на все соответствующие порты VLAN по умолчанию, при этом пакет рассматривается как многоадресная передача. Пересылка многоадресного трафика является эффективной, но не оптимальной, поскольку и несоответствующие порты получают пакеты многоадресной рассылки. Избыточные пакеты вызывают увеличение сетевого трафика. Фильтр многоадресной пересылки позволяет выполнять пересылку пакетов Layer 2 на набор портов.

Когда наблюдение на базе IGMP включено глобально для всей системы, все пакеты IGMP отправляются на процессор. Процессор анализирует входящие пакеты и определяет, какие порты и в какие многоадресные группы собираются вступить, какие порты обладают многоадресными маршрутизаторами, генерирующими запросы IGMP, и какие протоколы маршрутизации передают пакеты и многоадресный трафик.

Порты, запрашивающие добавление в определенную группу многоадресной передачи, выдают отчет IGMP, в котором указано, что группа многоадресной передачи принимает записи. В результате этого создается база данных фильтров многоадресной рассылки.

Чтобы включить наблюдение на базе протокола IGMP на устройстве, используйте страницу **Multicast Global Parameters** (Общие параметры передачи многоадресного трафика). Чтобы открыть страницу **Multicast Global Parameters** (Общие параметры передачи многоадресного трафика), выберите **Switch** (Коммутатор) → **Multicast Support** (Поддержка многоадресного трафика) → **Global Parameters** (Общие параметры) на панели дерева.

Рис. 7-36. Страница Multicast Global Parameters (Общие параметры передачи многоадресного трафика)



Страница [Multicast Global Parameters](#) (Общие параметры передачи многоадресного трафика) содержит следующие поля.

Bridge Multicast Filtering (Фильтрация многоадресного трафика через мост) - включает или отключает фильтрацию многоадресного трафика через мост. Значение по умолчанию: отключено.

IGMP Snooping Status (Состояние наблюдения по протоколу IGMP) - включает или отключает наблюдение по протоколу IGMP на устройстве. Значение по умолчанию: отключено.

Включение на устройстве фильтрации многоадресного трафика через мост

1. Откройте страницу **Multicast Global Parameters** (Общие параметры передачи многоадресного трафика).
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 Bridge Multicast (Мостовая многоадресная передача).

Включение на устройстве наблюдения на базе IGMP

1. Откройте страницу **Multicast Global Parameters** (Общие параметры передачи многоадресного трафика).
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 передачи многоадресного трафика и наблюдения на базе IGMP с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для включения многоадресной пересылки и наблюдения на базе IGMP, как показано на странице **Multicast Support** (Поддержка многоадресной пересылки).

Таблица 7-31. Команды консоли для включения передачи многоадресного трафика и наблюдения на базе IGMP

Команда консоли	Описание
<code>bridge multicast filtering</code>	Включает фильтрацию многоадресных адресов.
<code>ip igmp snooping</code>	Включает наблюдение по протоколу IGMP.

Далее приведен пример команд консоли.

```
Console (config)# bridge multicast filtering
```

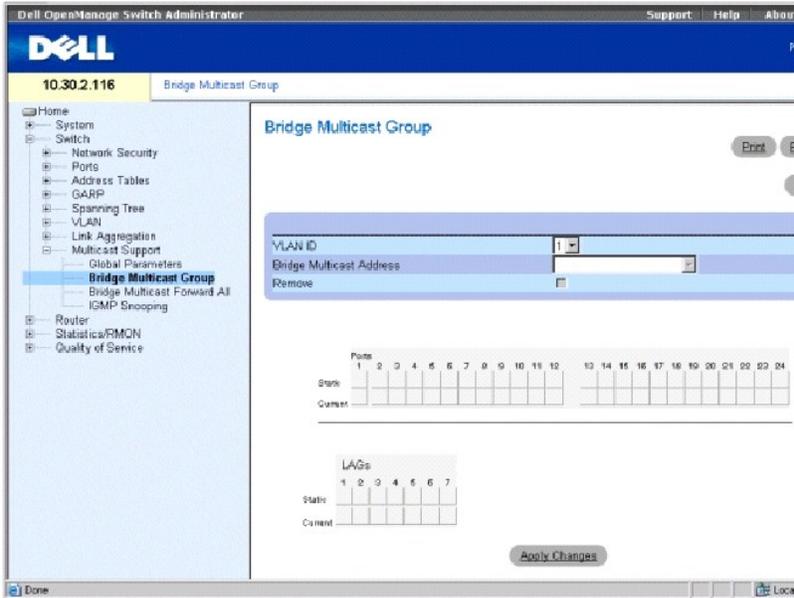
```
Console (config)# ip igmp snooping
```

Добавление записей адресов многоадресной передачи моста

На странице **Bridge Multicast Group** (Группа многоадресной передачи моста) показаны порты и группы LAG, связанные с группой службы многоадресной передачи, в таблицах **Ports** (Порты) и **LAG**. Таблицы **Port** и **LAG** также отражают принцип добавления порта или LAG в группу многоадресной передачи. Порты можно добавлять в существующую группу или в новые группы службы многоадресной передачи. Страница **Bridge Multicast Group** (Группа многоадресной передачи моста) позволяет создавать новые группы службы многоадресной передачи. На странице **Bridge Multicast Group** (Группа многоадресной передачи моста) также можно присвоить порты определенной группе многоадресной передачи.

Чтобы открыть страницу Bridge Multicast Group (Группа многоадресной передачи моста), выберите Switch (Коммутатор)→ Multicast Support (Поддержка многоадресного трафика)→ Bridge Multicast Address (Адрес многоадресной передачи моста) на панели дерева.

Рис. 7-37. Страница Bridge Multicast Group (Группа многоадресной передачи моста)



VLAN ID (Идентификатор VLAN) - определяет VLAN и содержит информацию об адресе группы многоадресной передачи.

Bridge Multicast Address (Адрес многоадресной передачи моста) - идентифицирует MAC/IP-адрес группы многоадресной передачи.

Remove (Удалить) - когда установлен этот флажок, адрес многоадресной передачи моста удаляется.

Ports (Порты) - порты, которые можно добавить в службу многоадресной передачи.

LAGs (Группы LAG) - группы LAG, которые можно добавить в службу многоадресной передачи.

В следующей таблице приведены параметры управления записями портов и групп LAG для IGMP.

Таблица 7-32. Параметры управления таблицей записей портов/LAG для IGMP

Управление портом	Описание
D	Показывает, что порт/группа LAG добавлена в группу многоадресной передачи динамически в текущей строке.
S	Связывает порт с многоадресной группой в качестве статического члена в строке <i>Static</i> (Статический). Показывает, что порт/группа LAG присоединена к многоадресной группе статически в строке <i>Current</i> (Текущий).
F	Показывает, что запись порта/группы LAG в группу многоадресной передачи запрещена.
Blank	Показывает, что порт не связан с группой многоадресной передачи.

Добавление адресов многоадресной передачи моста

1. Откройте страницу **Bridge Multicast Group** (Группа многоадресной передачи моста).
2. Нажмите кнопку **Add**, чтобы отобразить страницу **Add Bridge Multicast Group** (Добавление группы многоадресной передачи моста).

Рис. 7-38. Страница Add Bridge Multicast Group (Добавление группы многоадресной передачи моста)

Add Bridge Multicast Group Back

VLAN ID: ▼

New Bridge Multicast Address: (XX:XX:XX)

New Bridge MAC Multicast: (XX:XX:XX:XX:XX:XX)

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

Status: S F

Port: S D D D D D D D D D D D D D D D D D D D

LAGs: 1 2 3 4 5 6 7 8

Status: S F

Port: S D D

Apply Changes

3. Определите поля **VLAN ID** (Идентификатор VLAN) и **New Bridge Multicast Address** (Новый адрес многоадресной передачи моста).
4. Переключите порт на значение **S**, чтобы добавить его в выбранную группу многоадресной передачи.
5. Переключите порт на значение **F**, чтобы запретить добавление определенных адресов многоадресной передачи для определенного порта.
6. Нажмите кнопку **Apply Changes** (Применить изменения).

Адрес многоадресной передачи моста будет добавлен в многоадресную группу, а устройство обновлено.

Определение портов для получения службы многоадресной пересылки

1. Откройте страницу **Bridge Multicast Group** (Группа многоадресной передачи моста).
2. Определите поля **VLAN ID** (Идентификатор VLAN) и **Bridge Multicast Address** (Адрес многоадресной передачи моста).
3. Переключите порт на значение **S**, чтобы добавить его в выбранную группу многоадресной передачи.
4. Переключите порт на значение **F**, чтобы запретить добавление определенных адресов многоадресной передачи для определенного порта.
5. Нажмите кнопку **Apply Changes** (Применить изменения).

Порт будет назначен в группу многоадресной передачи, а устройство обновлено.

Назначение групп LAG для получения службы многоадресной пересылки

1. Откройте страницу **Bridge Multicast Group** (Группа многоадресной передачи моста).
2. Определите поля **VLAN ID** (Идентификатор VLAN) и **Bridge Multicast Address** (Адрес многоадресной передачи моста).
3. Переключите LAG на значение **S**, чтобы добавить его в выбранную группу многоадресной передачи.
4. Переключите LAG на значение **F**, чтобы запретить добавление определенных адресов многоадресной передачи для определенной группы LAG.
5. Нажмите кнопку **Apply Changes** (Применить изменения).

Группа LAG будет назначена в группу многоадресной передачи, а устройство обновлено.

Управление записями службы многоадресной пересылки с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для управления записями службы многоадресной пересылки, как показано на странице **Bridge Multicast Group** (Группа многоадресной передачи моста).

Таблица 7-33. Команды консоли для управления записями службы многоадресной пересылки

Команда консоли	Описание
<pre>bridge multicast address {mac_адрес_многоадресной_передачи ip_адрес_многоадресной_передачи} [add remove] {ethernet список_интерфейсов port-channel список_номеров_каналов_портов}</pre>	<p>Регистрирует адреса для многоадресной передачи на уровне MAC-адресов для таблицы мостов и добавляет в группу статические порты.</p>
<pre>bridge multicast forbidden address {mac_адрес_многоадресной_передачи ip_ адрес_многоадресной_передачи } [add remove] {ethernet список_интерфейсов port-channel список_номеров_каналов_портов}</pre>	<p>Запрещает добавление определенного адреса многоадресной передачи для определенных портов. Для возврата к значениям по умолчанию используйте форму по этой команды</p>
<pre>show bridge multicast address-table [vlan vlan- id] [address mac_ адрес_многоадресной_передачи ip_адрес_многоадресной_передачи] [format ip mac]</pre>	<p>Отображает информацию таблицы MAC-адресов для многоадресной передачи.</p>

Далее приведен пример команд консоли.

```
console#config

console(config)#vlan database

console(config-if)#vlan 8

console(config-if)#exit

console(config)#interface range ethernet g1-9

console(config-if)# switchport mode general

console(config-if)# switchport general allow vlan add 8

console(config)#interface vlan 8

Console(config-if)# bridge multicast address 0100.5e02.0203

add ethernet g1-9

Console(config-if)# exit

Console(config)# exit

Console # show bridge multicast address-table

Vlan MAC Address type Ports
```

```
1 0100.5e02.0203 static g1, g2
```

```
19 0100.5e02.0208 static g1-8
```

```
19 0100.5e02.0208 dynamic g 9-11
```

Forbidden ports for multicast addresses:

Vlan MAC Address Ports

```
1 0100.5e02.0203 g8
```

```
19 0100.5e02.0208 g8
```

```
Console# configuration
```

```
Console (config) # interface vlan 8
```

```
Console(config-if)# bridge multicast address 0100.5e02.0203
```

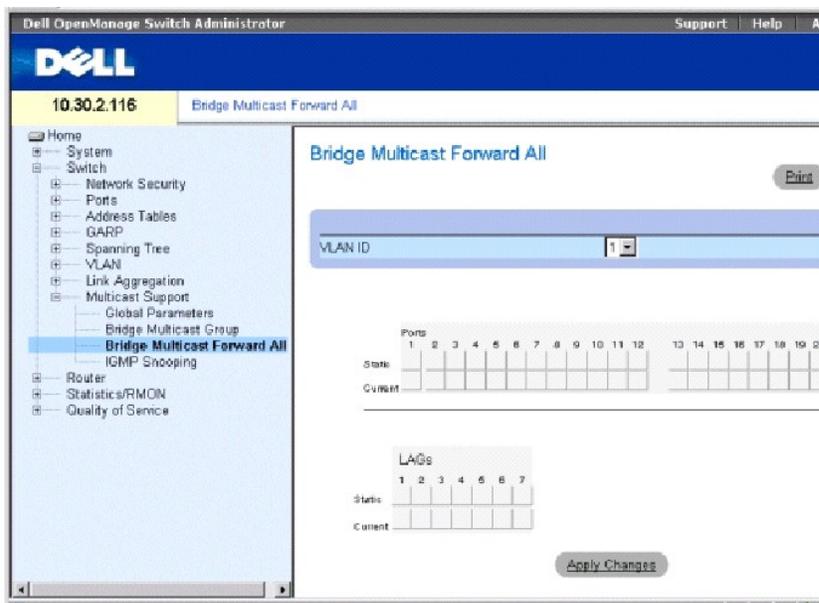
```
Console (config-if)# bridge multicast forbidden address 0100.5e02.0203 add ethernet g9
```

Назначение параметров многоадресной пересылки всем

Страница **Bridge Multicast Forward All** (Многоадресная передача моста всем) позволяет включить привязку портов или групп 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 группе VLAN.

Чтобы открыть страницу **Bridge Multicast Forward All** (Многоадресная передача моста всем), выберите **Switch** (Коммутатор) → **Multicast Support** (Поддержка многоадресного трафика) → **Bridge Multicast** (Многоадресная передача моста) → **Bridge Multicast Forward All** (Многоадресная передача моста всем) на панели дерева.

Рис. 7-39. Страница Bridge Multicast Forward All (Многоадресная передача моста всем)



VLAN ID (Идентификатор VLAN) - определяет VLAN пакета и содержит информацию об адресе группы многоадресной передачи.

Ports (Порты) - порты, которые можно добавить в службу многоадресной передачи.

LAGs (Группы LAG) - группы LAG, которые можно добавить в службу многоадресной передачи.

В следующей таблице приведены параметры управления настройками маршрутизатора и портов.

Таблица 7-34. Параметры управления маршрутизатором/портами для многоадресной передачи моста всем

Управление портом	Описание
D	Связывает порт с многоадресным маршрутизатором или коммутатором как динамический порт.
S	Связывает порт с многоадресным маршрутизатором или коммутатором как статический порт.
F	Запрещено
Blank	Указывает, что порт не подключен к маршрутизатору многоадресной передачи или коммутатору.

Привязка порта к маршрутизатору или коммутатору многоадресной передачи

1. Откройте страницу **Bridge Multicast Forward All** (Многоадресная передача моста всем).
2. Определите поле **VLAN ID** (Идентификатор VLAN).
3. Выберите порт в таблице **Ports** (Порты) и назначьте значение для порта.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Порт не подключен к маршрутизатору или коммутатору многоадресной передачи.

Привязка группы LAG к маршрутизатору или коммутатору многоадресной передачи

1. Откройте страницу **Bridge Multicast Forward All** (Многоадресная передача моста всем).
2. Определите поле **VLAN ID** (Идентификатор VLAN).
3. Выберите порт в таблице **LAGs** (Группы LAG) и укажите значение LAG.

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

Группа LAG привязывается к маршрутизатору или коммутатору многоадресной передачи.

Управление группами LAG и портами, связанными с маршрутизаторами многоадресной передачи с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для управления группами LAG и портами, привязанными к маршрутизаторам многоадресной передачи, как показано на странице **Bridge Multicast Forward All** (Многоадресная передача моста всем).

Таблица 7-35. Команды консоли для управления группами LAG и портами, привязанными к маршрутизаторам многоадресной передачи

Команда консоли	Описание
<code>show bridge multicast filtering <i>идентификатор_vlan</i></code>	Отображает настройку фильтра многоадресной передачи.
<code>bridge multicast forward-all {add remove} {ethernet <i>список_интерфейсов</i> port- channel <i>список_номеров_каналов_портов</i>}</code>	Разрешает пересылку всех многоадресных пакетов для порта. Для возврата к значениям по умолчанию используйте форму по этой команды.

Далее приведен пример команд консоли.

```
Console # show bridge multicast filtering 1
```

```
Filtering: Disabled
```

```
VLAN: 1
```

```
Forward-All
```

```
Port Static Status
```

```
-----
```

```
g1 - Filter
```

```
g2 - Filter
```

```
...
```

```
console# config
```

```
console(config)#vlan database
```

```
console(config-if)#vlan 8

console(config-vlan)#exit

console(config)#interface range ethernet g1-9

console(config-if)# switchport mode general

console(config-if)# switchport general allow vlan add 8

console(config)#interface vlan 8

Console(config-if)# bridge multicast address 0100.5e02.0203

add ethernet g1-9

Console(config-if)# exit

Console(config)# exit

Console# configuration

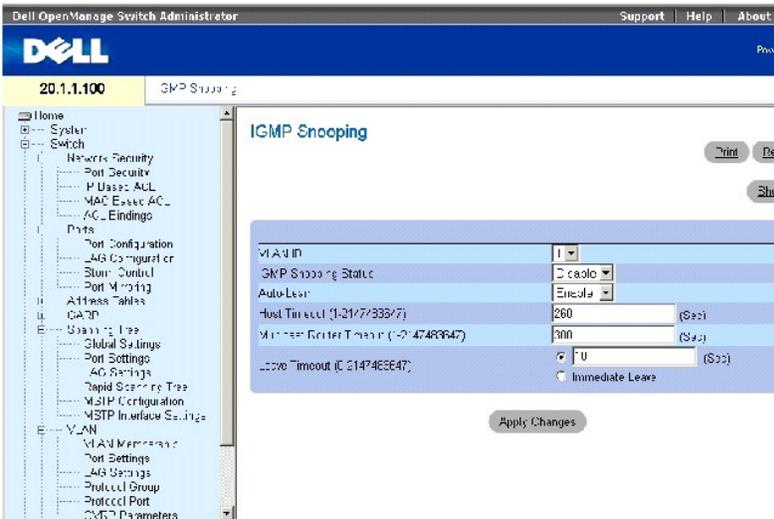
Console (config)# interface VLAN 1

Console (config-if)# bridge multicast forward-all add ethernet g8
```

Наблюдение по протоколу IGMP

Чтобы добавить записи IGMP, используйте страницу **IGMP Snooping** (Наблюдение по протоколу IGMP). Чтобы открыть страницу **IGMP Snooping** (Наблюдение по протоколу IGMP), выберите **Switch** (Коммутатор) → **Multicast Support** (Поддержка многоадресного трафика) → **IGMP Snooping** (Наблюдение по протоколу IGMP) на панели дерева.

Рис. 7-40. Страница IGMP Snooping (Наблюдение по протоколу IGMP)



VLAN ID (Идентификатор сети VLAN) - указывает идентификатор VLAN.

IGMP Snooping Status (Состояние наблюдения по протоколу IGMP) - включает или отключает наблюдение по протоколу IGMP для VLAN.

Auto Learn (Автоматическое распознавание) - включает или отключает автоматическое распознавание на устройстве.

Host Timeout (1-2147483647) (Время ожидания хоста) - время, по истечении которого запись наблюдения по протоколу IGMP устаревает. Значение по умолчанию: 260 секунд.

Multicast Router Timeout (1-2147483647) (Время ожидания многоадресного маршрутизатора) - время, по истечении которого запись многоадресного маршрутизатора устаревает. Значение по умолчанию: 300 секунд.

Leave Timeout (0-2147483647) (Время старения) - время в секундах после получения сообщения портом и до истечения срока хранения. **User-defined** (Определено пользователем) позволяет определить интервал времени ожидания, а **Immediate Leave** (Немедленно) определяет время ожидания немедленного выхода. Значение по умолчанию: 10 секунд.

Включение на устройстве наблюдения на базе IGMP

1. Откройте страницу **IGMP Snooping** (Наблюдение по протоколу IGMP).
2. Выберите идентификатор VLAN для устройства, на котором будет включено наблюдение на базе протокола IGMP.
3. Выберите **Enable** (Включено) в поле **IGMP Snooping Status** (Состояние наблюдения на базе IGMP).
4. Заполните поля на этой странице.
5. Нажмите кнопку **Apply Changes** (Применить изменения).

Наблюдение на базе IGMP будет включено на этом устройстве.

Отображение таблицы наблюдения по протоколу IGMP

1. Откройте страницу **IGMP Snooping** (Наблюдение по протоколу IGMP).
2. Нажмите кнопку **Show All** (Показать все), чтобы отобразить таблицу **IGMP Snooping Table** (Таблица наблюдения по протоколу IGMP).

Настройка наблюдения по протоколу IGMP с помощью команд консоли

В следующей таблице приведены команды консоли для настройки функции безопасности заблокированных портов, соответствующие полям на странице IGMP Snooping (Наблюдение по протоколу IGMP).

Таблица 7-36. Команды консоли для настройки наблюдения по протоколу IGMP

Команда консоли	Описание
<code>ip igmp snooping</code>	Включает наблюдение по протоколу IGMP.
<code>ip igmp snooping mrouter learn-pim-dvmrp</code>	Включает автоматическое распознавание портов многоадресного маршрутизатора в контексте определенной VLAN.
<code>ip igmp snooping host-time-out количество_секунд</code>	Настраивает время ожидания хоста.
<code>ip igmp snooping mrouter-time-out количество_секунд</code>	Настраивает время ожидания маршрутизатора.
<code>ip igmp snooping leave-time-out {количество_секунд immediate-leave}</code>	Настраивает время старения хоста.
<code>show ip igmp snooping interface идентификатор_vlan</code>	Отображает конфигурацию наблюдения по протоколу IGMP.
<code>show ip igmp snooping mrouter [interface идентификатор_vlan]</code>	Отображает информацию о динамически распознаваемых интерфейсах многоадресного маршрутизатора.

Далее приведен пример команд консоли.

```
Console (config)# ip igmp snooping
```

```
Console (config)# interface vlan 1
```

```
Console (config-if)# ip igmp snooping mrouter learn-pim-dvmrp
```

```
Console (config-if)# ip igmp snooping host-time-out 300
```

```
Console (config-if)# ip igmp snooping mrouter-time-out 200
```

```
Console(config-if)# exit
```

```
Console (config)# interface vlan 1
```

```
Console (config-if)# ip igmp snooping leave-time-out 60
```

```
Console(config-if)# exit
```

```
Console(config)# exit
```

```
Console # show ip igmp snooping interface 1000
```

```
IGMP Snooping is globally enabled
```

```
IGMP Snooping is enabled on VLAN 1000
```

```
IGMP host timeout is 300 sec
```

```
IGMP Immediate leave is disabled. IGMP leave timeout is 10 sec
```

```
IGMP mrouter timeout is 200 sec
```

```
Automatic learning of multicast router ports is enabled
```

```
Console> show igmp-snooping mrouter
```

```
VLAN Ports
```

```
-----
```

```
2 g9
```

[Назад на страницу Содержание](#)

[Назад на страницу Содержание](#)

Настройка маршрутизации

Системы Dell™ PowerConnect™ 6024/6024F

- [Обзор маршрутизации](#)
- [Настройка глобальной IP-маршрутизации](#)
- [Настройка протокола RIP](#)
- [Настройка параметров и фильтров OSPF](#)
- [Настройка многоадресной маршрутизации IP](#)

Обзор маршрутизации

Устройства в различных подсетях обмениваются данными друг с другом с использованием маршрутизатора Layer 3 между группами VLAN. Маршрутизация по умолчанию включена на коммутаторе. Однако необходимо настроить хотя бы один IP-интерфейс, чтобы коммутатор смог начать маршрутизацию сетевого трафика. Маршруты настраиваются либо статически, либо с использованием протокола RIP (Routing Information Protocol) или OSPF (Open Shortest Path First).

Более подробную информацию о протоколе RIP см. в разделе [«Настройка протокола RIP»](#).

Более подробную информацию о протоколе OSPF см. в разделе [«Настройка параметров и фильтров OSPF»](#).

Настройка глобальной IP-маршрутизации

Страница **Global Routing Parameters** (Параметры глобальной маршрутизации) содержит ссылки для настройки маршрутизации. Маршрутизация всегда включена, но она включается только в том случае, если система имеет один или несколько IP-адресов. Чтобы открыть страницу **Global Routing Parameters** (Параметры глобальной маршрутизации), выберите **Router**→ (Маршрутизатор), **Global Routing Parameters** (Параметры глобальной маршрутизации) на панели дерева.

Эта страница **Global Routing Parameters** (Параметры глобальной маршрутизации) содержит ссылки, которые позволяют выполнить следующие процедуры.

- 1 [Настройка таблицы IP Forwarding \(Пересылка IP\)](#)
- 1 [Настройка статических IP-маршрутов](#)
- 1 [Настройка VRRP](#)
- 1 [Настройка проверки подлинности для маршрутизации MD5](#)
- 1 [Настройка параметров цепочки ключей MD5](#)

Настройка таблицы IP Forwarding (Пересылка IP)

Используйте страницу **IP Forwarding** (Пересылка IP) для просмотра параметров маршрутизации, по которым выполняется пересылка IP-трафика. На этой странице приведен список IP-маршрутов для выбранных IP-адресов назначения, включая IP-маршруты, которые определяются статически или динамически. IP-маршруты основаны на масках сети, ближайших узлах, метрике и протоколах пересылки. Эти параметры определяют, как выполняется пересылка или отбрасывание конкретных пакетов. Когда на интерфейсе настраивается IP-адрес, он включается в таблицу пересылки IP.

Чтобы открыть страницу **IP Forwarding** (Пересылка IP), выберите **Router** (Маршрутизатор)→ **Global Routing Parameters** (Параметры глобальной маршрутизации)→ **IP Forwarding** (Пересылка IP) на панели дерева.

Рис. 8-1. Страница IP Forwarding (Пересылка IP)



Maximum Equal Cost Multipaths (ECMP) (Максимальное число путей с одинаковой стоимостью) - значение ECMP, которое необходимо определить при пересылке IP-пакетов. Значение ECMP показывает, сколько имеется путей от маршрутизатора до сети. Возможны значения от 1 до 4. Например, значение 1 показывает, что имеется только один путь до сети. Чем больше значение, тем больше требуется ресурсов. Изменения в этом поле вступают в силу только после сброса устройства.

Destination IP Address (IP-адрес назначения) - IP-сеть назначения.

Prefix Length (Длина префикса) - число бит, образующих префикс IP-адреса назначения. Длина находится в диапазоне 1-32 бит.

Next Hop (Gateway) (Ближайший узел (шлюз)) - адрес следующего маршрутизатора в маршруте до сети назначения.

Route Type (Тип маршрута) - показывает, как выполняется маршрутизация. Возможные значения:

Remote (Удаленный) - пакет пересылается.

Reject (Отклонить) - пакет отбрасывается.

Local (Локальный) - пакет отправляется в локальную сеть.

Metric (Метрика) - число узлов до сети назначения.

Protocol (Протокол) - протокол маршрутизации, по которому был добавлен этот маршрут.

Отображение таблицы пересылки IP

Таблица IP Forwarding (Пересылка IP) содержит список всех IP-маршрутов в системе.

1. Откройте страницу **IP Forwarding** (Пересылка IP).
2. Нажмите кнопку **Show All** (Показать все), чтобы отобразить таблицу **IP Forwarding** (Пересылка IP).

Просмотр таблицы пересылки IP с помощью команд консоли

В следующей таблице приведены команды консоли для просмотра таблицы IP Forwarding (Пересылка IP).

Таблица 8-1. Команды консоли для пересылки IP

Команда консоли	Описание
<code>show ip route [address]<ip- адрес></code>	Отображает текущее состояние таблицы маршрутизации.
<code>ip maximum-paths number-paths</code>	Управляет максимальным числом параллельных маршрутов, определенных в таблице маршрутизации.

Далее приведен пример команд консоли.

```
Console (config)# interface ip 10.10.10.2
```

```
Console (config-ip)# ip maximum-paths 2
```

```
Console (config-ip)# exit
```

```
Console(config)# exit
```

```
Console# exit
```

```
Console> show ip route
```

Коды: С - подключен, S - статический, R - RIP, O - OSPF, E - внешний OSPF

```
R 10.0.0.0/8 отклонен
```

```
C 10.0.1.1/32 подключен напрямую, Loopback0
```

```
C 10.0.1.0/24 подключен напрямую, Ethernet g1
```

```
C 10.0.2.0/24 подключен напрямую, Ethernet g2
```

```
R 10.8.2.0/24 [230/50] через 10.0.2.2, 00:17:19, Ethernet g2
```

```
S 10.9.1.0/24 [5/2] через 10.0.1.2, 17:19:18, Ethernet g1
```

```
S 10.9.1.0/24 [5/3] через 10.0.2.2, Backup Not Active
```

```
O 10.8.1.0/24 [30/2000] через 10.0.1.2, 00:39:08, Ethernet g1
```

S 172.1.0.0/16 [5/3] через 10.0.1.1, 18:21:58, Ethernet g1

S 172.1.1.0/24 [5/3] через 10.0.2.1, 17:12:19, Ethernet g1

S 172.1.1.1/32 [5/3] через 10.0.3.1, 19:51:18, Ethernet g1

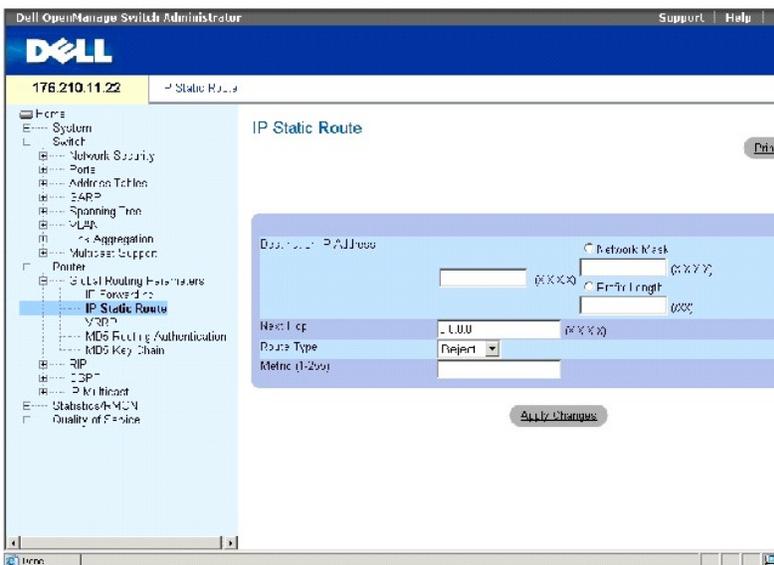
Максимальное число параллельных путей: 2

Настройка статических IP-маршрутов

Для определения статических маршрутов используйте страницу **IP Static Route** (Статичный IP-маршрут).

Чтобы открыть страницу **IP Static Route** (Статичный IP-маршрут), выберите **Router** (Маршрутизатор)→ **Global Routing Parameters** (Параметры глобальной маршрутизации)→ **IP Static Route** (Статичный IP-маршрут) на панели дерева.

Рис. 8-2. Страница IP Static Route (Статичный IP-маршрут)



Destination IP Address (IP-адрес назначения) - IP-сеть назначения статичного маршрута.

Network Mask (Маска сети) - маска сети назначения для этого маршрута.

Prefix Length (Длина префикса) - число бит, образующих префикс IP-адреса назначения. Длина находится в диапазоне 1-32 бит.

Next Hop (Ближайший узел) - показывает адрес следующей системы в маршруте.

Route Type (Тип маршрута) - показывает, как выполняется маршрутизация. Возможные значения:

Remote (Удаленный) - пакет пересылается.

Reject (Отклонить) - пакет отбрасывается.

Local (Локальный) - пакет отправляется в локальную сеть.

Metric (1-255) (Метрика (1-255)) - число узлов до сети назначения.

Добавление статических IP-маршрутов

 **ПРИМЕЧАНИЕ.** В качестве шлюза можно определить только маршрутизатор, подключенный напрямую.

1. Откройте страницу **IP Static Route** (Статичный IP-маршрут).
2. Определите поля на странице.

 **ПРИМЕЧАНИЕ.** Если выбрать для параметра **Route Type** (Тип маршрута) значение **Reject** (Отклонить), то сеть назначения станет недоступной.

Чтобы определить статичный маршрут до узла, находящегося в удаленной сети, выберите значение **Remote** (Удаленный) для параметра **Route Type** (Тип маршрута).

Чтобы определить статичный маршрут до узла, находящегося в локальной сети, выберите значение **Local** (Локальный) для параметра **Route Type** (Тип маршрута).

Destination IP Address (IP-адрес назначения) и **Network Mask** (Маска сети) соответствует адресу удаленной сети. **The Next Hop** (Следующий узел) - это адрес маршрутизатора, который напрямую подключен к коммутатору.

Destination IP Address (IP-адрес назначения) - адрес узла. В поле **Next Hop** (Следующий узел) необходимо указать значение 0.0.0.0.

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

Новый статичный маршрут будет добавлен, а устройство обновлено.

Удаление статичного IP-маршрута

1. Откройте страницу **IP Static Route** (Статичный IP-маршрут).
2. Нажмите кнопку **Show All** (Показать все), чтобы отобразить таблицу **IP Static Route Table** (Таблица статичных IP-маршрутов).
3. Установите флажок **Remove for the Destination IP address** (Удалить для IP-адреса назначения) для статичного маршрута, который необходимо удалить.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Статический маршрут будет удален, а устройство обновлено.

Настройка таблицы статических IP-маршрутов с помощью команд консоли

В следующей таблице приведены команды консоли для настройки таблицы статических IP-маршрутов.

Таблица 8-2. Команды консоли для таблицы статических IP-маршрутов

Команда консоли	Описание

```
ip route префикс {маска | длина-префикса} шлюз [metric расстояние] [reject- route] | Устанавливает статические IP-маршруты.
```

Далее приведен пример команд консоли.

```
Console (config)# ip route 172.16.0.0 255.255.0.0 131.16.1.1
```

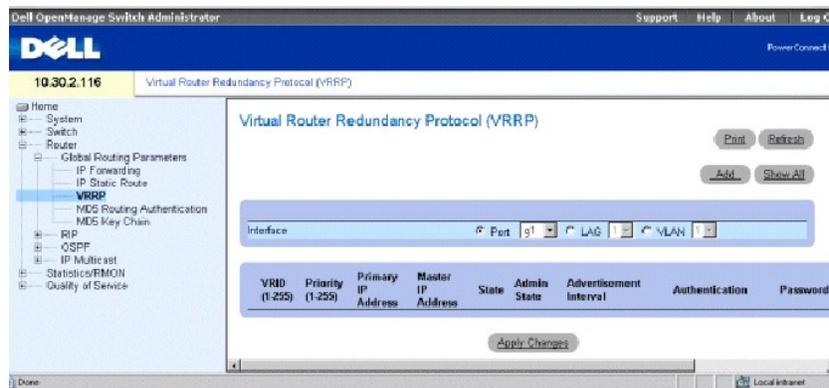
Настройка VRRP

Протокол VRRP (Virtual Router Redundancy Protocol) (VRRP) определяет протокол, который динамически назначает обязанности виртуальной маршрутизации одному из маршрутизаторов VRRP в локальной сети (главному маршрутизатору). Процесс выбора обеспечивает динамическое восстановление в случае отказа и передачу обязанностей маршрутизации, если главный маршрутизатор станет недоступен.

Преимущество VRRP заключается в том, что он исключает явление отказа одной точки, характерное для среды маршрутизации, предоставляя более доступный путь по умолчанию, и в то же время исключает необходимость настройки динамической маршрутизации или протоколов обнаружения маршрутизатора на каждом оконечном узле.

Страница **Virtual Router Redundancy Protocol (VRRP)** (Протокол VRRP) позволяет настроить параметры маршрутизации VRRP для коммутатора. Чтобы открыть страницу **Virtual Router Redundancy Protocol (VRRP)** (Протокол VRRP), выберите **Router** (Маршрутизатор) → **Global Routing Parameters** (Параметры глобальной маршрутизации) → **VRRP** на панели дерева.

Рис. 8-3. Страница Virtual Router Redundancy Protocol (VRRP) (Протокол VRRP)



Interface (Интерфейс) - тип и число интерфейсов, подключенных к маршрутизатору VRRP.

VRID (1-255) - идентификатор виртуального маршрутизатора.

Priority (Приоритет) (1-255) - приоритет маршрутизатора, используемый в процессе выбора виртуального маршрутизатора. Значение может определять, заменяет ли маршрутизатор VRRP с высоким приоритетом маршрутизатор VRRP с низким приоритетом.

Primary IP Address (Основной IP-адрес) - виртуальный IP-адрес, определенный с виртуальным маршрутизатором. Основной IP-адрес выбирается из числа реальных адресов интерфейса, настроенных на маршрутизаторе VRRP.

Master IP Address (Основной IP-адрес) - маршрутизатор VRRP, который является управляющим для этого виртуального маршрутизатора.

State (Состояние) - текущее состояние маршрутизатора. Возможные значения:

Master (Основной) - маршрутизатор работает как маршрутизатор пересылки для IP-адресов, связанных с виртуальным маршрутизатором. Основной маршрутизатор отвечает на запросы ARP со связанными IP-адресами в цели ARP, пересылает пакеты с виртуальным MAC-адресом (VMAC) в качестве MAC-адреса назначения и принимает пакеты, связанные с виртуальными IP-адресами (только в том случае, если маршрутизатор обладает собственными связанными IP-адресами).

Initialize (Инициализировать) - маршрутизатор ожидает события запуска. При получении события запуска маршрутизатор переходит в соответствующее состояние.

Backup (Резервирование) - маршрутизатор является резервным для основного маршрутизатора. Маршрутизатор постоянно контролирует, имеется ли основной маршрутизатор, с помощью периодической рассылки объявлений или рассылки специальных объявлений с основного маршрутизатора, информирующих о том, что он выключается.

Admin State (Состояние администрирования) - показывает, работает ли маршрутизатор.

Advertisement Interval (Интервал между объявлениями) - показывает частоту, с которой передаются отправления, когда маршрутизатор является основным.

Authentication (Проверка подлинности) - показывает, если не выполняется проверки подлинности, а также используются ли пароли для проверки подлинности обмена данными по протоколу VRRP.

Password (Пароль) - пароль используется для проверки подлинности обмена данными по протоколу VRRP.

Preempt (Вне очереди) - когда установлен этот флажок, маршрутизаторы VRRP с высоким приоритетом заменяют маршрутизаторы с низким приоритетом.

Remove (Удалить) - когда этот флажок установлен, запись VRRP удаляется из таблицы VRRP.

Добавление маршрутизаторов в группу VRRP

1. Откройте страницу **Virtual Router Redundancy Protocol (VRRP)** (Протокол VRRP).
2. Щелкните **Add (Добавить)**, чтобы отобразить страницу **Add VRRP Interface (Добавление интерфейса VRRP)**.

Рис. 8-4. Добавление интерфейса VRRP

Add VRRP Interface

Interface	g1	LAG	VLAN
Priority (1-255)	160		
Virtual Router Identifier (1-255)	1		
Virtual IP Address 1		(x.x.x.x)	
Virtual IP Address 2 (Optional)		(x.x.x.x)	
Virtual IP Address 3 (Optional)		(x.x.x.x)	
Virtual IP Address 4 (Optional)		(x.x.x.x)	
Virtual IP Address 5 (Optional)		(x.x.x.x)	
Virtual IP Address 6 (Optional)		(x.x.x.x)	
Virtual IP Address 7 (Optional)		(x.x.x.x)	
Virtual IP Address 8 (Optional)		(x.x.x.x)	
Primary IP Address	0.0.0.0		
Advertisement Interval	1	(Sec)	
Authentication	None		
Password (1-8 characters)			
Preempt	<input checked="" type="checkbox"/>		

3. Определите поля.

Для получения сведений о полях см. раздел [«Настройка VRRP»](#).

 **ПРИМЕЧАНИЕ.** Чтобы можно было *включить* состояние администрирования, необходимо предварительно определить интерфейсы VRRP.

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

Новый интерфейс VRRP будет добавлен, а устройство обновлено.

 **ПРИМЕЧАНИЕ.** В случае ввода недопустимого виртуального IP-адреса появится предупреждение, но виртуальный маршрутизатор будет добавлен. Рекомендуется удалить эту запись из таблицы виртуальных маршрутизаторов.

Изменение маршрутизаторов VRRP

1. Откройте страницу **Virtual Router Redundancy Protocol (VRRP)** (Протокол VRRP).
2. Выберите интерфейс в поле **Interface** (Интерфейс).
3. Определите поля, как необходимо.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Удаление записи VRRP

1. Откройте страницу **Virtual Router Redundancy Protocol (VRRP)** (Протокол VRRP).
2. Нажмите кнопку **Show All** (Показать все), чтобы отобразить таблицу **VRRP Table**.
3. Выберите запись таблицы.
4. Установите флажок **Remove** (Удалить).
5. Нажмите кнопку **Apply Changes** (Применить изменения).

Запись VRRP будет удалена, а устройство обновлено.

Настройка VRRP с помощью команд консоли

В следующей таблице приведены команды консоли для настройки VRRP.

Таблица 8-3. Команды консоли для VRRP

Команда консоли	Описание
<code>vrrp виртуальный-маршрутизатор ip ip-адрес [ip-адрес2...ip-адрес8]</code>	Определяет протокол VRRP (Virtual Router Redundancy Protocol) для интерфейса.
<code>vrrp виртуальный_маршрутизатор up</code>	Активирует протокол VRRP (Virtual Router Redundancy Protocol) для интерфейса.
<code>vrrp виртуальный_маршрутизатор timer секунды</code>	Настраивает временной интервал между отправкой сообщений с объявлениями.
<code>vrrp виртуальный_маршрутизатор priority приоритет</code>	Настраивает приоритет протокола VRRP (Virtual Router Redundancy Protocol) для интерфейса.
<code>vrrp виртуальный_маршрутизатор source-ip ip-адрес</code>	Определяет исходный IP-адрес (основной IP-адрес), используемый для сообщений протокола VRRP (Virtual Router Redundancy Protocol) для интерфейса.
<code>vrrp виртуальный_маршрутизатор authentication текст</code>	Включает проверку подлинности для протокола VRRP (Virtual Router Redundancy Protocol) для интерфейса.
	Включает внеочередность протокола VRRP (Virtual Router Redundancy Protocol) для интерфейса.

<code>vrrp виртуальный_маршрутизатор preempt</code>	
<code>show vrrp configuration [ethernet номер_интерфейса vlan идентификатор_vlan номер порта-канала]</code>	Отображает конфигурацию протокола VRRP (Virtual Router Redundancy Protocol).
<code>show vrrp status [ethernet номер_интерфейса vlan идентификатор_vlan номер порта-канала]</code>	Отображает состояние протокола VRRP (Virtual Router Redundancy Protocol).

Настройка VRRP с помощью команд консоли

Далее приведен пример команд консоли.

```
Console (config)# interface ethernet g8
```

```
Console(config-if)# vrrp 45 ip 172.16.1.1 172.16.2.1
```

```
Console(config-if)# vrrp 45 up
```

```
Console(config-if)# vrrp 45 timer 100
```

```
Console(config-if)# vrrp 45 priority 150
```

```
Console(config-if)# vrrp 45 source-ip 168.192.1.1
```

```
Console(config-if)# vrrp 45 authentication Dell
```

```
Console(config-if)# vrrp 45 preempt
```

```
Console(config-if)# exit
```

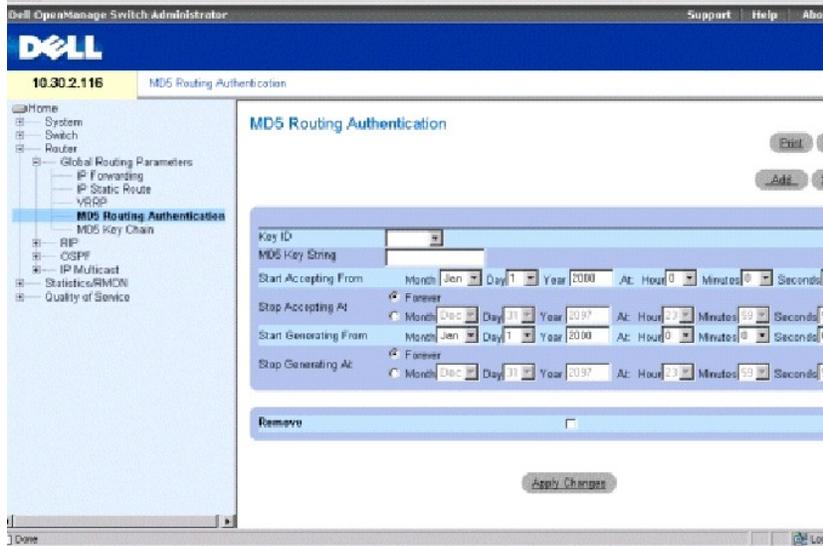
```
Console(config)# exit
```

Настройка проверки подлинности для маршрутизации MD5

Ключи MD5 используются в алгоритме проверки подлинности Message Digest-5. Для каждого ключа можно определить время начала и окончания для отправки и приема. Можно настроить ключи, которые являются активными, срок действия которых истекает во время сброса. Связанные между собой интерфейсы должны иметь одинаковый идентификатор ключа. Если временной диапазон ключей накладывается со стороны передачи, то устройство использует ключ с более поздним временем начала. При получении пакетов интерфейс использует ключ, указанный в значении **Key ID** (Идентификатор ключа) для пакета.

Для определения ключей и управления ими используйте страницу **MD5 Routing Authentication** (Проверка подлинности для маршрутизации MD5). Чтобы открыть страницу **MD5 Routing Authentication** (Проверка подлинности для маршрутизации MD5), выберите **Router** (Маршрутизатор) → **Global Routing Parameters** (Параметры глобальной маршрутизации) → **MD5 Routing Authentication** (Проверка подлинности для маршрутизации MD5) на панели дерева.

Рис. 8-5. Проверка подлинности для маршрутизации MD5



Key ID (Идентификатор ключа) - определяет идентификатор ключа.

MD5 Key String (Строка ключа MD5) - показывает пароль, который используется для проверки подлинности при маршрутизации.

Start Accepting From (Начать прием с) - дата и время, когда ключ MD5 начинает принимать трафик с указанным ключом MD5. В поле Start Accept (Начать прием) используется следующий формат **месяц день год: час минута секунда**.

Stop Accepting At (Прекратить прием) - дата и время, когда ключ MD5 перестает принимать трафик с указанным ключом MD5. В поле Stop Accept (Начать прием) используется следующий формат **месяц день год: час минута секунда**. Если выбрано значение Forever (Постоянно), для приема трафика с указанным ключом MD5 не устанавливается никаких ограничений.

Start Generating From (Начать генерацию с) - дата и время, когда пакеты протокола пересылаются с помощью ключей MD5. В поле Start Generate (Начать генерацию) используется следующий формат **месяц день год: час минута секунда**.

Stop Generating At (Прекратить генерацию) - дата и время, когда прекращается пересылка пакетов протокола с помощью ключей MD5. В поле Stop Generate (Начать генерацию) используется следующий формат **месяц день год: час минута секунда**. Если выбрано значение Forever (Постоянно), для приема трафика с указанным ключом MD5 не устанавливается никаких ограничений.

Remove (Удалить) - когда этот флажок установлен, ключ MD5 удаляется.

Добавление ключа MD5

1. Откройте страницу [MD5 Routing Authentication](#) (Проверка подлинности для маршрутизации MD5).
2. Щелкните **Add** (Добавить), чтобы отобразить страницу **Add MD5 Key** (Добавление ключа MD5).

Рис. 8-6. Добавление ключа MD5

Add MD5 Key

New Key ID (1-255)

MD5 Key String (16 Characters)

Start Accepting From Month: Jan Day: 1 Year: 2000 At: Hour: 0 Minutes: 0 Seconds: 0

Stop Accepting At Forever Month: Dec Day: 31 Year: 2097 At: Hour: 23 Minutes: 59 Seconds: 0

Start Generating From Month: Jan Day: 1 Year: 2000 At: Hour: 0 Minutes: 0 Seconds: 0

Stop Generating At Forever Month: Dec Day: 31 Year: 2097 At: Hour: 23 Minutes: 59 Seconds: 0

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

Новый ключ MD5 добавится в таблицу **MD5 Key Table** (Таблица ключей MD5), а устройство будет обновлено.

Изменение ключа MD5

1. Откройте страницу [MD5 Routing Authentication](#) (Проверка подлинности для маршрутизации MD5).
2. В раскрывающемся меню **Entry No.** (Номер записи) выберите ключ MD5, который необходимо изменить.
3. Измените значения в полях диалогового окна.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Новый ключ MD5 изменится, а устройство будет обновлено.

Удаление ключа MD5

1. Откройте страницу [MD5 Routing Authentication](#) (Проверка подлинности для маршрутизации MD5).
2. Нажмите кнопку **Show All** (Показать все), чтобы отобразить таблицу **MD5 Key Table** (Таблица ключей MD5).
3. Выберите запись в поле **Key ID** (Идентификатор ключа).
4. Установите флажок **Remove** (Удалить).
5. Нажмите кнопку **Apply Changes** (Применить изменения).

Ключ MD5 будет удален, а устройство обновлено.

Настройка проверки подлинности MD5 с помощью команд консоли

В следующей таблице приведены команды консоли для настройки проверки подлинности MD5.

Таблица 8-4. Команды консоли для проверки подлинности MD5

Команда консоли	Описание
<code>key идентификатор_ключа</code>	Создает ключ проверки подлинности.

<pre>accept-lifetime { duration time-to-start day-of-the-month день _месяца year-to-start key-lifetime- duration-in-seconds } { infinite time-to-start day-of-the-month день _месяца year-to-start } { time-to-start day-of-the-month день _месяца year-to-start time-to-stop day-of-the-month день_месяца year-to-stop }</pre>	<p>Устанавливает временной интервал, в течение которого можно получить ключ проверки подлинности в цепочке ключей.</p>
<pre>send-lifetime { duration time-to-start day-of-the-month день _месяца year-to-start key-lifetime- duration-in-seconds } { infinite time-to-start day-of-the-month день _месяца year-to-start } { time-to-start day-of-the-month день _месяца year-to-start time-to-stop day-of-the-month день_месяца year-to-stop }</pre>	<p>Устанавливает временной интервал, в течение которого можно отправить ключ проверки подлинности в цепочке ключей.</p>

Далее приведен пример команд консоли.

```
Console (config)# key 3
```

```
Console (config-key)# accept-lifetime duration 13:30:00 Jan 25 2002 7200
```

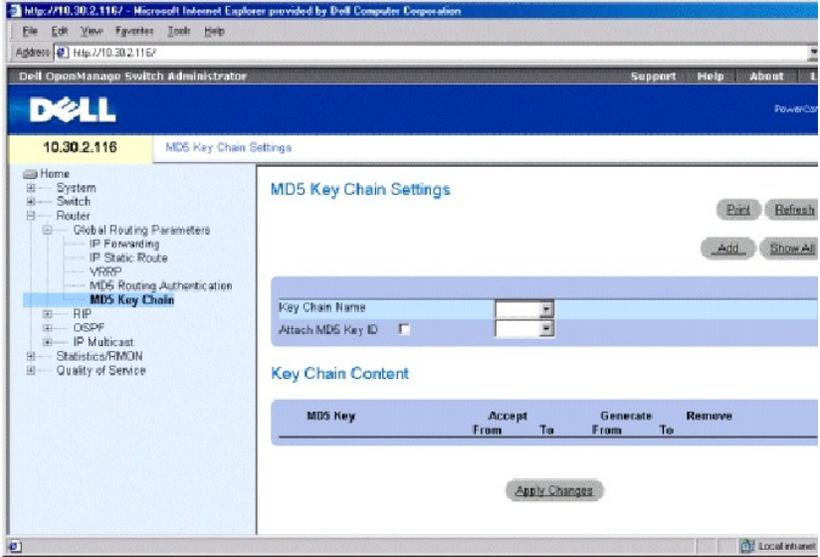
```
Console (config-key)# send-lifetime duration 14:00:00 Jan 25 2002 3600
```

Настройка параметров цепочки ключей MD5

После определения ключей они группируются в так называемую «цепочку ключей». Для каждого интерфейса маршрутизатора можно назначить одновременно несколько ключей. Ключи можно группировать в цепочки для удобства их назначения для интерфейсов. Каждый ключ можно включать в несколько цепочек ключей. Цепочки ключей назначаются для интерфейсов в параметрах интерфейса RIP или OSPF. Ключи MD5 добавляются в цепочку ключей MD5 для создания цепочки ключей.

Для определения цепочки ключей и назначения в них ключей используйте страницу MD5 Key Chain Settings (Параметры цепочки ключей MD5). Чтобы открыть страницу MD5 Key Chain Settings (Параметры цепочки ключей MD5), выберите Router (Маршрутизатор) → Global Routing Parameters (Параметры глобальной маршрутизации) → MD5 Key Chain (Цепочка ключей MD5) на панели дерева.

Рис. 8-7. Параметры цепочки ключей MD5



Key Chain Name (Имя цепочки ключей) - имена цепочки ключей, определяемые пользователем.

Attach MD5 Key ID (Приложить идентификатор ключа MD5) - показывает строковый идентификатор ключа, присоединенный к цепочке ключей.

MD5 Key (Ключ MD5) - ключ, принадлежащий цепочке ключей.

Accept From (Принимать с) - дата и время, когда выбранный ключ MD5 начинает принимать трафик с указанным ключом MD5. В поле **Accept From** (Принимать с) используется следующий формат **месяц день год: час минута секунда**. Поле **Accept From** (Принимать с) - ключ, определяемый на странице [MD5 Routing Authentication](#) (Проверка подлинности для маршрутизации MD5).

Accept To (Принимать по) - дата и время, когда выбранный ключ MD5 прекращает принимать трафик с указанным ключом MD5. В поле используется следующий формат **месяц день год: час минута секунда**. Поле **Accept To** (Принимать с) - ключ, определяемый на странице [MD5 Routing Authentication](#) (Проверка подлинности для маршрутизации MD5).

Generate From (Генерировать с) - дата и время, когда выбранный ключ MD5 начинает пересылать трафик. В поле **Generate From** (Генерировать с) установлен следующий формат **месяц день год: час минута секунда**. Поле **Generate From** (Генерировать с) - это ключ, определяемый на странице [MD5 Routing Authentication](#) (Проверка подлинности для маршрутизации MD5).

Generate To (Генерировать по) - дата и время, когда выбранный ключ MD5 прекращает пересылать трафик. В поле **Generate To** (Генерировать по) установлен следующий формат **месяц день год: час минута секунда**. Поле **Generate To** (Генерировать по) - это ключ, определяемый на странице [MD5 Routing Authentication](#) (Проверка подлинности для маршрутизации MD5).

Remove (Удалить) - когда этот флажок установлен, ключ MD5 удаляется из таблицы MD5 Key Chain Table (Таблица цепочек ключей MD5).

Добавление цепочки ключей MD5

1. Откройте страницу [MD5 Key Chain Settings](#) (Параметры цепочки ключей MD5).
2. Щелкните **Add** (Добавить), чтобы отобразить страницу **Add Key Chain** (Добавление цепочки ключей).
3. Введите значения в полях **New Key Chain Name** (Имя новой цепочки ключей) и **Attach MD5 Key No.** (Приложить номер ключа MD5).
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Новая цепочка ключей MD5 добавится в таблицу MD5 Key Chain Table (Таблица цепочек ключей MD5), а устройство будет обновлено.

Изменение цепочки ключей MD5

1. Откройте страницу [MD5 Key Chain Settings](#) (Параметры цепочки ключей MD5).
2. Измените значения полей **Name** (Имя) и **Key Chain ID** (Идентификатор цепочки ключей).
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Новая цепочка ключей MD5 изменится, а устройство будет обновлено.

Удаление цепочки ключей MD5

1. Откройте страницу [MD5 Key Chain Settings](#) (Параметры цепочки ключей MD5).
2. Нажмите кнопку **Show All** (Показать все), чтобы отобразить таблицу **MD5 Key Chain Table** (Таблица цепочек ключей MD5).
3. Выберите запись в поле **Key Chain Name** (Имя цепочки ключей).
4. Установите флажок **Remove** (Удалить).
5. Нажмите кнопку **Apply Changes** (Применить изменения).

Новая цепочка ключей MD5 удалится, а устройство будет обновлено.

Настройка цепочек ключей с помощью команд консоли

В следующей таблице приведены команды консоли для настройки цепочек ключей.

Таблица 8-5. Команды консоли для настройки цепочки ключей

Команда консоли	Описание
<code>key-chain имя_цепочки</code>	Определяет группу ключей проверки подлинности.
<code>key идентификатор_ключа</code>	Определяет ключ проверки подлинности в цепочке ключей.
<code>key-string текст</code>	Определяет строку проверки подлинности для ключа.
<code>accept-lifetime начальное_время конечное_время {infinite начальное_время duration начальное_время секунды} no accept-lifetime</code>	Устанавливает временной интервал, в течение которого действителен ключ для проверки подлинности входящих пакетов.
<code>send-lifetime начальное_время конечное_время {infinite начальное_время duration начальное_время секунды} no send-lifetime</code>	Устанавливает временной интервал, в течение которого действителен ключ проверки подлинности для создания сборника MD5 для исходящих пакетов.
<code>show key-chains [имя_цепочки]</code>	Отображает данные цепочки ключей.

Далее приведен пример команд консоли.

```
Console (config)# key chain M
```

```
Console (config-key-chain)# key 1
```

```
Console (config-key)# key-string mountain
```

```
Console (config-key)# accept-lifetime duration 13:30:00 Jan 25 2002 7200
```

```
Console (config-key)# send-lifetime duration 14:00:00 Jan 25 2002 3600
```

```
Console (config-key)# exit
```

```
Console(config)# exit
```

```
Console# show key-chains
```

```
key chain internal
```

```
key 1
```

```
accept: 13:30:00 Jan 25 2002 duration 7200
```

send: 14:00:00 Jan 25 2002 duration 3600

key 2

accept: 14:30:00 Jan 25 2002 duration 7200

send: 15:00:00 Jan 25 2002 duration 3600

key chain external

key 1

accept: 13:30:00 Jan 25 2002 until 15:30:00 Jan 25 2002

send: 14:00:00 Jan 25 2002 until 15:00:00 Jan 25 2002

key 2

accept: 14:30:00 Jan 25 2002 until 16:30:00 Jan 25 2002

send: 15:00:00 Jan 25 2002 until 16:00:00 Jan 25 2002

25 2002

Настройка протокола RIP

Протокол RIP (Routing Information Protocol) - это наиболее часто используемый стандарт Интернета для внутренних протоколов шлюза. Протокол выполняет широковещательную передачу данных маршрутизации для определения наискорейшего маршрута до следующего места назначения. RIP - это протокол дистанционно-векторной маршрутизации, который идеально подходит для малых сетей. Маршруты определяются по наименьшему числу узлов. Обновления маршрутизации содержат пары значений, состоящих из IP-адреса и расстояния до узла.

Протокол RIP версии 2 выполняет следующее.

- 1 Поддерживает маски подсетей.
- 1 Предоставляет методы проверки подлинности.
- 1 Поддерживает протоколы маршрутизации.
- 1 Обеспечивает большее распространение и предъявляет меньшие требования к размеру полосы пропускания.

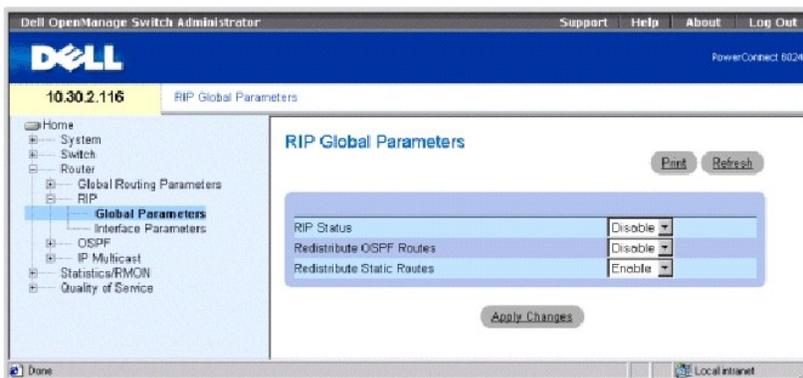
Протокол RIP настраивается на странице RIP. Чтобы открыть страницу RIP, выберите Router (Маршрутизатор)→ RIP на панели дерева.

Определение общих параметров RIP

Страница **RIP Global Parameters** (Общие параметры RIP) содержит поля для включения протокола RIP на устройстве, обеспечивая перераспределение трафика OSPF и статических маршрутов.

Выберите **Router** (Маршрутизатор) → **RIP Global Parameters** (Общие параметры) на панели дерева, чтобы отобразить страницу **RIP Global Parameters** (Общие параметры RIP).

Рис. 8-8. Страница RIP Global Parameters (Общие параметры RIP)



RIP Status (Состояние RIP) - включает или отключает протокол RIP на устройстве.

Redistribute OSPF Routes (Перераспределение маршрутов OSPF) - когда включен этот параметр, выполняется перераспределение маршрутов из OSPF в RIP. Перераспределение маршрутов подразумевает импорт сторонних интерфейсов маршрутизации в RIP.

Redistribute Static Routes (Перераспределение статических маршрутов) - когда включен этот параметр, выполняется перераспределение маршрутов из статических маршрутов в RIP.

Включение RIP, перераспределения маршрутов OSPF, перераспределения статических маршрутов

1. Откройте страницу **RIP Global Parameters** (Общие параметры RIP).
2. Выберите **Enabled** (Включен) в поле общего параметра RIP, который необходимо включить.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

RIP будет включен на устройстве.

Настройка общих параметров RIP с помощью команд консоли

В следующей таблице приведены команды консоли для настройки общих параметров RIP.

Таблица 8-6. Команды консоли для настройки общих параметров RIP

Команда консоли	Описание
<code>router rip enable</code>	Включает протокол RIP (Routing Information Protocol) на устройстве.
<code>no router rip enable</code>	Отключает протокол RIP (Routing Information Protocol) на устройстве.

<code>router rip redistribute ospf</code>	Объявляет маршруты, определенные OSPF в процессе RIP.
<code>no router rip redistribute ospf</code>	Прекращает объявление о маршрутах, определенных OSPF в процессе RIP.
<code>router rip redistribute static</code>	Объявляет маршруты, статически настроенные в процессе RIP.
<code>no router rip redistribute static</code>	Прекращает объявление о маршрутах, настроенных статически в процессе RIP.

Далее приведен пример команд консоли.

```
Console (config)# router rip enable
```

```
Console (config)# router rip redistribute ospf
```

```
Console (config)# router rip redistribute static
```

```
Console (config)# no router rip enable
```

```
Console (config)# no router rip redistribute ospf
```

```
Console (config)# no router rip redistribute static
```

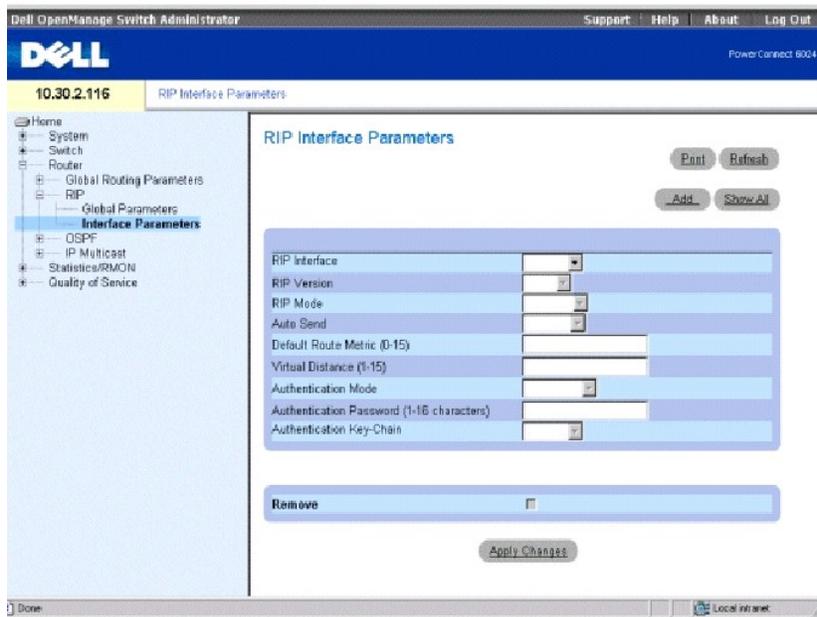
Определение параметров интерфейса RIP

Используйте страницу **RIP Interface Parameters** (Параметры интерфейса RIP) для определения IP-адресов, для которых включен протокол RIP, определения метрики маршрутов, включения функции автоотправки, определения виртуального расстояния и состояния IP-адреса.

 **ПРИМЕЧАНИЕ.** Чтобы определить интерфейс RIP, необходимо включить протокол RIP. Для получения дополнительной информации см. раздел [«Включение RIP, перераспределения маршрутов OSPF, перераспределения статических маршрутов»](#).

Чтобы открыть страницу **RIP Interface Parameters** (Параметры интерфейса RIP), выберите **Router** (Маршрутизатор)→ **RIP**→ **RIP Interface Parameters** (Параметры интерфейса RIP) на панели дерева.

Рис. 8-9. Страница RIP Interface Parameters (Параметры интерфейса RIP)



RIP Interface (Интерфейс RIP) - текущий IP-адрес интерфейса.

RIP Version (Версия RIP) - тип передаваемого RIP. Возможные значения:

Вер. 1 - передает обновления RIP, соответствующие RFC 1058.

Вер. 2 - указывает, что устройство передает обновления RIP 2.

RIP Mode (Режим RIP) - тип управления RIP. Возможные значения:

RX - на устройстве выполняется прием широковещательной передачи RIP.

RX & TX - на устройстве выполняется прием и широковещательная передача RIP.

Auto Send - (Автопередача) - разрешает устройству отправлять сообщения RIP только с использованием метрики по умолчанию, что позволяет станциям определить адрес маршрутизатора по умолчанию. В результате маршрутизатор не передает объемные обновления RIP по каналам связи, если не существует маршрутизатора для их получения. Когда включена функция **Auto Send** (Автопередача), передается краткое обновление RIP, позволяющее станциям контролировать RIP для выполнения обнаружения маршрутизаторов и т.д., а также для отправки обновления RIP для маршрутизаторов, которые могут быть добавлены в сеть позже.

Если обновление RIP принимается на интерфейсе, функция **Auto Send** (Автопередача) отключается для этого интерфейса и передаются полные обновления RIP. Если устройство обнаружит другое сообщение RIP, функция **Auto Send** (Автопередачи) отключается.

Default Route Metric (1-16) (Метрика маршрута по умолчанию (1-16)) - метрика записи маршрута по умолчанию в RIP обновляет создаваемый на этом интерфейсе. Значение ноль указывает, что маршрут по умолчанию не создается.

Virtual Distance (1-16) (Виртуальное расстояние (1-16)) - виртуальное число узлов, назначенное для интерфейса. Это позволяет точно настроить алгоритм маршрутизации RIP.

Authentication Mode (Режим проверки подлинности) - тип проверки подлинности интерфейса, пароль или ключ MD5, используемые для проверки подлинности сообщений RIP версии 2.

Authentication Password (Пароль для проверки подлинности) - пароль для проверки подлинности.

Authentication Key-Chain (Цепочка ключей для проверки подлинности) - цепочка ключей для проверки подлинности.

Remove (Удалить) - когда установлен этот флажок, удаляется интерфейс RIP.

Добавление интерфейса RIP

1. Откройте страницу **RIP Interface Parameters** (Параметры интерфейса RIP).
2. Щелкните **Add** (Добавить), чтобы отобразить страницу **New RIP Interface** (Добавление нового интерфейса RIP).
3. Заполните поля на этой странице.

На этой странице те же поля, что и на странице **RIP Interface Parameters** (Параметры интерфейса RIP).

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

Изменение параметров интерфейса RIP

1. Откройте страницу **RIP Interface Parameters** (Параметры интерфейса RIP).
2. Выполните необходимые изменения в полях.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Параметры интерфейса RIP будут изменены, а устройство обновлено.

Удаление интерфейса RIP

1. Откройте страницу **RIP Interface Parameters** (Параметры интерфейса RIP).
2. С помощью раскрывающегося меню **RIP Interface** (Интерфейс RIP) выберите интерфейс RIP.
3. Установите флажок **Remove** (Удалить).
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Интерфейс RIP будет удален, а устройство обновлено.

Настройка интерфейсов RIP с помощью команд консоли

В следующей таблице приведены команды консоли для настройки общих параметров RIP.

Таблица 8-7. Команды консоли для настройки RIP

Команда консоли	Описание
<code>rip</code>	Включает протокол RIP для интерфейса.
<code>rip version {1 2}</code>	Указывает версию протокола RIP.
<code>rip passive-interface</code>	Отключает отправку обновлений маршрутизации для интерфейса.

<code>rip auto-send</code>	Автоматически определяют, требуется ли отправка данных RIP на интерфейс.
<code>rip offset смещение</code>	Добавляет смещение к метрике, полученной по протоколу RIP перед добавлением ее в таблицу интерфейса.
<code>rip default-route offset смещение</code>	Создает маршрут по умолчанию для RIP, применяя значение смещения.
<code>rip authentication {text текст / имя_цепочки_md5}</code>	Включает проверку подлинности для пакетов RIP версии 2 и указывает тип проверки подлинности.
<code>show ip rip</code>	Отображает данные IP RIP
<code>show ip rip md5</code>	Отображает данные IP RIP MD5.

Далее приведен пример команд консоли.

```
Console (config)# router rip enable
```

```
Console(config)# interface ip 100.1.1.1
```

```
Console(config-ip)# rip
```

```
Console(config-ip)# rip version 1
```

```
Console(config-ip)# rip passive interface
```

```
Console(config-ip)# rip auto-send
```

```
Console(config-ip)# rip offset 5
```

```
Console(config-ip)# rip default-route offset 5
```

```
Console(config-ip)# rip authorization text dell
```

```
Console (config-ip)# exit
```

```
Console(config)# exit
```

```
Console# show ip rip
```

RIP включен.

OSPF leaking is enabled.

Static leaking is enabled.

Interface State Ver Offset Default Route Passive Auto Send Auth

176.16.0.0/16 Enabled 2 1 Disabled No Yes MD5

192.168.0.0/16 Enabled 2 1 Disabled No No Текст

Настройка параметров и фильтров OSPF

OSPF (Open Shortest Path First) - это внутренний протокол шлюза, позволяющий маршрутизаторам обмениваться сообщениями о состоянии каналов для сбора информации о сети и определения наилучшего маршрута на основании расстояния между узлами сети.

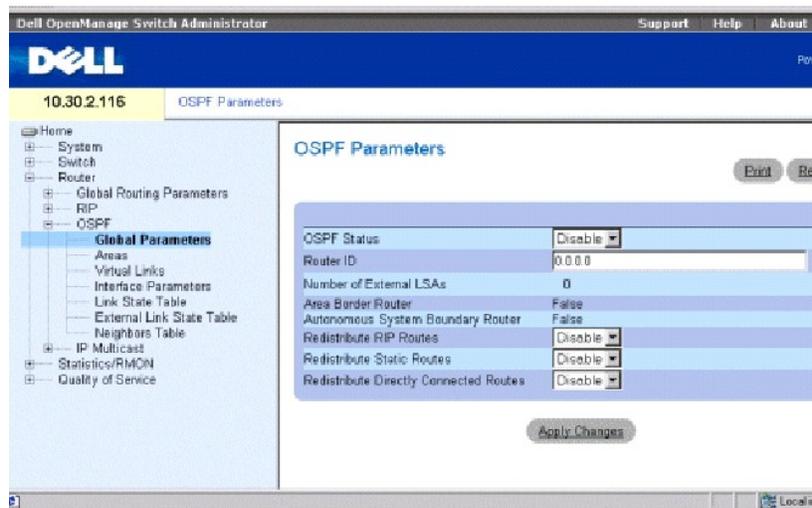
OSPF - это протокол состояния канала, а не дистанционно-векторной маршрутизации, и поэтому для него необходима меньшая полоса пропускания, чем для RIP. Для включения и определения OSPF используется:

- 1 [Настройка параметров OSPF](#)
- 1 [Настройка областей OSPF](#)
- 1 [Настройка виртуальных соединений OSPF](#)
- 1 [Просмотр таблицы состояния канала](#)
- 1 [Просмотр таблицы состояния внешних каналов](#)
- 1 [Просмотр таблицы соседей OSPF](#)

Настройка параметров OSPF

OSPF находит лучший маршрут по расстоянию между узлами. OSPF включается на странице **OSPF Parameters** (Параметры OSPF). Чтобы открыть страницу **OSPF Parameters** (Параметры OSPF), выберите **Router** (Маршрутизатор) → **OSPF Global Parameters** (Общие параметры) на панели дерева.

Рис. 8-10. Страница OSPF Global Parameters (Общие параметры OSPF)



OSPF Status (Состояние OSPF) - включает протокол OSPF по крайней мере для одного интерфейса или отключает его для всех интерфейсов.

Router ID (Идентификатор маршрутизатора) - номер идентификатора маршрутизатора. По умолчанию в качестве идентификатора маршрутизатора используется IP-адрес устройства. **Router ID** (Идентификатор маршрутизатора) - это дополнительное поле, в качестве значения по умолчанию для которого используется наименьший IP-интерфейс устройства.

Number of External LSAs (Число внешних LSA) - число внешних оповещений о состоянии канала (LSA) в базе данных состояния канала.

Area Border Router (ABR) (Граничный маршрутизатор области) - указывает, что устройство является граничным маршрутизатором области. Если устройство настроено как ABR, оно подключено к двум или более областям. Одна область является магистральной.

Autonomous System Boundary Router (ASBR) (Граничный маршрутизатор автономной системы) - указывает, что устройство настроено как ASBR. Если устройство настроено как ASBR, устройство может импортировать данные маршрутизации из протоколов маршрутизации отличных от OSPF.

Redistribute RIP Routes (Перераспределение маршрутов RIP) - включает или отключает перераспределение маршрутов, вставленных в таблицу IP маршрутизации протоколом RIP для объявления OSPF как внешних маршрутов.

Redistribute Static Routes (Перераспределение статических маршрутов) - включает объявление всех статически настроенных маршрутов как внешних маршрутов OSPF или отключает перераспределение статических маршрутов.

Redistribute Directly Connected Routes (Перераспределение маршрутов подключенных напрямую) - включает объявление всех внешних маршрутов как внешних маршрутов OSPF или отключает перераспределение внешних маршрутов, подключенных напрямую.

Включение OSPF

1. Откройте страницу **OSPF Parameters** (Параметры OSPF).
2. Определите поля **OSPF Status** (Состояние OSPF), **Router ID** (Идентификатор маршрутизатора), **Redistribute RIP Routes** (Перераспределение маршрутов RIP), **Redistribute Static Routes** (Перераспределение статических маршрутов) и **Redistribute Directly Connected Routes** (Перераспределение маршрутов, подключенных напрямую).
3. Нажмите кнопку **Apply Changes** (Применить изменения).

OSPF включен на устройстве.

 **ПРИМЕЧАНИЕ.** Процессы OSPF можно удалить только с помощью команды консоли `clear ip ospf process`.

Включение OSPF с помощью команд консоли

В следующей таблице приведены команды консоли для включения OSPF.

Таблица 8-8. Команды консоли для включения OSPF

Команда консоли	Описание
<code>router ospf enable</code>	Включает процесс маршрутизации OSPF.
<code>router ospf router-id ip-адрес</code>	Настраивает идентификатор маршрутизатора OSPF.
<code>router ospf redistribute rip</code>	Включает объявление маршрутов, которые распознаются процессом RIP в процессе маршрутизации OSPF.
	Объявление маршрутов, настроенных статически, в процессе маршрутизации OSPF.

router ospf redistribute static	Объявление маршрутов, подключенных напрямую.
outer ospf redistribute connected	

Далее приведен пример команд консоли.

```
Console (config)# router ospf enable
```

```
Console (config)# router ospf router-id 196.127.2.1
```

```
Console (config)# router ospf redistribute rip
```

```
Console (config)# router ospf redistribute static
```

Настройка областей OSPF

Страница **OSPF Areas** (Области OSPF) содержит информацию для определения и изменения областей OSPF, внутри которых определяются интерфейсы и виртуальные каналы. После создания области OSPF протокол OSPF автоматически включается для всех IP-интерфейсов.

Чтобы открыть страницу **OSPF Areas** (Области OSPF), выберите **Router** (Маршрутизатор) → **OSPF Areas** (Области) на панели дерева.

Рис. 8-11. Страница OSPF Areas (Области OSPF)



Area ID (Идентификатор области) - идентификатор области. в формате IP-адреса.

Import Autonomous System External (Импорт внешних автономной системы) - показывает, является ли эта область областью «заглушки». Возможные значения:

Import External (Импорт внешних) - внешние объявления о состоянии канала автономной системы (LSA) можно импортировать в область.

Import No External (Импорт не внешних) - внешние объявления LSA невозможно импортировать в область; поэтому эта область называется областью «заглушки».

Area Summary (Сводка по областям) - управляет импортом сводки по областям LSA в тупиковые области. Эта переменная не оказывает влияние на другие области. Возможные значения:

No Area Summary (Без сводки по областям) - указывает, что эта область является полностью тупиковой областью.

Send Area Summary (Отправить сводку по областям) - указывает, что эта область не полностью является областью «заглушки».

Область «заглушки» - это область, в которую не попадают внешние объявления LSA. Области, которые являются полностью тупиковыми, используют маршрут по умолчанию для достижения только мест назначения, являющихся внешними для автономной системы, но также и все мест назначения, являющихся внешними для области. Чтобы использовать поддержку тупиковых областей протокола OSPF, необходимо использовать маршрутизацию по умолчанию в тупиковой области.

Default Stub Metric (0-16777216) (Метрика тупиковой области по умолчанию (0-16777216)) - метрика маршрута по умолчанию, созданного для тупиковой области. Тупиковые области не импортируют внешние AS. Поэтому маршрут по умолчанию создается граничным маршрутизатором области для тупиковой области.

Metric Type (Тип метрики) - тип метрики протокола.

Remove (Удалить) - когда установлен этот флажок, IP-адрес удаляется из таблицы областей OSPF.

Определение новой области OSPF

1. Откройте страницу **OSPF Areas** (Области OSPF).
2. Щелкните **Add** (Добавить), чтобы отобразить страницу **Add an OSPF Area** (Добавление области OSPF).
3. Введите значения в полях диалогового окна.

 **ПРИМЕЧАНИЕ.** Поле **Stub Metric** (Метрика тупиковой области) определяется для граничных маршрутизаторов области.

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

Новая область будет добавлена в таблицу областей OSPF.

Изменение параметров области OSPF

1. Откройте страницу **OSPF Areas** (Области OSPF).
2. Выберите **Area ID** (Идентификатор области).

Отобразятся параметры для области OSPF.

3. Выполните необходимые изменения в полях.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Параметры области будут изменены и сохранены на устройстве.

Удаление области OSPF

1. Откройте страницу **OSPF Areas** (Области OSPF).

2. Нажмите кнопку **Show All** (Показать все), чтобы отобразить таблицу областей OSPF.
3. Выберите область OSPF и установите флажок **Remove** (Удалить).
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Область OSPF будет удалена из таблицы, а устройство обновлено.

Определение областей OSPF с помощью команд консоли

В следующей таблице приведены команды консоли для определения областей OSPF.

Таблица 8-9. Команды консоли для определения областей OSPF

Команда консоли	Описание
<code>router ospf area идентификатор_области stub</code>	Определяет область как тупиковую. Чтобы отключить эту функцию, используйте форму по этой команды.
<code>router ospf area идентификатор_области стоимость_по_умолчанию cost</code>	Указывает стоимость для маршрута сводки по умолчанию, передаваемой в тупиковую область.

Далее приведен пример команд консоли.

```
Console (config)# router ospf enable
```

```
Console (config)# router ospf area 7.7.7.7 stub
```

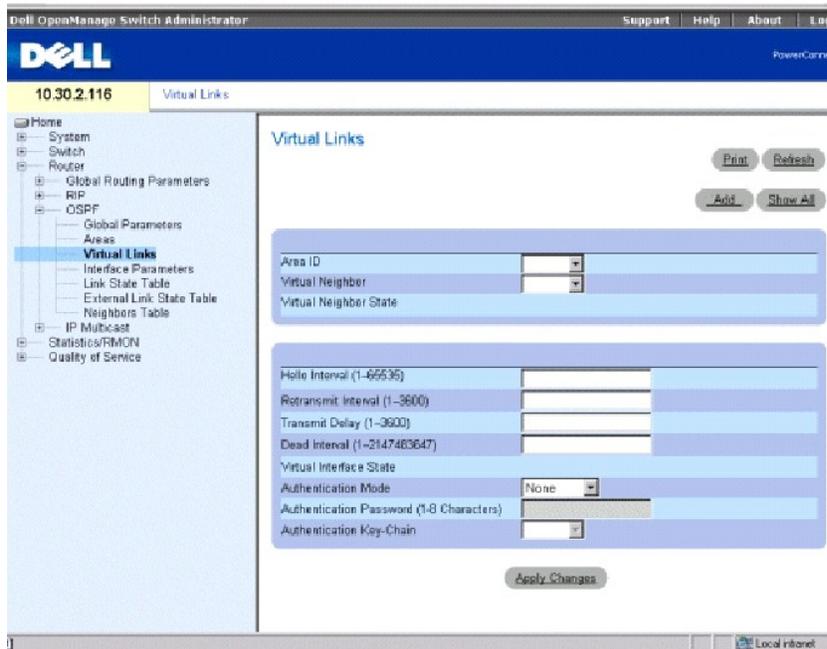
```
Console (config)# router ospf area 192.168.3.1 default-cost 10000
```

Настройка виртуальных соединений OSPF

OSPF требует, чтобы все области были связаны между собой с помощью магистральной области. Однако если область не подсоединена к магистрале, можно соединить два граничных маршрутизатора области с помощью виртуального канала. Виртуальные каналы определяются путем настройки виртуального соседа. Виртуальные каналы можно настраивать через тупиковую область.

Определите виртуальные каналы на странице **Virtual Links** (Виртуальные каналы). Чтобы открыть страницу **Virtual Links** (Виртуальные каналы), выберите **Router** (Маршрутизатор) → **OSPF** → **Virtual Links** (Виртуальные каналы) на панели дерева.

Рис. 8-12. Страница Virtual Links (Виртуальные каналы)



Area ID (Идентификатор области) - Идентификатор области интерфейса OSPF транзитной области.

Virtual Neighbor (Виртуальный сосед) - идентификатор маршрутизатора виртуального соседа.

Virtual Neighbor State (Состояние виртуального соседа) - состояние виртуального соседа.

Hello Interval (1-65535) (Интервал приветствия (1-65535)) - время в секундах между Hello-пакетами. Все устройства, подключенные к общей сети, должны иметь одинаковый интервал приветствия. Значение по умолчанию: 10 секунд.

Retransmit Interval (0-3600) (Интервал повторной передачи (0-3600)) - время (в секундах) между повторной передачей объявлений о состоянии канала (LSA) для соседних узлов, принадлежащих интерфейсу. Значение должно быть больше ожидаемой задержки обратной передачи между двумя маршрутизаторами, подключенными к сети. Значение по умолчанию: 5 секунд.

Transmit Delay(0-3600) (Задержка передачи (0-3600)) - приблизительное время (в секундах), необходимое для отправки пакета о состоянии канала для интерфейса. Объявления LSA в пакете обновления имеют свой возраст, которые увеличивается на данное значение перед передачей. Значение по умолчанию: 1 секунда.

Dead Interval (0-2147483647) (Интервал отключения (1-2147483647)) - время в секундах, по истечении которого маршрутизатор, не посылающий пакеты Hello, отключается. Значение должно быть кратным значению **Hello Interval** (Интервал приветствия). Все маршрутизаторы, подключенные к общей сети, должны иметь одинаковое значение для этого параметра. Значение по умолчанию: 60 секунд.

Virtual Interface State (Состояние виртуального интерфейса) - показывает состояние виртуального интерфейса.

Authentication Mode (Режим проверки подлинности) - тип проверки подлинности интерфейса, пароль или ключ MD5, используемые для проверки подлинности сообщений о состоянии канала OSPF.

Authentication Password (1-8 Characters) (Пароль проверки подлинности (1-8 символов)) - пароль (восемь символов или менее), используемый для проверки сообщений о состоянии канала OSPF.

Authentication Key-Chain (Цепочка ключей проверки подлинности) - цепочка ключей MD5, используемая для проверки подлинности сообщений о состоянии канала OSPF.

Добавление виртуального канала

1. Откройте страницу **Virtual Links** (Виртуальные каналы).
2. Щелкните **Add** (Добавить), чтобы отобразить страницу **Add a Virtual Link** (Добавление виртуального канала).

Рис. 8-13. Страница Add a Virtual Link (Добавление виртуального канала)

The screenshot shows a web browser window titled "Add a Virtual Link" with a "Default" button in the top right corner. The main content area contains a form with the following fields and controls:

- Area ID:** A dropdown menu currently showing "Virtual Link 1".
- Virtual Link ID:** A text input field.
- Hello Interval (1-65535):** A text input field with a "(Sec)" label.
- Retransmit Interval (3-3500):** A text input field with a "(Sec)" label.
- Transmit Delay (1-3000):** A text input field with a "(Sec)" label.
- Dead Interval (1-147485647):** A text input field with a "(Sec)" label.
- Authentication Mode:** A dropdown menu currently showing "Password".
- Authentication Password (1-63 Character):** A text input field.
- Authentication Key-Chain:** A dropdown menu currently showing "Name of Key Chain".

At the bottom of the form is an "Apply Changes" button.

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

Будет добавлен новый виртуальный канал OSPF.

Изменение виртуальных каналов

1. Откройте страницу **Virtual Links** (Виртуальные каналы).
2. Выберите идентификатор области в раскрывающемся меню **Area ID** (Идентификатор области).

Отобразятся параметры для поля.

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

Параметры виртуального канала OSPF будут изменены и сохранены на устройстве.

Удаление виртуального канала OSPF

1. Откройте страницу **Virtual Links** (Виртуальные каналы).
2. Нажмите кнопку **Show All** (Показать все), чтобы отобразить таблицу **Virtual Links Table** (Таблица виртуальных каналов).
3. Выберите виртуальный канал.

Появятся параметры полей для записи таблицы.

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

Виртуальный канал будет удален, а устройство обновлено.

Просмотр виртуальных каналов OSPF с помощью команд консоли

В следующей таблице приведены команды консоли для определения областей OSPF.

Таблица 8-10. Команды консоли для виртуальных каналов OSPF

Команда консоли	Описание
<code>show ip ospf virtual-links [area идентификатор_области] [router идентификатор_маршрутизатора]</code>	Отображает параметры и текущее состояние виртуальных каналов OSPF.
<code>router ospf area area идентификатор_виртуального_канала_идентификатор_маршрута</code>	Добавляет виртуальный канал.

Далее приведен пример команд консоли.

```
Console (config)# show ip ospf virtual-links
```

```
Virtual Link to router 192.168.101.2 is up
```

```
Virtual link has simple password authentication
```

```
Transit area 0.0.0.1
```

```
Transmit Delay is 1 sec, State POINT_TO_POINT
```

```
Timer intervals configured, Hello 10, Dead 40, Retransmit 5
```

```
Adjacency State FULL
```

```
Console (config)#router ospf area 176.16.1.0 virtual-link 176.16.8.7
```

```
Console (config)#router ospf area 176.16.1.0 virtual-link 176.16.8.7
```

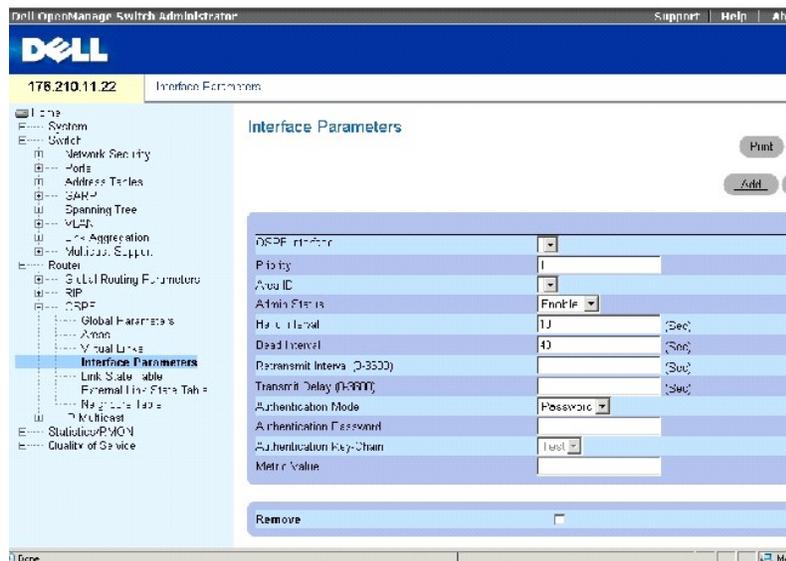
Настройка параметров интерфейса OSPF

После определения общих параметров OSPF можно настроить протокол OSPF для каждого интерфейса.

Функция автосоздания позволяет автоматически настроить OSPF для каждого интерфейса после определения области. Интерфейсы OSPF также могут определяться пользователем. Таблица интерфейсов OSPF включает IP-маршрутизацию, используя данные OSPF.

Чтобы открыть страницу **Interface Parameters** (Параметры интерфейса), выберите **Router** (Маршрутизатор) → **OSPF** → **Interface Parameters** (Параметры интерфейса) на панели дерева.

Рис. 8-14. Страница Interface Parameters (Параметры интерфейса)



OSPF Interface (Интерфейс OSPF) - IP-адрес интерфейса OSPF.

Priority (Приоритет) - приоритет интерфейса. Значение 0 показывает, что устройство нельзя определить в качестве устройства назначения в текущей сети. Если несколько устройств имеют одинаковый приоритет, используется идентификатор маршрутизатора. Возможные значения поля: 0-255. Значение по умолчанию: 1.

Area ID (Идентификатор области) - идентификатор области интерфейса OSPF.

Admin Status (Состояние администратии) - включает или отключает процессы OSPF.

Hello Interval (Интервал приветствия) - временной интервал в секундах между Hello-пакетами. Все устройства, подключенные к общей сети, должны иметь одинаковый интервал приветствия. Возможные значения поля: 1-65535. Значение по умолчанию: 10 секунд.

Dead Interval (Интервал отключения) - интервал времени в секундах, по истечении которого маршрутизатор, не посылающий пакеты Hello, отключается. Значение должно быть кратным значению Hello Interval (Интервал приветствия). Все маршрутизаторы, подключенные к общей сети, должны иметь одинаковое значение для этого параметра. Возможные значения поля: 1-2147483647. По умолчанию это четырехкратное значение Hello Interval (Интервала приветствия).

Retransmit Interval (0-3600) (Интервал повторной передачи (0-3600)) - интервал времени в секундах между повторной передачей объявлений о состоянии канала (LSA) для соседних узлов, принадлежащих интерфейсу. Значение должно быть больше ожидаемой задержки обратной передачи между двумя маршрутизаторами, подключенными к сети. Значение по умолчанию: 5 секунд.

Transmit Delay (0-3600) (Задержка передачи (0-3600)) - приблизительное время (в секундах), необходимое для отправки пакета о состоянии канала для интерфейса. Объявления LSA в пакете обновления имеют свой возраст, которые увеличивается на данное значение перед передачей. Значение по умолчанию: 1 секунда.

Authentication Mode (Режим проверки подлинности) - тип проверки подлинности интерфейса, пароль или ключ MD5, используемые для проверки подлинности сообщений о состоянии канала OSPF.

Authentication Password (Пароль проверки подлинности) - пароль, используемый для проверки сообщений о состоянии канала OSPF. Максимальная длина пароля составляет восемь символов.

Authentication Key-Chain (Цепочка ключей проверки подлинности) - цепочка ключей MD5, используемая для проверки подлинности сообщений о состоянии канала OSPF.

Metric Value (Значение метрики) - метрика для этого типа услуги для интерфейса. Возможные значения поля: 1-65535.

Remove (Удалить) - когда установлен этот флажок, интерфейс OSPF удаляется.

Добавление интерфейса OSPF

1. Откройте страницу **Interface Parameters** (Параметры интерфейса).
2. Нажмите кнопку **Add** (Добавить), чтобы отобразить страницу **Add OSPF Interface** (Добавление OSPF интерфейса).

Рис. 8-15. Добавление интерфейса OSPF

Add OSPF Interface

New OSPF Interface	
Area ID	
Priority (0-255)	1
Admin Status	Enable
Hello Interval (1-65535)	10 (Sec)
Dead Interval (1-2147483647)	40 (Sec)
Retransmit Interval (1-3600)	5 (Sec)
Transmit Delay (1-3600)	1 (Sec)
Authentication Mode	None
Authentication Password	
Authentication Key-Chain	
Metric Value (1-65535)	10

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

Будет добавлен новый интерфейс OSPF для устройства.

Изменение параметров OSPF

1. Откройте страницу **Interface Parameters** (Параметры интерфейса).
2. Выберите интерфейс OSPF, чтобы отобразить параметры полей для записи таблицы.
3. Измените необходимые параметры.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Параметры интерфейса OSPF изменятся и сохранятся на устройстве.

Удаление интерфейса OSPF

1. Откройте страницу **Interface Parameters** (Параметры интерфейса).

2. Нажмите кнопку **Show All** (Показать все), чтобы отобразить таблицу **OSPF Interface Table** (Таблица интерфейса OSPF).
3. Выберите интерфейс OSPF.
4. Установите флажок **Remove** (Удалить).
5. Нажмите кнопку **Apply Changes** (Применить изменения).

Интерфейс OSPF удалится.

Определение интерфейсов OSPF с помощью команд консоли

В следующей таблице приведены команды консоли для определения интерфейсов OSPF.

Таблица 8-11. Команды консоли для интерфейса OSPF

Команда консоли	Описание
<code>ospf</code>	Создает процесс маршрутизации OSPF для интерфейса.
<code>ospf area идентификатор_области</code>	Определяет идентификатор области интерфейса.
<code>ospf enable</code>	Активирует OSPF для интерфейса.
<code>ospf priority значение</code>	Устанавливает приоритет маршрутизатора, который используется при выборе маршрутизатора для сети.
<code>ospf hello-interval секунды</code>	Указывает время между hello-пакетами, отправляемыми программой для интерфейса.
<code>ospf dead-interval секунды</code>	Устанавливает временной интервал, в течение которого hello-пакеты не должны отправляться, прежде чем соседи объявят маршрутизатор отключенным.
<code>ospf retransmit-interval секунды</code>	Определяет временной интервал между повторной передачей объявлений о состоянии канала (LSA) для соседних узлов интерфейса, принадлежащих интерфейсу.
<code>ospf transmit-delay секунды</code>	Устанавливает приблизительное время, необходимое для отправки пакета о состоянии канала для интерфейса.
<code>ospf authentication {text text md5 имя_цепочки}</code>	Включает проверку подлинности для пакетов OSPF и указывает тип проверки подлинности.
<code>clear ip ospf process [интерфейс]</code>	Отменяет повторное распространение в соответствии с маршрутизацией OSPF.
<code>show ip ospf interface [интерфейс]</code>	Отображает данные интерфейса, относящиеся к OSPF.

Далее приведен пример команд консоли.

```
Console(config)# interface ip 1.100.100.100
```

```
Console(config-ip)# ospf
```

```
Console(config-ip)# ospf area 192.168.2.1
```

Console(config-ip)# ospf enable

Console(config-ip)# ospf priority 100

Console(config-ip)# ospf hello-interval 100

Console(config-ip)# ospf dead-interval 100

Console(config-ip)# ospf retransmit-interval 60

Console(config-if)# ospf retransmit-delay 60

Console(config-ip)# ospf authentication text abab

Console(config-ip)# ospf authentication md5 mychain

Console (config-ip)# exit

Console(config)# exit

Console# clear ip ospf process 192.168.3.1

Console# exit

Console# show ip ospf interface 192.168.1.1

IP interface 192.168.1.1/16 is up, OSPF is enabled

Area 0.0.0.0, Router ID 192.77.99.1, Network Type BROADCAST, Cost: 10

Interface has simple password authentication

Transmit Delay is 1 sec, State OTHER, Priority 1

Designated Router id 192.168.1.11, Interface address 192.168.1.11

Backup Designated router id 192.168.1.28, Interface addr 192.168.1.28

Timer intervals configured, Hello 10, Dead 60, Retransmit 5

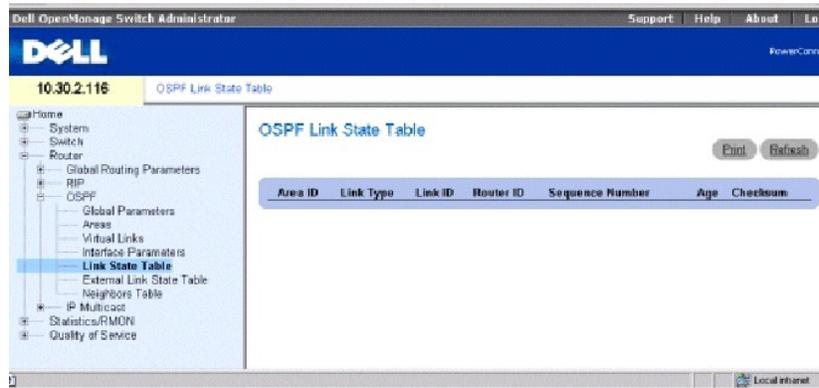
Neighbor Count is 8, Adjacent neighbor count is 2

Adjacent with neighbor 192.168.1.28 (Backup Designated Router)

Просмотр таблицы состояния канала

Страница OSPF Link State Table (Таблица состояний каналов OSPF) содержит данные объявления о состоянии канала для областей, к которым подключено устройство. Выберите Router (Маршрутизатор)→ OSPF→ Link State Table (Таблица состояний канала) на панели дерева.

Рис. 8-16. Таблица состояния каналов OSPF



Area ID (Идентификатор области) - идентификатор области.

Link Type (Тип канала) - показывает тип канала для области.

Link ID (Идентификатор канала) - часть домена маршрутизации, описываемая объявлением. Это либо идентификатор маршрутизатора, либо IP-адрес.

Router ID (Идентификатор маршрутизатора) - исходный маршрутизатор в автономной системе.

Sequence Number (Номер по порядку) - порядковый номер канала. Порядковый номер определяет старые и дублирующиеся объявления о состоянии канала. Чем больше порядковый номер, тем позднее отправлено объявление.

Age (Срок действия) - указывает на срок действия объявления о состоянии канала в секундах.

Checksum (Контрольная сумма) - контрольная сумма полных данных объявления, исключая значение **Age** (Срок действия).

Просмотр таблицы состояния каналов OSPF с помощью команд консоли

В следующей таблице приведены команды консоли для просмотра таблицы OSPF Link State Table (Таблица состояния каналов OSPF).

Таблица 8-12. Каналы консоли для просмотра состояния каналов OSPF

--	--

Команда консоли	Описание
show ip ospf [идентификатор_области] database	Отображает информационные списки, относящиеся к базе данных OSPF для заданного маршрутизатора.

Далее приведен пример команд консоли.

```
console> show ip ospf database
```

```
OSPF Router with ID 200.1.1.11
```

```
Router Link States(Area 0)
```

```
Link ID ADV Router Age Seq# Checksum Link count
```

```
200.1.1.8 200.1.1.8 1381 0x8000010D 0xEF60 2
```

```
200.1.1.11 200.1.1.11 1460 0x800002FE 0xEB3D 4
```

```
200.1.1.12 200.1.1.12 2027 0x80000090 0x875D 3
```

```
200.1.1.27 200.1.1.27 1323 0x800001D6 0x12CC 3
```

```
Net Link States(Area 0)
```

```
Link ID ADV Router Age Seq# Checksum
```

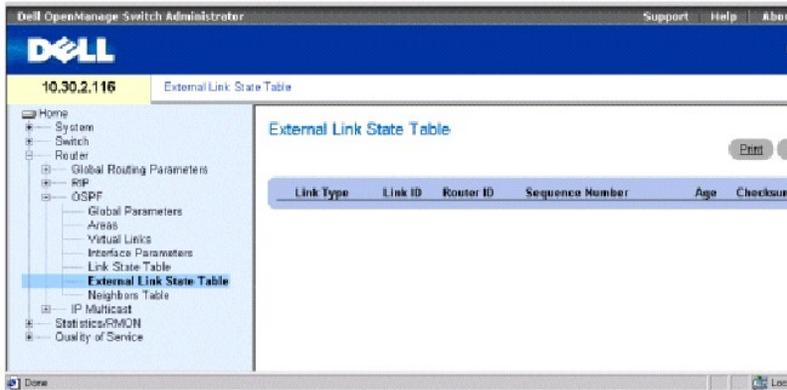
```
140.1.1.27 200.1.1.27 1323 0x8000005B 0xA8EE
```

```
141.1.1.11 200.1.1.11 1461 0x8000005B 0x7AC
```

Просмотр таблицы состояния внешних каналов

Таблица External Link State (Состояние внешних каналов) содержит данные объявления о состоянии каналов. Данные таблицы состояния внешних каналов получает от источников, отличных от маршрутов OSPF. Чтобы открыть страницу External Link State (Состояние внешних каналов), выберите Router (Маршрутизатор) → OSPF → External Link State Table (Таблица состояния внешних каналов) на панели дерева.

Рис. 8-17. Таблица состояния внешних каналов



Link Type (Тип канала) - тип внешнего канала. Каждое объявление о состоянии канала имеет определенный формат. Это поле всегда является внешним каналом.

Link ID (Идентификатор канала) - часть домена маршрутизации, описываемая объявлением. Это либо идентификатор маршрутизатора, либо IP-адрес.

Router ID (Идентификатор маршрутизатора) - исходный маршрутизатор в автономной системе.

Sequence Number (Номер по порядку) - порядковый номер внешнего канала. Порядковый номер определяет старые и дублирующиеся объявления о состоянии канала. Чем больше порядковый номер, тем позднее отправлено объявление.

Age (Срок действия) - показывает срок действия объявления о состоянии канала в секундах.

Checksum (Контрольная сумма) - контрольная сумма полных данных объявления, исключая значение **Age** (Срок действия).

Просмотр таблицы состояния внешних каналов OSPF с помощью команд консоли

В следующей таблице приведены команды консоли для просмотра таблицы внешних маршрутов OSPF.

Таблица 8-13. Команды консоли для просмотра таблицы внешних маршрутов OSPF

Команда консоли	Описание
<code>show ip ospf [идентификатор_области] database [external] [идентификатор_состояния_канала]</code>	Отображает базу данных, относящуюся к OSPF, для заданного маршрутизатора.

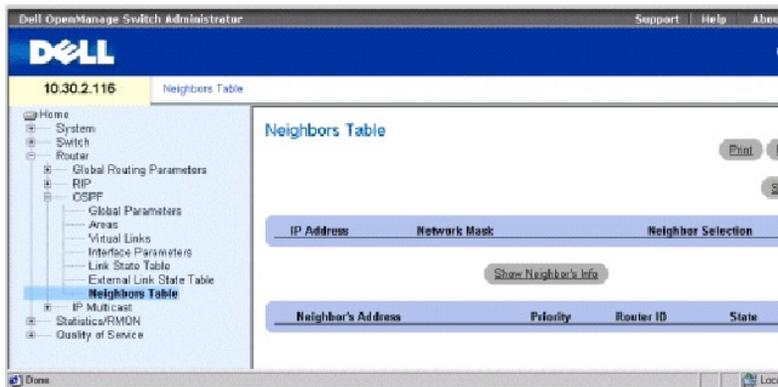
Далее приведен пример команд консоли.

```
Console> show ip ospf database
```

Просмотр таблицы соседей OSPF

В таблице соседей OSPF описаны все соседи в местонахождении маршрутизатора субъекта. Чтобы открыть страницу **Neighbor Table** (Таблица соседей), выберите **Router** (Маршрутизатор) → **OSPF Neighbors Table** (Таблица соседей) на панели дерева.

Рис. 8-18. Таблица соседей



IP Address (IP-адрес) - IP-адрес, который использует этот сосед в своем IP-адресе источника.

Network Mask (Маска сети) - маска сети соседнего интерфейса.

Neighbor Selection (Выбор соседей) - указывает, какие необходимо отображать данные о соседях устройства.

Neighbor's Address (Адрес соседа) - IP-адрес соседа.

Priority (Приоритет) - приоритет соседа.

Router ID (Идентификатор маршрутизатора) - идентификатор маршрутизатора соседа.

State (Состояние) - текущее состояние соседа.

Отображение списка соседей

1. Откройте страницу **OSPF Neighbors Table** (Таблица соседей OSPF).
2. В столбце **Neighbor Selection** (Выбор соседей) нажмите кнопку выбора соседа, данные которого требуется просмотреть.
3. Выберите **Show Neighbor's Info** (Показать данные соседа).

Данные соседа отобразятся внизу страницы.

Отображение таблицы всех соседей

1. Откройте страницу **Neighbors Table** (Таблица соседей).
2. Нажмите кнопку **Show All** (Показать все), чтобы отобразить таблицу **All Neighbors Table** (Таблица всех соседей).

Просмотр данных соседей OSPF с помощью команд консоли

В следующей таблице приведены команды консоли для просмотра таблицы данных соседей OSPF.

Таблица 8-14. Команды консоли для просмотра соседей OSPF

Команда консоли	Описание
show ip ospf neighbor [<i>интерфейс</i>]	Отображает данные о соседях OSPF для каждого интерфейса.

Далее приведен пример команд консоли.

```
Console> show ip ospf neighbor
```

```
ID Pri State Address IP-interface
```

```
-----
```

```
192.168.1.11 1 FULL /DR 192.168.1.11 192.168.1.1
```

```
192.168.1.12 2 FULL /DROTHER 192.168.1.12 192.168.1.1
```

```
192.168.2.11 1 FULL /DR 192.16 8.2.11 192.168.2.1
```

```
192.168.2.12 2 FULL /DROTHER 192.168.2.12 192.168.2.1
```

```
Console> show ip ospf neighbor 192.168.1.1
```

```
Neighbor 192.168.1.11, Address 192.168.1.11
```

```
In the area 0.0.0.0
```

```
Neighbor priority is 1, State is FULL
```

```
Options 2
```

```
Neighbor 192.168.1.12, Address 192.168.1.12
```

```
In the area 0.0.0.0
```

```
Neighbor priority is 2, State is FULL
```

```
Options 2
```

Настройка многоадресной маршрутизации IP

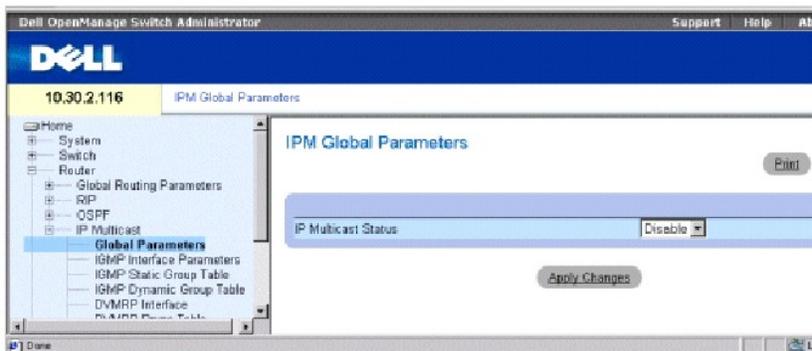
Многоадресная маршрутизация максимально увеличивает ресурсы сети. Один хост посылает данные группе узлов (а не отдельному узлу) внутри IP-сети с использованием IP-адреса многоадресной группы. Многоадресная маршрутизация IP реализована в PowerConnect 6024/6024F с использованием следующих протоколов:

1. **Internet Group Member Protocol (IGMP)** (Протокол IGMP) - предоставляет метод для обнаружения, в котором заинтересованы клиенты во время приема определенных передач.
1. **Distance Vector Multicast Routing Protocol (DVMRP)** (Протокол дистанционно-векторной многоадресной маршрутизации (DVMRP)) - позволяет маршрутизаторам определять дерево передачи и копировать пакеты внутри дерева маршрутизации.

Определение общих параметров IPM

Включение многоадресной маршрутизации IP выполняется на странице **IPM Global Parameters** (Общие параметры IPM). Чтобы открыть страницу **IPM Global Parameters** (Общие параметры IPM), выберите **Router** (Маршрутизатор)→ **IP Multicast** (Многоадресная передача IP)→ **Global Parameters** (Общие параметры) на панели дерева.

Рис. 8-19. Общие параметры IPM



IP Multicast Status (Состояние IP многоадресной передачи) - включает или отключает маршрутизацию IPM на устройстве.

Включение маршрутизации IPM на устройстве

1. Откройте страницу **IPM Global Parameters** (Общие параметры RIP).
2. Выберите **Enable** (Включено) в поле **IPM Multicast Status** (Состояние многоадресного IP).
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Многоадресная маршрутизация IP включена на устройстве.

Включение многоадресной маршрутизации с помощью команд консоли

В следующей таблице приведены команды консоли для включения многоадресной маршрутизации.

Таблица 8-15. Команды консоли для многоадресной маршрутизации

Команда консоли	Описание
ip multicast-routing	Включает многоадресную маршрутизацию IP.

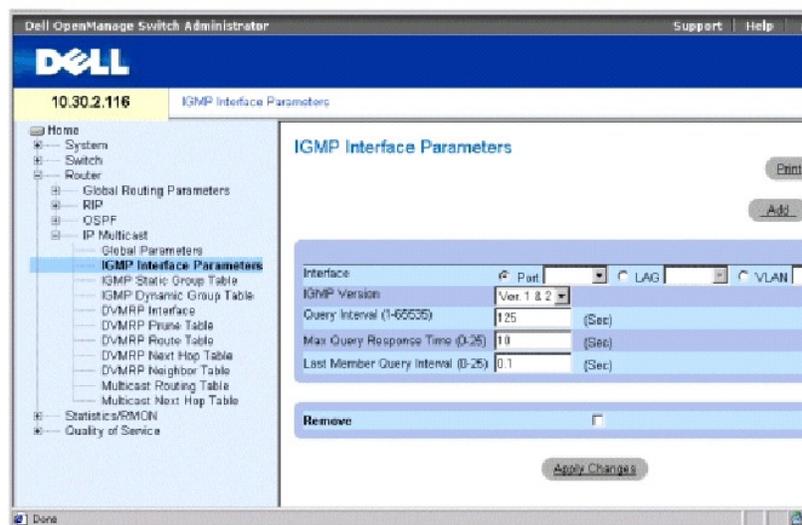
Далее приведен пример команд консоли.

```
Console (config)# ip multicast-routing
```

Определение параметров интерфейса IGMP

Протокол IGMP (Internet Group Membership Protocol) устанавливает принадлежность узла группе многоадресной передачи. Протокол IGMP позволяет узлу уведомлять маршрутизаторы о том, что они могут получать многоадресные пакеты, адресованные определенной многоадресной группе. Чтобы открыть страницу **IGMP Interface Parameters** (Параметры интерфейса IGMP), выберите **Router** (Маршрутизатор) → **IP Multicast** (Многоадресная передача IP) → **IGMP Interface Parameters** (Параметры интерфейса IGMP) на панели дерева.

Рис. 8-20. Параметры интерфейса IGMP



Interface (Интерфейс) - содержит список IP-адресов интерфейсов, для которых включен протокол IGMP.

IGMP Version (Версия IGMP) - текущая программного обеспечения IGMP. Значение по умолчанию: Ver. 1&2.

Query Interval (1-65535) (Интервал запроса (1-65535)) - время в секундах между передачей сообщений запроса. Можно настроить число сообщений IGMP передаваемых в подсети, изменяя значение поля Query Interval (Интервал запроса). Чем больше значение, тем реже отправляются сообщения IGMP. Значение по умолчанию: 125 секунд.

Max Query Response Time (0-25) (Максимальное время ответа на запрос (0-25)) - максимальное время ответа на запросы IGMP. Время ответа определяет количество трафика для каждой подсети. Изменение времени ответа влияет на объем сетевого трафика. Чем больше значение, тем больше проходит времени между ответами узлов. Значение по умолчанию: 10 секунд.

Last Member Query Interval (0-25) (Интервал запроса последнего члена (0-25)) - изменяет задержку перед выходом для сети. Чем меньше значение, тем меньше времени требуется для определения потери последнего члена группы. Значение по умолчанию: 0.1.

Remove (Удалить) - когда установлен этот флажок, удаляется интерфейс IGMP.

Добавление интерфейса IGMP

1. Откройте страницу **IGMP Interface Parameters** (Параметры интерфейса IGMP).
2. Нажмите кнопку **Add** (Добавить), чтобы отобразить страницу **Add an IGMP Interface** (Добавить интерфейс IGMP).
3. Выберите интерфейс в раскрывающемся меню **New Interface** (Новый интерфейс).
4. Заполните поля на этой странице.
5. Нажмите кнопку **Apply Changes** (Применить изменения).

Будет добавлен новый интерфейс IGMP для устройства.

Изменение интерфейса IGMP

1. Откройте страницу **IGMP Interface Parameters** (Параметры интерфейса IGMP).
2. Выберите интерфейс, который необходимо изменить.
3. Измените необходимые поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Параметры интерфейса IGMP изменятся и сохранятся на устройстве.

Удаление интерфейса IGMP

1. Откройте страницу **IGMP Interface Parameters** (Параметры интерфейса IGMP).
2. Нажмите кнопку **Show All** (Показать все), чтобы отобразить страницу **IGMP Interface Table** (Таблица интерфейса IGMP).
3. Выберите интерфейс IGMP и установите флажок **Remove** (Удалить).
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Интерфейс IGMP будет удален.

Настройка параметров интерфейса IGMP с помощью команд консоли

В следующей таблице приведены команды консоли для настройки параметров интерфейса IGMP.

Таблица 8-16. Команды консоли для настройки параметров интерфейса IGMP

Команда консоли	Описание
<code>ip igmp</code>	Создает IGMP для интерфейса.
<code>ip igmp query-interval секунды</code>	Настраивает частоту, с которой программное обеспечение отправляет узлу IGMP сообщения с запросом.
<code>ip igmp query-max-response-time секунды [десять_се кунды]</code>	Настраивает максимальное время ответа на запросы IGMP.
<code>ip igmp last-member-query-interval секунды [десять_се кунды]</code>	Настраивает частоту, с которой маршрутизатор отправляет IGMP сообщения с запросом узла, относящиеся к группе.
<code>show ip igmp interface [ethernet номер_интерфейса vlan</code>	Отображает данные интерфейса, относящиеся к IGMP.

идентификатор_vlan / но мер пор та-канала]

Далее приведен пример команд консоли.

```
Console (config)# interface ethernet g1
```

```
Console (config-if)# ip igmp
```

```
Console (config-if)# ip igmp query-interval 60
```

```
Console (config-if)# ip igmp query-max-response-time 20
```

```
Console (config-if)# ip igmp last-member-query-interval 200
```

```
Console(config-if)# exit
```

```
Console(config)# exit
```

```
Console# disable
```

```
Console> show ip igmp interface
```

```
Interface Version Query Last Max Querier Interval Member response router
```

```
[sec] [mSec] [Sec]
```

```
-----
```

```
eth g1 2 60 1000 10 198.92.37.33
```

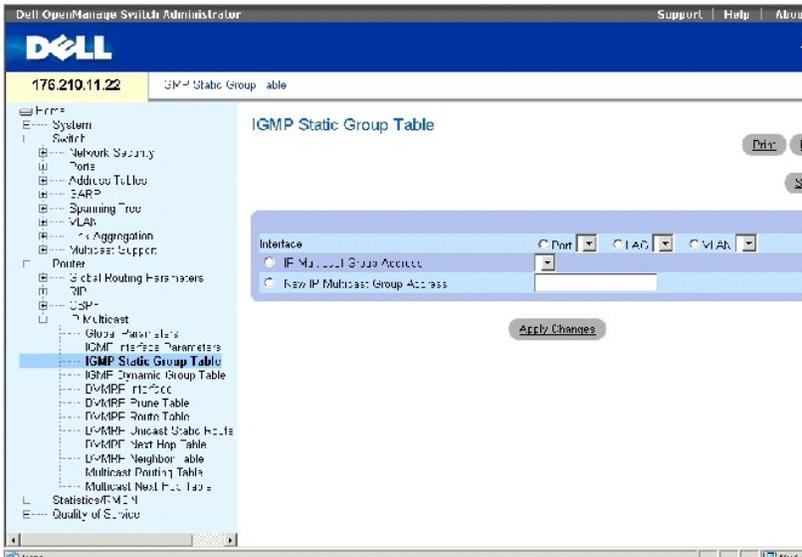
```
eth g2 60 1000 10 198.92.36.131
```

Определение статических групп интерфейсов IGMP

Таблица **IGMP Static Group Table** (Таблица статической группы IGMP) включает статическое определение группы IGMP для определенного интерфейса.

Чтобы открыть страницу **IGMP Static Group Table** (Таблица статической группы IGMP), выберите **Router** (Маршрутизатор) → **IP Multicast** (Многоадресная передача IP) → **IGMP Static Group Table** (Таблица статической группы IGMP) на панели дерева.

Рис. 8-21. Таблица статической группы IGMP



Interface (Интерфейс) - определенный порт VLAN или группа LAG, для которых назначена определенная многоадресная группа.

IP Multicast Group Address (IP-адрес многоадресной группы) - IP-адрес многоадресной группы, назначенный для интерфейса.

New IP Multicast Group Address (Новый IP-адрес многоадресной группы) - новый IP-адрес многоадресной группы, назначенный для интерфейса.

Назначение интерфейса для многоадресной группы

1. Откройте **IGMP Static Group Table** (Таблица статической группы IGMP).
2. Выберите интерфейс в поле **Interface** (Интерфейс).
3. Выберите IP-адрес в поле **Multicast Group Address** (Адрес многоадресной группы) или определите новый адрес многоадресной группы в поле **New Multicast Group Address** (Новый адрес многоадресной группы).
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Отображение таблицы статического интерфейса группы

1. Откройте **IGMP Static Group Table** (Таблица статической группы IGMP).
2. Нажмите кнопку **Show All** (Показать все), чтобы отобразить **Static Interface Grouping Table** (Таблица статической группировки интерфейсов).

На странице находятся следующие поля:

- 1 **Interface** (Интерфейс) - IP-адрес группы многоадресной передачи, к которой принадлежит порт.
- 1 **IP Multicast Group** (Группа многоадресной передачи IP) - группа многоадресной передачи IP, к которой принадлежит интерфейс.
- 1 **Group Up Time** (Время группировки) - показывает в делениях время, прошедшее после создания записи. Время указывается в формате «часы-минуты-секунды».
- 1 **Last Reporter** (Последний генератор) - последний элемент, добавляемый в группу многоадресной передачи IP. Если в группу многоадресной передачи IP не добавлено элементов, значение будет 0.0.0.0.
- 1 **Remove** (Удалить) - когда установлен этот флажок, интерфейс IGMP удаляется.

Настройка статического интерфейса группы с помощью команд консоли

В следующей таблице приведены команды консоли для статической группировки интерфейсов.

Таблица 8-17. Команды консоли для настройки статического интерфейса группы

Команда консоли	Описание
<code>ip igmp static-group адрес_ группы</code>	Настраивает маршрутизатор, который необходимо статически добавить в указанную группу для интерфейса.

Далее приведен пример команд консоли.

```
Console (config)# interface ethernet g5
```

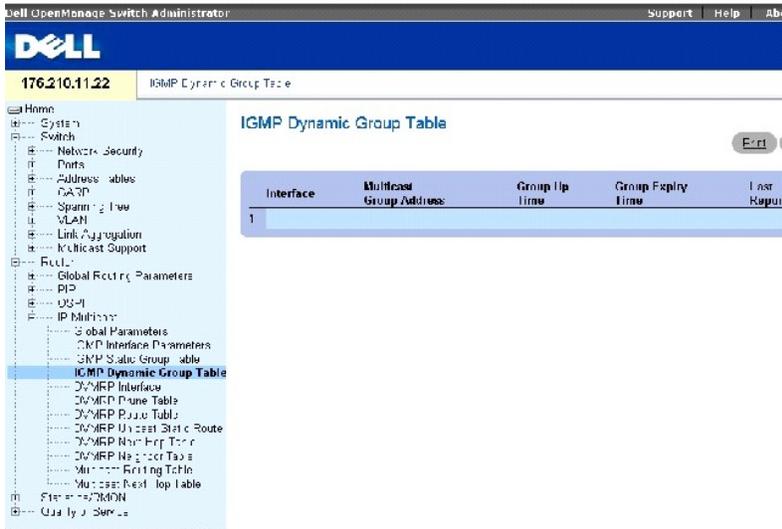
```
Console (config-if)# ip igmp static-group 192.168.4.1
```

Просмотр таблицы динамической группы IGMP

Таблица **IGMP Dynamic Group Table** (Таблица динамической группы IGMP) отображает данные IGMP относительно каждой группы многоадресной передачи IP, элементы которой были динамически назначены для интерфейса на физическом порту.

Чтобы открыть таблицу **IGMP Dynamic Group Table** (Таблица динамической группы IGMP), выберите **Router** (Маршрутизатор) → **IP Multicast** (Многоадресная передача IP) → **IGMP Dynamic Group Table** (Таблица динамической группы IGMP) на панели дерева.

Рис. 8-22. Таблица динамической группы IGMP



Interface (Интерфейс) - указывает интерфейс, принадлежащий группе многоадресной передачи IP.

Multicast Group Address (Адрес группы многоадресной передачи) - адрес группы многоадресной передачи IGMP.

Group Up Time (Время группировки) - показывает в делениях время, прошедшее после создания записи. Время указывается в формате «часы-минуты-секунды».

Group Expiry Time (Срок действия группы) - период времени, по истечении которого динамическая запись считается устаревшей. Время указывается в

формате «часы-минуты-секунды».

Last Reporter (Последний генератор) - последний элемент, добавляемый в группу многоадресной передачи IP. Если в группу многоадресной передачи IP не добавлено элементов, значение будет 0.0.0.0.

Просмотр групп IGMP с помощью команд консоли

В следующей таблице приведены команды консоли для просмотра групп IGMP.

Таблица 8-18. Команды консоли для просмотра групп IGMP

Команда консоли	Описание
<code>show ip igmp groups [ip-адрес группы] [ethernet номер_интер_фейса vlan идентификат op_vlan / номер порт а-канала]</code>	Отображает группу многоадресной передачи с получателями, которые напрямую подключены к маршрутизатору и которые были определены по протоколу IGMP (Internet Group Membership Protocol).

Далее приведен пример команд консоли:

```
Console> show ip igmp groups
```

```
Group Address Interface Uptime Expires Last Reporter
```

```
-----
```

```
239.255.255.254 eth g1 1w0d 00:02:19 172.21.200.159
```

```
224.0.1.40 eth g3 1w0d 00:02:15 172.21.200.1
```

```
224.0.1.40 eth g3 1w0d 00:02:1 static
```

```
224.0.1.1 eth g1 1w0d 00:02:11 172.21.200.11
```

```
224.9.9.2 eth g1 1w0d 00:02:17 172.21.200.155
```

```
232.1.1.1 eth g1 5d21h 00:02:11 172.21.200.206
```

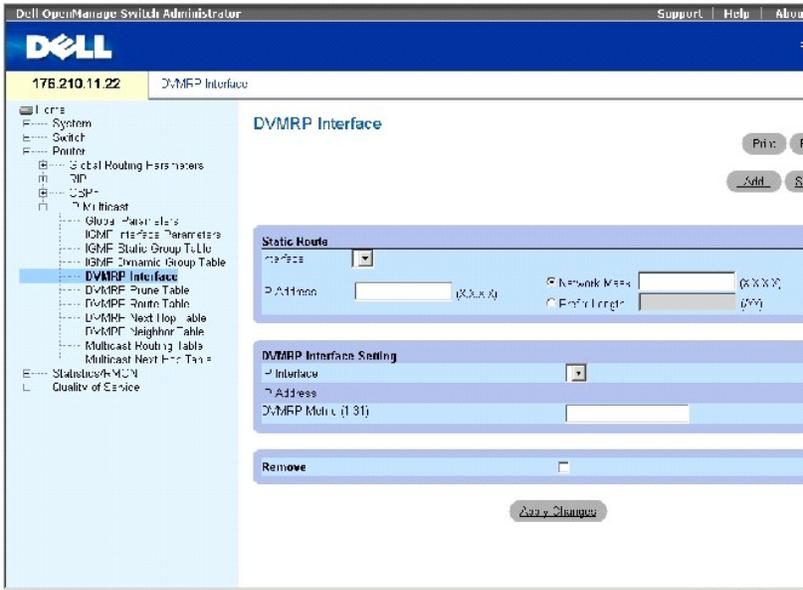
Настройка интерфейсов DVMRP

Протокол DVMRP (Distance Vector Multicast Routing Protocol) использует алгоритм многоадресной пересылки на обратном пути (RPF) для создания деревьев многоадресной доставки на основе источников. DVMRP - это протокол проверки RPF основанный на данных маршрутизации DVMRP. Данные маршрутизации собираются во время маршрутизации обмена данными.

Страница [DVMRP Interface](#) (Интерфейс DVMRP) содержит информацию о настройке интерфейса DVMRP.

Чтобы открыть страницу [DVMRP Interface](#) (Интерфейс DVMRP), выберите **Router** (Маршрутизатор) → **IP Multicast** (Многоадресная передача IP) → **DVMRP Interface** (Интерфейс DVMRP) на панели дерева.

Рис. 8-23. Интерфейс DVMRP



Страница [DVMRP Interface](#) (Интерфейс DVMRP) содержит следующие поля.

STATIC ROUTE (СТАТИЧНЫЙ МАРШРУТ)

Interface (Интерфейс) - номер интерфейса, для которого включен протокол DVMRP.

IP Address (X.X.X.X) (IP-адрес (X.X.X.X)) - указывает IP-адрес источника, для которого включен протокол DVMRP.

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

Prefix Length /XX (Длина префикса /XX) - указывает число бит, образующих префикс исходного IP-адреса или сетевую маску исходного IP-адреса.

DVMRP INTERFACE SETTING (НАСТРОЙКА ИНТЕРФЕЙСА DVMRP)

IP Interface (Интерфейс) - номер интерфейса, для которого включен протокол DVMRP.

IP Address (IP-адрес) - указывает IP-адрес источника, для которого включен протокол DVMRP.

DVMRP Metric (1-31) (Метрика DVMRP (1-31)) - показывает расстояние, используемое для расчета вектора расстояния. Метрика DVMRP - это расстояние интерфейса между маршрутизатором, генерирующим отчет, и исходной сетью. Значение по умолчанию: 1.

Remove (Удалить) - когда установлен этот флажок, интерфейс DVMRP удаляется.

Добавление нового интерфейса DVMRP

1. Откройте страницу [DVMRP Interface](#) (Интерфейс DVMRP).
2. Щелкните **Add** (Добавить), чтобы отобразить страницу **Add a DVMRP Interface** (Добавление DVMRP интерфейса).
3. Определите номер интерфейса и метрику DVMRP.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Интерфейс DVMRP будет добавлен в список **IP Interface (IP-интерфейсов)**, а устройство обновлено.

Изменение интерфейса DVMRP

1. Откройте страницу [DVMRP Interface](#) (Интерфейс DVMRP).
2. Выберите интерфейс в списке **IP Interface (IP-интерфейс)**.
3. Измените необходимые поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Интерфейс DVMRP будет добавлен в список **DVMRP Interface List** (Список интерфейсов DVMRP), а устройство обновлено.

Удаление интерфейса DVMRP

1. Откройте страницу [DVMRP Interface](#) (Интерфейс DVMRP).
2. Выберите интерфейс в списке **IP Interface (IP-интерфейс)**.
3. Установите флажок **Remove** (Удалить).
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Измененный интерфейс DVMRP будет удален из списка **IP Interface (IP-интерфейсов)**, а устройство удалено.

Настройка интерфейсов DVMRP с помощью команд консоли

В следующей таблице приведены команды консоли для настройки и просмотра интерфейсов DVMRP.

Таблица 8-19. Команды консоли для DVMRP

Команда консоли	Описание
<code>ip dvmrp</code>	Включает DVMRP для интерфейса.
<code>no ip dvmrp</code>	Отключает DVMRP для интерфейса.
<code>ip dvmrp metric метрика</code>	Настраивает метрику интерфейса для DVMRP. Метрика может иметь значение от 1 до 31.
<code>no ip dvmrp metric</code>	Отключает метрику интерфейса для DVMRP.
<code>show ip dvmrp interface [ethernet номер_интерфейса vlan идентификатор_vlan port-channel номер]</code>	Отображает таблицу интерфейса.

Далее приведен пример команды консоли:

```
Console (config-if)# interface ethernet g5
```

```
Console (config-if)# ip dvmrp
```

```
Console (config-if)# ip dvmrp metric 15
```

```
Console(config-if)# exit
```

```
Console(config)# exit
```

```
Console> show ip dvmrp interface
```

```
Multicast routing enabled.
```

```
Multicast routing protocol is DVMRP.
```

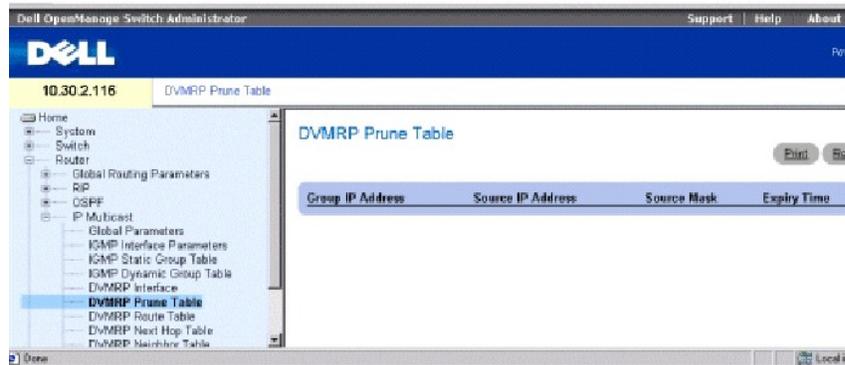
```
Interface IP address Metric RCV Bad RCV Bad Sent Packets Routes Routes
```

```
eth g1 172.16.1.1 10 0 12
```

Таблица усе­че­ния DVMRP

На странице DVMRP Prune Table (Таблица усе­че­ния DVMRP) показано состояние усе­че­ния восходящего потока маршрутизаторов. Чтобы открыть страницу DVMRP Prune Table (Таблица усе­че­ния DVMRP), выберите Router (Маршрутизатор) → IP Multicast (Многоадресная передача IP) → DVMRP Prune Table (Таблица усе­че­ния DVMRP) на панели дерева.

Рис. 8-24. Таблица усе­че­ния DVMRP



Group IP Address (IP-адрес группы) - IP-адрес группы усе­че­ния.

Source IP Address (IP-адрес источника) - IP-адрес источника для усечения.

Source Mask (Маска источника) - IP-маска источника для усечения.

Expiry Time (Время истечения срока) - оставшееся время, прежде чем восходящий поток будет усечен.

Просмотр таблицы усечения DVMRP с помощью команд консоли

В следующей таблице приведены команды консоли для просмотра таблицы усечения.

Таблица 8-20. Команды консоли таблицы DVRMP

Команда консоли	Описание
<code>show ip dvmrp prune [group адрес_группы] [адрес_источника]</code>	Отображает таблицу.

Далее приведен пример команды консоли:

```
Console> show ip dvmrp prune
```

```
Group Source Expiry Time
```

```
-----
```

```
224.192.78.88 171.68.0.0/16 00:02:52
```

```
224.192.78.89 171.68.0.0/16 00:08:52
```

Таблица маршрутизации DVMRP

Страница **DVMRP Route Table** (Таблица маршрутизации DVMRP) содержит сведения о маршрутах, определенных с помощью обмена данными маршрутизации DVMRP. Чтобы открыть страницу **DVMRP Route Table** (Таблица маршрутизации DVMRP), выберите **Router** (Маршрутизатор)→ **IP Multicast** (Многоадресная передача IP)→ **DVMRP Route Table** (Таблица маршрутизации DVMRP) на панели дерева.

Рис. 8-25. Таблица маршрутизации DVMRP



Source IP Address (IP-адрес источника) - IP-адрес источника информации многоадресной маршрутизации.

Source Mask (Маска источника) - сетевая маска IP-адреса источника.

Upstream Neighbor (Сосед восходящего потока) - IP-адрес соседа RPF восходящего потока, с которого принимаются датаграммы IP источника.

Upstream Interface (Интерфейс восходящего потока) - IP-адрес интерфейса восходящего потока.

Metric (Метрика) - расстояние до исходной подсети, выраженное в числе узлов.

Expiry Time (Время истечения срока) - время до истечения срока хранения записи.

Up Time (Время работы) - время, прошедшее с момента распознавания маршрутизатора другим маршрутизатором.

Просмотр таблицы маршрутизации DVMRP с помощью команд консоли

В следующей таблице приведены команды консоли для просмотра таблицы маршрутизации DVMRP.

Таблица 8-21. Команды консоли для таблицы маршрутизации DVMRP

Команда консоли	Описание
<code>show ip dvmrp route [ip-адрес] [ip-адрес]</code>	Отображает таблицу маршрутизации DVMRP.

Далее приведен пример команды консоли:

```
Console> show ip dvmrp route
```

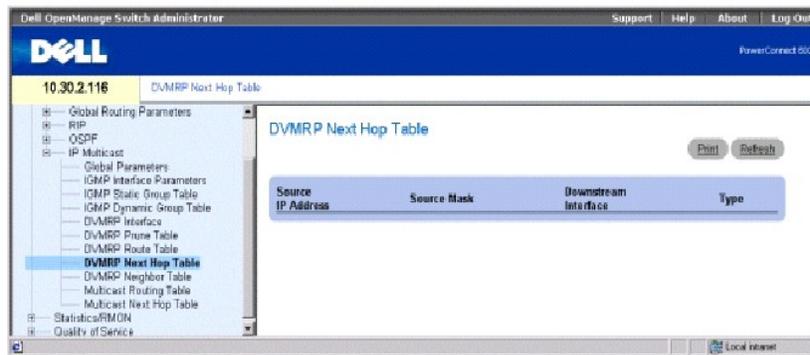
```
Source Neighbor Interface Metric Expiry Up Time Time
```

171.68.0.0/16 192.168.1.28/16 eth g116 11016 100:02:5216 107:55:50

Таблица ближайших узлов DVMRP

Страница **DVMRP Next Hop Table** (Таблица ближайших узлов DVMRP) содержит сведения относительно следующего узла для исходящего интерфейса для пакетов многоадресной передачи IP. Чтобы открыть страницу **DVMRP Next Hop Table** (Таблица ближайших узлов DVMRP), выберите **Router** (Маршрутизатор) → **IP Multicast** (Многоадресная передача IP) → **DVMRP Next Hop Table** (Таблица ближайших узлов DVMRP) на панели дерева.

Рис. 8-26. Таблица ближайших узлов DVMRP



Source IP Address (IP-адреса источника) - IP-адрес источника для следующего узла исходящего интерфейса.

Source Mask (Маска источника) - маска источника для следующего узла исходящего интерфейса.

Downstream Interface (Интерфейс нисходящего потока) - исходящий интерфейс ближайшего узла.

Type (Тип) - указывает тип ближайшего узла. Возможные значения:

Branch (Ветвь) - указывает, что имеется еще один узел после этого узла.

Leaf (Лист) - указывает, что это последний узел маршрута.

Просмотр таблицы ближайших узлов DVMRP с помощью команд консоли

В следующей таблице приведены команды консоли для просмотра таблицы ближайших узлов DVMRP.

Таблица 8-22. Команды консоли для просмотра таблицы ближайших узлов DVMRP

Команда консоли	Описание
<code>show ip dvmrp next-hop [ethernet номер_интерфейса vlan идентификатор_vlan номер порта-</code>	Отображает таблицу ближайших узлов DVMRP.

Далее приведен пример команды консоли:

```
Console> show ip dvmrp next-hop
```

```
Source Interface Hop Type
```

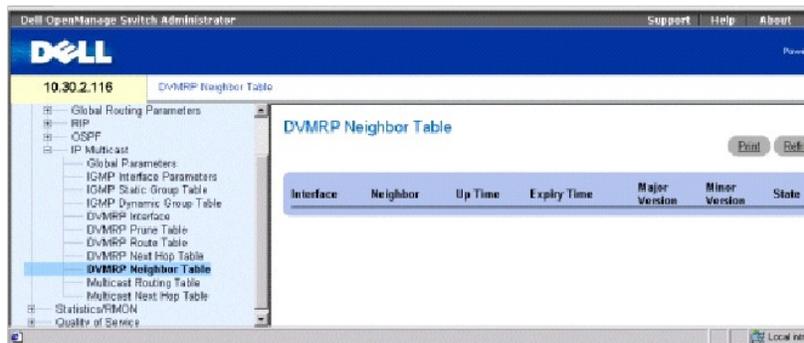
```
-----
```

```
198.92.37.100/32 eth g2 Leaf
```

Таблица соседей DVMRP

Страница **DVMRP Neighbor Table** (Таблица соседей DVMRP) содержит сведения об интерфейсах соседних портов. Соседи DVMRP обнаруживаются с помощью сообщений DVMRP. Чтобы открыть страницу **DVMRP Neighbor Table** (Таблица соседей DVMRP), выберите **Router** (Маршрутизатор) → **IP Multicast** (Многоадресная передача IP) → **DVMRP Neighbor Table** (Таблица соседей DVMRP) на панели дерева.

Рис. 8-27. Таблица соседей DVMRP



Interface (Интерфейс) - номер интерфейса, для которого включен протокол DVMRP.

Neighbor (Сосед) - IP-адрес соседнего интерфейса.

Up Time (Время работы) - время, прошедшее с того момента, когда соседний интерфейс стал соседом.

Expiry Time (Время истечения срока) - показывает минимальное время до завершения работы интерфейса.

Major Version (Основная версия) - номер основной версии соседнего маршрутизатора.

Minor Version (Младшая версия) - номер младшей версии соседнего маршрутизатора.

State (Состояние) - состояние соседнего устройства.

Просмотр таблицы соседей DVMRP с помощью команд консоли

В следующей таблице приведены команды консоли для просмотра таблицы соседей DVMRP.

Таблица 8-23. Команды консоли для просмотра таблицы соседей DVMRP

Команда консоли	Описание
<code>show ip dvmrp neighbor [ethernet номер_интерфейса vlan идентификатор_vlan номер порта- канала]</code>	Отображает таблицу соседей DVMRP.

Далее приведен пример команды консоли:

```
Console> show ip dvmrp neighbor ethernet g1
```

```
Interface Neighbor Up Expiry Version Capabilities RCV Bad State Time Time Routes Routes
```

```
-----
```

```
eth g1 192.168.1.28 2 0:20:00 0:02:55 3.255 L,P,G,M 11 0 Active
```

```
eth g1 192.168.1.10 2 0:20:00 0:02:55 3.255 L,P,G,M 18 0 Active
```

```
eth g2 192.168.1.28 2 0:20:00 0:02:55 3.255 L,P,G,M 11 0 Active
```

```
eth g2 192.168.1.89 2 0:20:00 0:02:55 3.255 L,P,G,M 18 0 Active
```

Просмотр таблицы многоадресной маршрутизации IP

Таблица **IP Multicast (IPM) Routing Table** (Таблица маршрутизации многоадресной передачи IP) содержит сведения о маршрутизации многоадресной передачи IP-пакетов от определенного источника до группы многоадресной передачи IP, известной маршрутизатору многоадресной передачи IP.

Чтобы открыть страницу **IP Multicast (IPM) Routing Table** (Таблица маршрутизации многоадресной передачи IP), выберите **Router** (Маршрутизатор) → **IP Multicast** (Многоадресная передача IP) → **Multicast Routing Table** (Таблица маршрутизации многоадресной передачи) на панели дерева.

Рис. 8-28. Таблица маршрутизации многоадресной передачи IP (IPM)

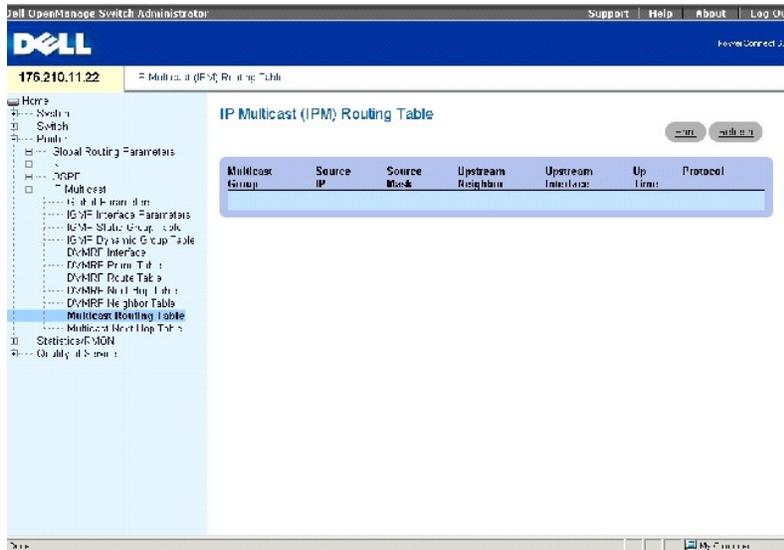


Таблица [IP Multicast \(IPM\) Routing Table](#) (Таблица маршрутизации многоадресной передачи IP (IPM)) содержит следующие поля.

Multicast Group (Группа многоадресной передачи) - IP-адрес группы многоадресной передачи.

Source IP (IP-адрес источника) - IP-адрес устройства источника, для которого назначены данные многоадресной передачи.

Source Mask (Маска источника) - маска всего IP-адреса источника или его части.

Upstream Neighbor (Сосед восходящего потока) - IP-адрес следующего устройства восходящего потока, с которого принимаются пакеты на IP-адрес.

Upstream Interface (Интерфейс восходящего потока) - номер порта, на который передаются и принимаются пакеты многоадресной передачи.

Up Time (Время работы) - показывает время, прошедшее с момента получения маршрутизатором данных многоадресной передачи.

Protocol (Протокол) - определяет тип протокола, используемого для определения данных многоадресной передачи. Для этого проекта возможно только значение **DVMRP**, которое показывает, что для определения данных многоадресной передачи использовался протокол дистанционно-векторной многоадресной маршрутизации.

Отображение таблицы многоадресной маршрутизации IP с помощью команд консоли

В следующей таблице приведены команды консоли для просмотра таблицы многоадресной маршрутизации IP.

Таблица 8-24. Команды консоли для таблицы многоадресной маршрутизации IP

Команда консоли	Описание
<code>show ip mroute [group адрес_группы] [source адрес_источника] [ethernet номер_интерфейса]</code>	Отображает содержимое таблицы многоадресной маршрутизации IP.

```
vlan идентификатор_vlan | номер_порта канала
```

Далее приведен пример команд консоли.

```
Console> show ip mroute
```

```
Group Source Upstream Interface Up Time Expiry Time Owner
```

```
-----  
  
224.0.255.1 198.92.37.100/32 10.20.37.33 eth g1 20:20:00 0:02:55 dvmrp  
  
224.0.255.1 199.92.37.100/32 10.20.37.33 eth g1 1d:4h:20m 0:02:55 dvmrp  
  
224.1.255.1 198.92.37.100/32 10.20.37.33 eth g1 21:20:00 0:02:55 dvmrp  
  
224.1.255.1 199.92.37.100/32 10.20.37.33 eth g1 1d:5h:20m 0:02:55 dvmrp  
  
224.8.255.1 179.82.17.200/32 10.20.37.33 vlan 127 1w:1d:2h 0:02:55 dvmrp  
  
224.8.255.1 179.82.17.200/32 10.20.37.33 vlan 128 3m:2w:2d 0:02:55 dvmrp  
  
224.8.255.1 179.82.17.200/32 10.20.37.33 vlan 129 1y:2m:2w 0:02:55 dvmrp  
  
224.9.255.1 179.82.17.200/32 10.20.37.33 p-c 7 1d:5h:20m 0:02:55 dvmrp
```

Просмотр таблицы ближайших узлов многоадресной передачи IP

Страница **IPM Next Hop Table** (Таблица ближайших узлов IPM) содержит сведения о ближайших узлах многоадресной передачи. Чтобы открыть страницу, выберите **Router** (Маршрутизатор) → **IP Multicast** (Многоадресная передача IP) → **Multicast Next Hop Table** (Таблица ближайших узлов многоадресной передачи) на панели дерева.

Рис. 8-29. Таблица ближайших узлов IPM



Multicast Group (Группа многоадресной передачи) - IP-адрес группы многоадресной передачи.

Source IP (IP-адрес источника) - IP-адрес устройства источника, для которого назначены данные многоадресной передачи.

Source Mask (Маска источника) - маска всего IP-адреса источника или его части.

Interface (Интерфейс) - номер порта, на который передаются и принимаются пакеты многоадресной передачи.

State (Состояние) - указывает, что порт и ближайший узел используются для передачи многоадресных пакетов. Возможные значения:

Pruned (Усечен) - порт и ближайший узел не используются для передачи многоадресных пакетов.

Forwarding (Пересылка) - порт и ближайший узел в настоящий момент используются для передачи многоадресных пакетов.

Up Time (Время работы) - указывает время, прошедшее с момента получения маршрутизатором данных многоадресной передачи.

Protocol (Протокол) - тип протокола, используемого для определения данных многоадресной передачи. Для этого продукта возможно только значение DVMRP, которое показывает, что для определения данных многоадресной передачи использовался протокол дистанционно-векторной многоадресной маршрутизации.

Отображение таблицы ближайших узлов IPM с помощью команд консоли

В следующей таблице приведены команды консоли для просмотра таблицы ближайших узлов многоадресной передачи IP.

Таблица 8-25. Команды консоли для просмотра таблицы ближайших узлов IPM

Команда консоли	Описание
<code>show ip mroute-next-hop [group адрес_группы] [source адрес_источника]</code>	Отображает содержание таблицы ближайших узлов многоадресной передачи IP.

Далее приведен пример команд консоли.

```
Console> show ip mroute-next-hop
```

```
Group Source Interface Up Time Expiry Time State Owner
-----
224.0.255.1 198.92.37.100/32 eth g2 2 0:20:00 0:02:55 Forward igmp
224.0.255.1 199.92.37.100/32 eth g2 1 :4d:20m 0:02:55 Forward igmp
224.1.1.255.1 198.92.37.100/32 eth g2 2 1:20:00 0:02:55 Forward dvmrp
224.1.1.255.1 199.92.37.100/32 eth g2 1 :4d:20m 0:02:55 Forward dvmrp
```

[Назад на страницу Содержание](#)

[Назад на страницу Содержание](#)

Настройка качества обслуживания

Системы Dell™ PowerConnect™ 6024/6024F

- [Обзор качества обслуживания](#)
- [Настройка общих параметров QoS](#)
- [Настройка основного режима QoS](#)
- [Настройка расширенного режима QoS](#)

Страница Quality of Service (Качество обслуживания) содержит ссылки на основные страницы настройки качества обслуживания (QoS). Чтобы открыть страницу, выберите Quality of Service (Качество обслуживания) на панели дерева.

Обзор качества обслуживания

Сетевой трафик обычно является непредсказуемым, и единственной общей гарантией, которую может предоставить сетевой администратор, - это приложить все усилия для обеспечения максимально возможной скорости доставки трафика. Чтобы решить эту задачу, сетевые администраторы применяют качество обслуживания (QoS) во всей сети. Это гарантирует, что приоритеты сетевого трафика определяются в соответствии с указанными критериями, а также что определенный трафик обрабатывается специальным образом. Качество обслуживания в сети оптимизирует быстродействие сети и связано с двумя основными функциями.

- 1 Классификация входящего трафика по классам обработки на основе атрибута, включая:
 - входящий интерфейс;
 - содержание пакета;
 - сочетание этих атрибутов.
- 1 Обеспечение различных механизмов для определения принадлежности ресурсов сети различным классам обработки, включая:
 - назначение сетевого трафика для определенной аппаратной очереди;
 - назначение внутренних ресурсов;
 - формирование трафика.

В настоящем документе термины класс обслуживания (CoS) и качество обслуживания (QoS) используются в следующем контексте.

- 1 Класс обслуживания предоставляет различное обслуживание трафика Layer 2. Класс обслуживания относится к классификации трафика по классам, которые обрабатываются как единое целое, без отдельных настроек для каждого потока. Качество обслуживания обычно связывают со службой 802.1p, которая классифицирует потоки согласно их приоритетам Layer 2, в соответствии с настройкой в заголовке VLAN.
- 1 Качество обслуживания относится к трафику Layer 2 и выше. Качество обслуживания поддерживает индивидуальные настройки для каждого потока, даже внутри одного класса трафика.

Функция качества обслуживания содержит следующие компоненты:

- 1 **Access Control Lists (ACLs)** (Списки управления доступом ACL) - используются для определения того, какой трафик может попадать в систему, а какой должен быть отброшен. Настройки класса обслуживания и качества обслуживания применяются только для трафика, отвечающего определенным критериям. Списки ACL используются для обеспечения качества обслуживания и безопасности сети.
- 1 **Traffic Classification** (Классификация трафика) - классифицирует каждый входящий пакет по принадлежности к заданному классу трафика на основе содержания пакета и контекста.
- 1 **Assignment to Hardware Queues** (Назначение для аппаратных очередей) - распределяет входящие пакеты по очередям пересылки. Пакеты пересылаются в определенную очередь для обработки в соответствии с классом трафика, к которому они принадлежат, как это определено механизмом классификации.
- 1 **Traffic Class-Handling Attributes** (Атрибуты обработки классов трафика) - применяет различные механизмы качества обслуживания и классов обслуживания для различных классов, включая:
 - управление полосой пропускания;
 - формирование;
 - ограничение.

Списки управления доступом

Списки ACL проверяют входящие пакеты и классифицируют их по логическим группам на основе различных критериев. Для групп ACL определены

специальные действия, которые выполняются с каждым пакетом, который попадает по классификации в эту группу. Списки ACL разрешает следующие действия:

- 1 пересылка;
- 1 запрет;
- 1 запрет и отключение порта.

Списки ACL используются для следующих основных целей.

- 1 В качестве механизма обеспечения безопасности, разрешающего или запрещающего попадание пакетов в группу. Этот механизм описан в разделе, посвященном безопасности сети.
- 1 В качестве механизма классификации пакетов по классам трафика, для которых выполняются различные действия CoS/QoS.

Списки ACL содержат множество классификационных правил и действий. Элемент управления доступом (ACE) состоит из одного классификационного правила и соответствующего действия. Один список ACL может содержать один или несколько элементов ACE.

Последовательность элементов ACE внутри списка ACL является важной, поскольку они применяются по методу первого подходящего. Элементы ACE обрабатываются последовательно, начиная с первого элемента ACE. Если пакет совпадает с классификацией ACE, выполняется действие ACE, и обработка списка ACL прекращается. Если требуется обработать несколько списков ACL, то действие по умолчанию применяется только после обработки всех этих списков. При использовании настройки отбрасывания трафика по умолчанию пользователю требуется в явном виде разрешить весь разрешенный трафик, включая трафик управления, например telnet, HTTP или SNMP, который передается на сам маршрутизатор.

Можно определить два типа списков ACL.

- 1 IP ACL - применяется только к пакетам IP. Все поля классификации связаны с IP-пакетами.
- 1 MAC ACL - применяется к любому пакету, включая пакеты, не являющиеся IP-пакетами. Поля классификации основаны только на полях Layer 2.

Списки ACL можно применить для интерфейса двумя способами:

- 1 Policy (Политика) - в этой форме списки ACL группируются вместе в более сложную структуру, называемую политикой. Политика может содержать как списки ACL, так и правила качества обслуживания (QoS). Пользователь может применять политику для интерфейса (см. раздел «Расширенный режим QoS»).
- 1 Simple (Простой) - в простой форме для интерфейса применяется один список ACL (MAC или IP). Несмотря на то, что политику нельзя применять для интерфейса, можно применить основные правила качества обслуживания (QoS), которые выполняют классификацию пакетов по очередям вывода (см. раздел «Основной режим QoS»).

Привязка к очередям

Можно выбрать поведение доверия или выбрать поля службы вывода, включая:

- 1 VLAN Priority Tags (VPT) (Метки приоритета VLAN) - метки VPT привязываются к очередям вывода на основе VPT. Сопоставление очередям может настраивать пользователь. По умолчанию используется следующее сопоставление меток VPT очередям вывода. Queue 1 (Очередь 1) имеет самый низкий приоритет, как показано в следующей таблице.

Таблица 10-1. Таблица сопоставления VPT по умолчанию

Значение VPT	Номер очереди
0	3
1	1
2	2
3	4
4	5
5	6
6	7
7	8



ПРИМЕЧАНИЕ. Сопоставление метки VPT с очередью вывод выполняется по всей системе и может включаться или отключаться для каждого порта отдельно.

- 1 802.1p Port-Based (802.1p на основе портов) - для немеченных при поступлении пакетов по умолчанию назначается метка VPT по

умолчанию, которая может устанавливаться пользователями отдельно для каждого порта. После назначения метки VPT пакет обрабатывается так, как будто он уже был получен с этим тегом. Сопоставление меток VPT очередям вывода основано на тех же определениях на основе меток 802.1p, которые задает пользователь.

- 1 **Layer 3 Predefined Field** (Предварительно определенное поле Layer 3) - пользователь может настроить в системе использование IP DSCP входящего пакета для очередей приоритета вывода. Сопоставление IP DSCP приоритетной очереди задается для всей системы. Если активен этот режим, пакет не IP всегда будет попадать по классификации в очередь с максимальной возможной скоростью доставки. Сопоставление по умолчанию показано в следующей таблице:

Таблица 10-2. Таблица сопоставления DSCP по умолчанию

Значение DSCP	Номер очереди
0-7	q1 (низший приоритет)
8-15	q2
16-23	q3
24-31	q4
32-39	q5
40-47	q6
48-55	q7
56-63	q8 (высший приоритет)

 **ПРИМЕЧАНИЕ.** Значения DSCP 3, 11, 19, 27, 35, 43, 51 и 59 сопоставляются с q1, q2 ... q8. Эти параметры не изменяются.

- 1 **Layer 4 Predefined Fields** (Предварительно определенные поля Layer 4) - настраивают использование в системе порта назначения TCP/UDP входящего пакета для сопоставления пакета с очередями приоритета вывода. Сопоставление порта назначения TCP/UDP с приоритетной очередью настраивается для всей системы в двух отдельных таблицах. Его можно включать или отключать отдельно для каждого порта.
- 1 **None (Нет)** - весь трафик будет попадать по классификации в очередь с максимальной возможной скоростью доставки.

После постановки пакетов в определенную очередь можно применить различные службы, используя выбранный метод классификации. Можно настроить график для очередей вывода, следующие методы:

- 1 строгий приоритет;
- 1 режим WRR (Weighted Round Robin);
- 1 сочетание этих методов.

Схемы графиков указываются для каждой системы. Значения весов WRR для очередей можно назначать в любом порядке. Параметры весов можно назначать отдельно для каждого порта.

Для каждого интерфейса или очереди можно также настроить следующее формирование на выходе:

- 1 объем данных;
- 1 гарантированная скорость передачи данных (CIR);
- 1 действия в случае превышения ограничения для трафика.

Режимы QoS

В PowerConnect 6024/6024F возможно использование QoS в основном и расширенном режимах QoS.

режима QoS

В основном режиме QoS можно активизировать один режим доверия, включая:

- 1 VPT
- 1 DSCP
- 1 TCP
- 1 UDP

- 1 None (Нет)

Кроме того, один список ACL, основанный на MAC- или IP-адресах, может быть напрямую подключен к интерфейсу (дополнительную информацию см. в разделе [Настройка безопасности сети](#)). На основе определенной классификации в очередь вывода назначаются только пакеты, имеющие признак действия Forward (Пересылка).

Для правильной конфигурации выходной очереди можно установить следующие основные режимы обслуживания:

- 1 **Minimum Delay** (Минимальная задержка) - для очереди назначается политика строгого приоритета, а трафик назначается для очереди с высшим приоритетом.
- 1 **Best Effort** (Максимально возможная скорость доставки) - трафик назначается для очереди с низшим приоритетом
- 1 **Bandwidth Assignments** (Назначение полосы пропускания) - полосу пропускания можно настраивать путем настройки схемы графиков WRR и выбора весовых коэффициентов прав.

расширенного режима QoS

Расширенный режим качества обслуживания (QoS) определяет правила для указания классификации потока и назначает систему правил, относящихся к управлению полосой пропускания. Правила определяются в списках управления классификацией (CCL).

Списки управления классификацией (CCL) устанавливаются в соответствии с классификацией, определенной в списке ACL, и их нельзя определить, пока не будет определен действительный список ACL. Когда списки управления классификацией (CCL) определены, можно сгруппировать списки CCL и ACL вместе в более сложную структуру, называемую «политикой». Политики могут быть назначены для интерфейса. Списки ACL/CCL в форме политики применяются в той последовательности, в какой они отображаются в политике. К порту можно подключить только одну политику.

В расширенном режиме QoS списки ACL могут быть назначены непосредственно для интерфейса. Однако для интерфейса нельзя одновременно применять и политику, и список ACL.

После назначения пакетов для определенной очереди можно применить такие службы, как настройка очередей вывода для схемы графика или настройка формирования на выходе для размера последовательности, CIR или CBS для каждого интерфейса или для каждой очереди.

Пример настройки службы

Расширенный режим QoS можно использовать для назначения следующих служб для сетевого трафика:

- 1 **Best Effort** (Максимально возможная скорость доставки) - трафик назначается для очереди с низшим приоритетом.
- 1 **802.1p** - значение VPT устанавливается в соответствии с классификацией.
- 1 **IP DSCP** - значение устанавливается в соответствии с классификацией.
- 1 **Minimum Delay** (Минимальная задержка) - для очереди назначается политика строгого приоритета, а трафик назначается для очереди с высшим приоритетом.
- 1 **Ingress Metering/Rate Limiting** (Измерение на входе/Ограничение скорости) - задается максимальная величина полосы пропускания, свыше которой весь трафик отбрасывается. Это выполняется путем установки измерителя трафика на входе, настроенного на максимальную полосу пропускания, и настройки четкой политики для отбрасывания трафика. Для эффективной настройки этой службы суммарная полоса пропускания для конкретного выходного порта не должна превышать его скорость.

Настройка общих параметров QoS

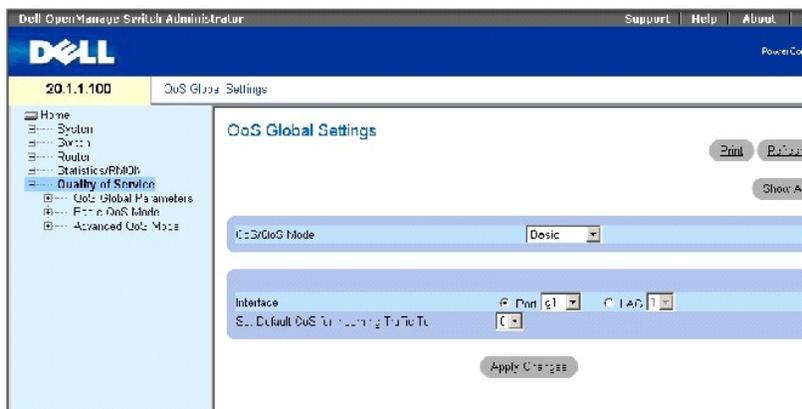
Страница QoS Global Parameters (Общие параметры QoS) содержит ссылки на страницы QoS, на которых включается функция QoS, назначаются значения и перенастраивается сопоставление параметров DSCP, определяется управление очередями сетевого трафика и классификация трафика. Чтобы открыть эту страницу, выберите Quality of Service (Качество обслуживания)→ QoS Global Parameters (Общие параметры QoS) на панели дерева.

Определение параметров QoS

Используйте страницу QoS Global Settings (Общие параметры QoS) для выбора режима QoS и настройки класса обслуживания CoS по умолчанию для входящего трафика на выбранном интерфейсе. Чтобы открыть эту страницу, выберите Quality of Service (Качество обслуживания)→ QoS Global

Parameters (Общие параметры QoS) → QoS Settings (Параметры QoS) на панели дерева.

Рис. 10-1. Страница общие параметры QoS



QoS Mode (Режим QoS) - включает или отключает основной или расширенный режим QoS. Основной режим включен по умолчанию.

ПРИМЕЧАНИЕ. При переключении между основным и расширенным режимами QoS некоторые настройки могут быть потеряны.

Interface (Интерфейс) - порт или группа LAG, для которых определена политика CoS по умолчанию.

Set Default CoS for Incoming Traffic To (Задать CoS по умолчанию для входящего трафика) - определяет значение по умолчанию CoS для входящих пакетов, для которых не определена метка VLAN. Возможные значения поля: 0-7. По умолчанию для CoS установлено значение 0.

Выбор режима обслуживания

1. Откройте страницу QoS Settings (Параметры QoS).
2. Выберите режим обслуживания в поле QoS Mode (Режим QoS).
3. Нажмите кнопку Apply Changes (Применить изменения).

Режим QoS будет выбран, а устройство обновлено.

Установка значения по умолчанию CoS для входящего трафика на интерфейсе

1. Откройте страницу QoS Settings (Параметры QoS).
2. Выберите интерфейс и выберите в раскрывающемся списке значение CoS по умолчанию для входящего трафика.
3. Нажмите кнопку Apply Changes (Применить изменения).

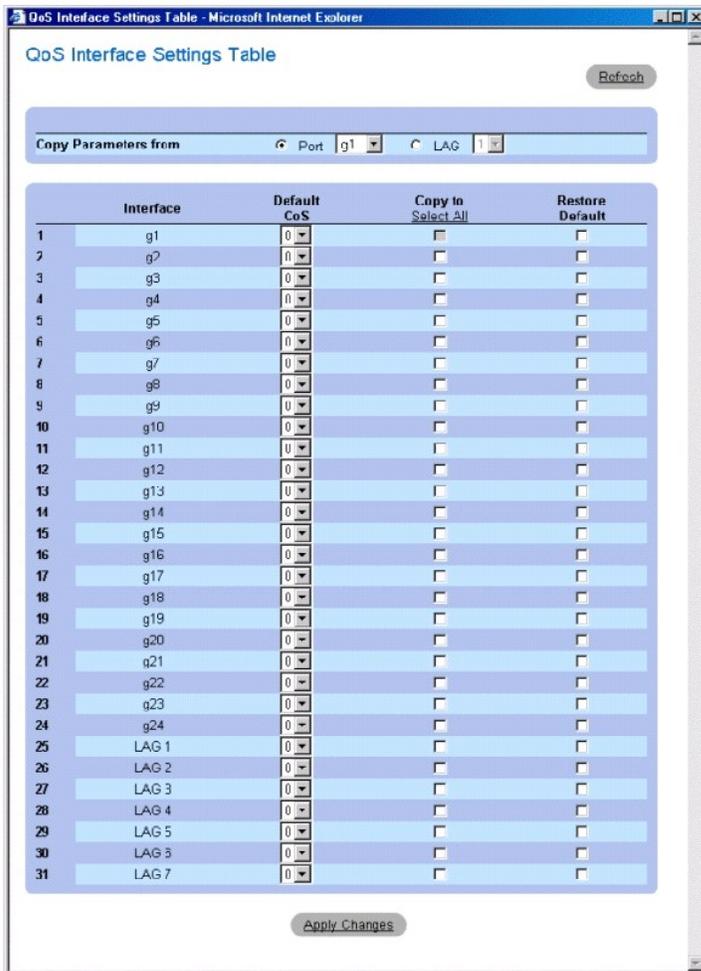
Будет установлено значение CoS по умолчанию для входящего трафика интерфейса, а устройство обновлено.

Копирование параметров интерфейса QoS

1. Откройте страницу QoS Settings (Параметры QoS).
2. Нажмите кнопку Show All (Показать все), чтобы отобразить страницу QoS Interface Settings Table (Таблица параметров интерфейса QoS).
3. Выберите интерфейс, из которого необходимо скопировать параметры QoS во все интерфейсы или в интерфейсы, перечисленные в QoS Interface Settings Table (Таблица параметров интерфейса QoS).
4. Установите флажок Copy to (Копировать в), чтобы определить каждый интерфейс, для которого будут скопированы параметры QoS, или нажмите Select All (Выбрать все) для копирования параметров QoS во все перечисленные интерфейсы.

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

Рис. 10-2. Страница таблицы параметров интерфейса QoS



Определение параметров QoS с помощью команд консоли

Таблица 10-3. Команды консоли для определения параметров QoS

Команда консоли	Описание
qos [расширенный]	Включает или отключает QoS в основном или расширенном режиме для всего устройства.
show qos	Отображает режим QoS для всего устройства.
qos cos default- cos	Настройка значения по умолчанию CoS для интерфейса.

Далее приведен пример команд консоли.

```
Console(config)# qos
```

```
Console (config)# interface ethernet g5
```

```
Console (config-if)# qos cos 3
```

```
Console(config-if)# exit
```

```
Console(config)# exit
```

```
Console# show qos
```

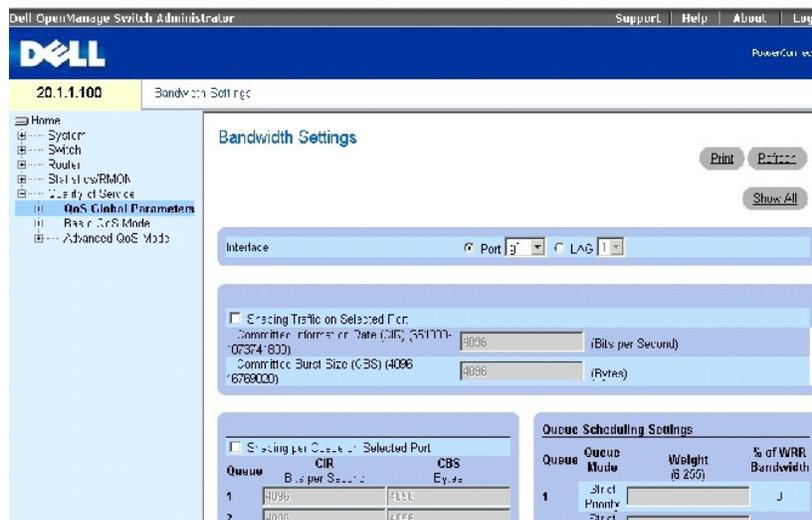
```
QoS: basic
```

```
Basic trust: vpt
```

Определение параметров полосы пропускания

Для определения параметров полосы пропускания определенного входящего интерфейса используйте страницу **Bandwidth Settings** (Параметры полосы пропускания). Изменение графика очередей влияет на общие параметры очередей. Чтобы открыть эту страницу, выберите **Quality of Service** (Качество обслуживания) → **QoS Global Parameters** (Общие параметры QoS) → **Bandwidth Settings** (Параметры полосы пропускания) на панели дерева.

Рис. 10-3. Параметры полосы пропускания



Страница [Bandwidth Settings](#) (Параметры полосы пропускания) содержит следующие поля.

Interface (Интерфейс) - порт или группа LAG, для которых определяются параметры полосы пропускания.

Shaping Traffic on Selected Port (Формирование трафика для выбранного порта) - настраивает гарантированную скорость передачи данных (CIR) и гарантированный объем данных (CBS) для интерфейса. Возможно одновременное использование формирования для очереди и интерфейса. Формирование определяется по наименьшей из указанных величин.

Shaping per Queue on Selected Port (Формирование очереди для выбранного порта) - настраивает CIR и CBS для отдельных очередей. Возможно одновременное использование формирования для очереди и интерфейса. Формирование определяется по наименьшей из указанных величин.

Queue Scheduling Settings (Параметры планирования очереди) - настраивает веса для каждой очереди WRR.

WRR Weight (0-255) (Вес WRR (0-255)) - назначает веса для каждой очереди WRR. Очереди WRR определены для каждого порта и имеют диапазон 6-255. Для каждой очереди можно установить значение веса 0, в этом случае она перестанет работать и полностью закроется.

Формирование трафика для выбранного интерфейса

1. Откройте страницу **Bandwidth Settings** (Параметры полосы пропускания).
2. Выберите интерфейс.
3. Установите флажок **Shaping Traffic on Selected Port** (Формирование трафика для выбранного порта).
4. Введите значение CIR и CBS для интерфейса.
5. Нажмите кнопку **Apply Changes** (Применить изменения).

Значения CIR и CBS будут настроены для выбранного интерфейса, а устройство обновлено.

Формирование трафика для отдельных очередей

1. Откройте страницу **Bandwidth Settings** (Параметры полосы пропускания).
2. Выберите интерфейс.
3. Установите флажок **Shaping per Queue on Selected Port** (Формирование очереди для выбранного порта).
4. Введите значения CIR и CBS для каждой очереди.
5. Нажмите кнопку **Apply Changes** (Применить изменения).

Значения CIR и CBS будут настроены для каждой очереди выбранного интерфейса, а устройство обновлено.

Настройка параметров планирования очереди для порта

1. Откройте страницу **Bandwidth Settings** (Параметры полосы пропускания).

 **ПРИМЕЧАНИЕ.** Используйте страницу **Global Queue Settings** (Общие параметры очереди) для изменения общих параметров планирования очереди.

2. Для каждой из восьми очередей настройте значение **Strict Priority** (Строгий приоритет) или введите значение **Weight** (Вес).
3. Для каждой очереди, которая установлена как очередь WRR для системы в целом, необходимо ввести вес.

Весовой коэффициент определяет частоту, с которой планировщик удаляет пакеты из каждой очереди. Коэффициент для каждой очереди определяется весом очереди, деленным на сумму всех весов очередей (нормализованный вес). Таким образом задается полоса пропускания для каждой очереди.

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

Устройство будет обновлено.

Отображение таблицы параметров полосы пропускания порта

1. Откройте страницу **Bandwidth Settings** (Параметры полосы пропускания).
2. Нажмите кнопку **Show All** (Показать все), чтобы отобразить страницу **Port Bandwidth Settings Table** (Таблица параметров полосы пропускания порта).

Рис. 10-4. Таблица параметров полосы пропускания порта

Port	Shaping Type	Per Port Shaping Rates		Copy to Selected
		CIR	CBS	
1 g1	None			<input type="checkbox"/>
2 g2	None			<input type="checkbox"/>
3 g3	None			<input type="checkbox"/>
4 g4	None			<input type="checkbox"/>
5 g5	None			<input type="checkbox"/>
6 g6	None			<input type="checkbox"/>
7 g7	None			<input type="checkbox"/>
8 g8	None			<input type="checkbox"/>
9 g9	None			<input type="checkbox"/>
10 g10	None			<input type="checkbox"/>
11 g11	None			<input type="checkbox"/>
12 g12	None			<input type="checkbox"/>
13 g13	None			<input type="checkbox"/>
14 g14	None			<input type="checkbox"/>
15 g15	None			<input type="checkbox"/>
16 g16	None			<input type="checkbox"/>
17 g17	None			<input type="checkbox"/>
18 g18	None			<input type="checkbox"/>
19 g19	None			<input type="checkbox"/>
20 g20	None			<input type="checkbox"/>
21 g21	None			<input type="checkbox"/>
22 g22	None			<input type="checkbox"/>
23 g23	None			<input type="checkbox"/>
24 g24	None			<input type="checkbox"/>
25 LAG 1	None			<input type="checkbox"/>
26 LAG 2	None			<input type="checkbox"/>
27 LAG 3	None			<input type="checkbox"/>
28 LAG 4	None			<input type="checkbox"/>
29 LAG 5	None			<input type="checkbox"/>
30 LAG 6	None			<input type="checkbox"/>
31 LAG 7	None			<input type="checkbox"/>

Shaping Type (Тип формирования) - возможно формирование по портам, по очередям, по тому и другому, а также оно может совсем не выполняться.

Per Port Shaping Rates (Скорости формирования по портам) - CIR и CBS определяются по портам. Для просмотра формирования по очередям используйте страницу редактирования.

Копирование параметров полосы пропускания порта

1. Откройте страницу **Bandwidth Settings** (Параметры полосы пропускания).
2. Нажмите кнопку **Show All** (Показать все), чтобы отобразить страницу **Port Bandwidth Settings Table** (Таблица параметров полосы пропускания порта).
3. Выберите интерфейс, из которого необходимо скопировать параметры полосы пропускания порта во все интерфейсы или в интерфейсы, перечисленные в **Port Bandwidth Settings Table** (Таблице параметров полосы пропускания порта).
4. Установите флажок **Copy to** (Копировать в), чтобы определить каждый интерфейс, для которого будут скопированы параметры полосы пропускания порта или нажмите **Select All** (Выбрать все) для копирования параметров полосы пропускания порта во все перечисленные интерфейсы.
5. Нажмите кнопку **Apply Changes** (Применить изменения).

Определение параметров полосы пропускания порта с помощью команд консоли

Таблица 10-4. Команды консоли для параметров полосы пропускания порта

Команда консоли	Описание

<code>traffic-shape {гарантированная_скорость гарантированный_объем} [идентификатор_очереди]</code>	Настройка формирователя для входящего порта или очереди.
<code>wrr-queue bandwidth sec1 sec2 ... sec_n</code>	Назначает веса WRR для очередей выхода.
<code>priority-queue out num- of-queues число_очередей</code>	Настраивает число очередей со строгим приоритетом.
<code>show qos interface [ethernet номер_интерфейса vlan идентификатор_vlan port-channel номер] [buffers queuing policers shapers]</code>	Отображает данные интерфейса QoS.

Далее приведен пример команд консоли.

```
Console (config)# interface ethernet g5
```

```
Console(config-if)# traffic-shape 124000 96000
```

```
Console(config-if)# wrr-queue bandwidth 1 2 3 4 5 6 7 8
```

```
Console(config-if)# exit
```

```
Console(config)# priority-queue out num-of-queues 2
```

```
Console(config)# exit
```

```
Console> show qos interface ethernet g1 buffers
```

```
Ethernet g1
```

```
Notify Q depth:
```

```
qid-size
```

```
1 - 125
```

```
2 - 125
```

```
3 - 125
```

```
4 - 125
```

```
5 - 125
```

```
125 - 6
```

7 - 125

8 - 125

qid WRED thresh0 thresh1 thresh2

1 dis 100 100 100

2 dis 100 100 100

3 dis 100 100 100

4 dis 100 100 100

5 Ena N/A N/A N/A

6 Ena N/A N/A N/A

7 Ena N/A N/A N/A

8 Ena N/A N/A N/A

qid MinDP0 MaxDP0 ProbDP0 MinDP1 MaxDP1 ProbDP1 MinDP2 MaxDP2 ProbDP2 weight

1 N/A N/A N/A N/A N/A N/A N/A N/A N/A N/A

2 N/A N/A N/A N/A N/A N/A N/A N/A N/A N/A

3 N/A N/A N/A N/A N/A N/A N/A N/A N/A N/A

4 N/A N/A N/A N/A N/A N/A N/A N/A N/A N/A

5 50 60 13 65 80 6 85 95 4 2

6 50 60 13 65 80 6 85 95 4 2

7 50 60 13 65 80 6 85 95 4 2

8 50 60 13 65 80 6 85 95 4 2

Console> show qos interface ethernet g1 queueing

Ethernet g1

wrr bandwidth weights and EF priority:

qid-weights EF - Priority

1 - 125 dis- N/A

2 - 125 dis- N/A

3 - 125 dis- N/A

4 - 125 dis- N/A

5 - N/A ena- 5

6 - 125 dis- N/A

7 - 125 dis- N/A

8 - N/A ena- 8

Cos-queue map:

cos-qid

0-3

1 - 1

2 - 2

3 - 4

4 - 5

5 - 6

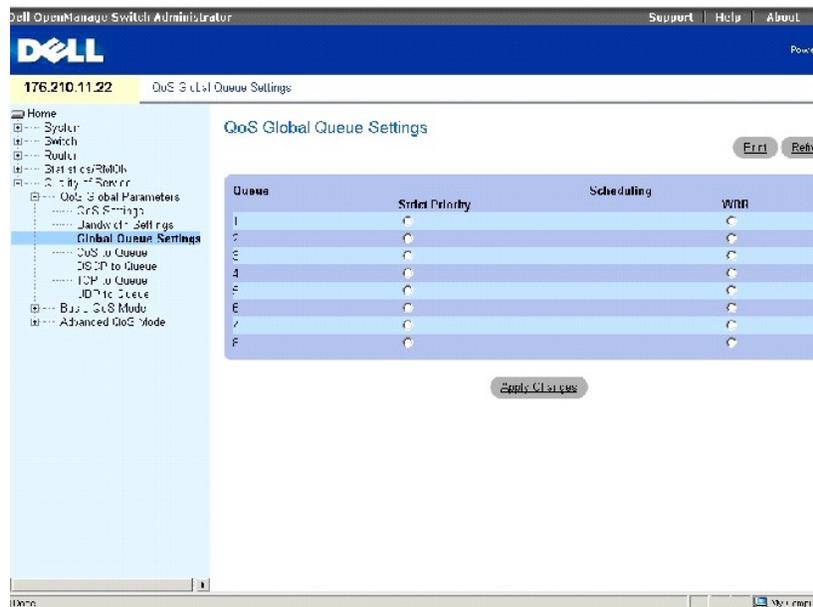
6 - 7

Определение общих параметров очереди

Для общего изменения параметров планирования очереди используйте страницу [Global Queue Settings](#) (Общие параметры очереди).

Чтобы открыть эту страницу, выберите Quality of Service (Качество обслуживания) → QoS Global Parameters (Общие параметры QoS) → Queue Settings (Параметры очереди) на панели дерева.

Рис. 10-5. Общие параметры очереди



Страница [Global Queue Settings](#) (Общие параметры очереди) содержит следующие поля.

Queue (Очередь) - указывает на номер очереди.

Strict Priority (Строгий приоритет) - показывает, что планирование трафика основано строго на приоритете очереди. Это значение по умолчанию для очередей.

WRR - показывает, что планирование трафика основано на весах Weighted Round Robin (WRR) для назначенных очередей выхода. Весы WRR определяются на странице [Bandwidth Settings](#) (Параметры полосы пропускания).

Настройка общих параметров планирования очереди

1. Откройте страницу [Global Queue Settings](#) (Общие параметры очереди).
2. Для каждой очереди выберите Strict Priority (Строгий приоритет) или WRR (Weighted Round Robin).

Параметры WRR устанавливаются для порта на странице [Bandwidth Settings](#) (Параметры полосы пропускания).

При выборе параметра для любой очереди автоматически выбирается тип планирования для следующих очередей. Каждая очередь перед выбранной очередью использует противоположный тип планирования приоритетов. Например, если выбрано Strict Priority (Строгий приоритет) для очереди 6, для очередей 7 и 8 будет также выбран параметр Strict Priority (Строгий приоритет); для очередей с 1 по 5 будет выбран параметр WRR.

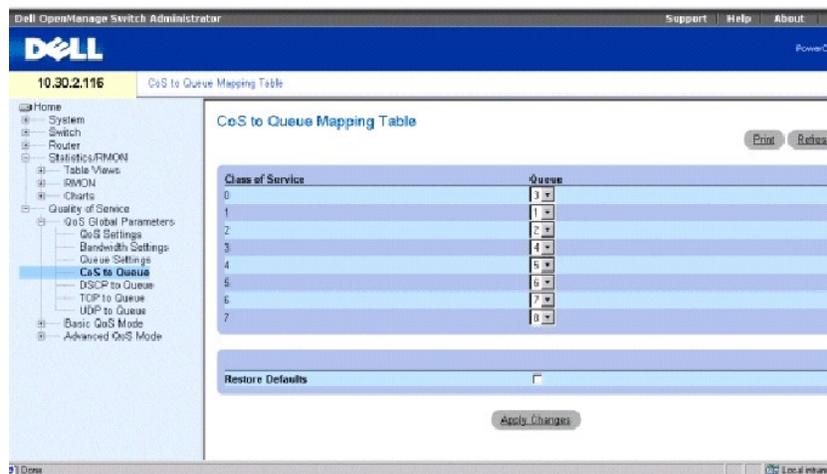
ПРИМЕЧАНИЕ. Как минимум две очереди необходимо настроить как очереди WRR.

3. Нажмите кнопку [Apply Changes](#) (Применить изменения), чтобы обновить устройство.

Определение привязки CoS к очереди

На странице CoS to Queue Mapping Table (Таблица привязки CoS к очереди) можно выполнить привязку значений CoS к определенной очереди. Чтобы открыть эту страницу, выберите Quality of Service (Качество обслуживания) → QoS Global Parameters (Общие параметры CoS) → CoS to Queue (Привязка CoS к очереди) на панели дерева.

Рис. 10-6. Страница CoS to Queue Mapping Table Page (Таблица привязки CoS к очереди)



Class of Service (Класс обслуживания) - метка приоритета VLAN 802.1Q во входящих пакетах.

Queue (Очередь) - привязка CoS к выбранной очереди. Возможны следующие значения для очереди: 1-8.

Входящие пакеты с определенным значением CoS привязываются к определенной очереди, если для CoS включен **Trust** (Доверенный режим).

Restore Defaults (Восстановить значения по умолчанию) - восстанавливает для всех очередей значения параметров класса по умолчанию.

Привязка CoS к очередям

1. Откройте страницу **CoS to Queue Mapping Table** (Таблица привязки CoS к очереди).
2. Выберите очередь для каждой записи **Class of Service** (Класс обслуживания).
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Значение CoS будет привязано к очередям, а устройство обновлено.

Восстановление значения по умолчанию для привязки CoS к очередям:

1. Откройте страницу **CoS to Queue Mapping Table** (Таблица привязки CoS к очереди).
2. Выберите **Restore Defaults** (Восстановить значения по умолчанию).
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Для параметров привязки CoS к очередям будут установлены значения по умолчанию, а устройство обновлено.

Привязка значений CoS к очередям с помощью команд консоли

Следующая таблица содержит команды консоли для привязки значений CoS к очередям.

Таблица 10-5. Команды консоли для привязки значений CoS к очередям

Команда консоли	Описание
<code>wrr-queue cos-map идентификатор_очереди cos1 ... cos8</code>	Привязывает назначенные значения CoS к одной из очередей выхода.
<code>show qos map [dscp-queue tcp-port-queue udp-port-queue dscp-policed dscp-mutation]</code>	Отображает все привязки для QoS

Далее приведен пример команд консоли.

```
console(config)# wrr-queue cos-map 7 246
```

```
console(config)# show qos map dscp-queue
```

```
Dscp-queue map:
```

```
d1 : d2 0 1 2 3 4 5 6 7 8 9
```

```
-----
```

```
0 : 01 01 01 01 01 01 01 01 02 02
```

```
1 : 02 02 02 02 02 02 03 03 03 03
```

```
2 : 03 03 03 03 04 04 04 04 04 04
```

```
3 : 04 04 05 05 05 05 05 05 05 05
```

```
4 : 06 06 06 06 06 06 06 06 07 07
```

```
5 : 07 07 07 07 07 07 08 08 08 08
```

```
6 : 08 08 08 08
```

```
console(config)# show qos map tcp-port-queue
```

```
Tcp port-queue map:
```

Port queue

6000 1

6001 2

6002 3

console(config)# show qos map udp-port-queue

Udp port-queue map:

Port queue

8000 1

8001 2

console(config)# show qos map dscp-policed

Policed-dscp map:

d1 : d2 0 1 2 3 4 5 6 7 8 9

0 : 00 01 02 03 04 05 06 07 08 09

1 : 10 11 12 13 14 15 16 17 18 19

2 : 20 21 22 23 24 25 26 27 28 29

3 : 30 31 32 33 34 35 36 37 38 39

4 : 40 41 42 43 44 45 46 47 48 49

5 : 50 51 52 53 54 55 56 57 58 59

```
6 : 60 61 62 63
```

```
console(config)# show qos map dscp-mutation
```

```
Dscp-dscp mutation map:
```

```
d1 :d2 0 1 2 3 4 5 6 7 8 9
```

```
-----
```

```
0 : 00 01 02 03 04 05 06 07 08 09
```

```
1 : 10 11 12 13 14 15 16 17 18 19
```

```
2 : 20 21 22 23 24 25 26 27 28 29
```

```
3 : 30 31 32 33 34 35 36 37 38 39
```

```
4 : 40 41 42 43 44 45 46 47 48 49
```

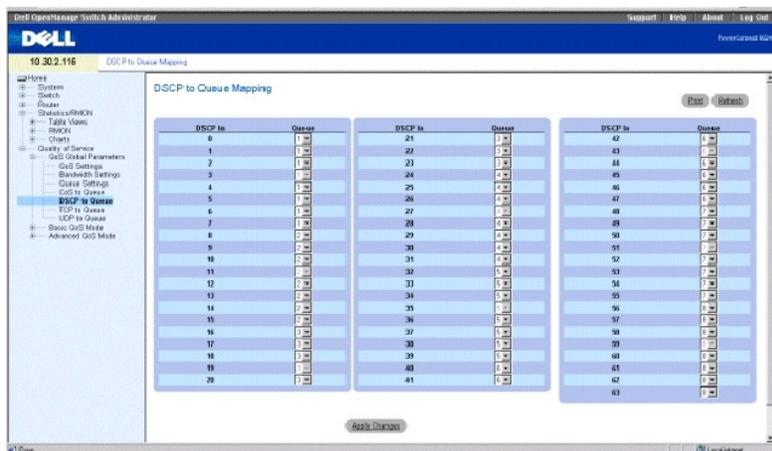
```
5 : 50 51 52 53 54 55 56 57 58 59
```

```
6 : 60 61 62 63
```

Определение привязки DSCP к очереди

На странице **DSCP to Queue Mapping** (Привязка DSCP к очереди) можно выполнить привязку значений DSCP к определенной очереди. Чтобы открыть эту страницу, выберите **Quality of Service** (Качество обслуживания) → **QoS Global Parameters** (Общие параметры QoS) → **DSCP to Queue** (Привязка DSCP к очереди) на панели дерева.

Рис. 10-7. Страница DSCP to Queue Mapping (Привязка DSCP к очереди)



DSCP In (DSCP входящего пакета) - показывает значение DSCP (Differentiated Services Code Point) во входящем пакете

Queue (Очередь) - привязка значения DSCP к выбранной очереди.

Входящие пакеты с определенным значением DSCP привязываются к определенной очереди, если для DSCP включен **Trust** (Доверенный режим). Значения DSCP 3, 11, 19, 27, 35, 43, 51 и 59 сопоставляются с q1, q2 ... q8. Эти параметры не изменяются.

Привязка DSCP к очередям

1. Откройте страницу **DSCP to Queue Mapping** (Привязка DSCP к очереди).
2. Выберите очередь для каждого уровня DSCP.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Значение DSCP будет привязано к очередям, а устройство обновлено.

Привязка значений DSCP к очередям с помощью команд консоли

Таблица 10-6. Команды консоли для привязки DSCP к очередям

Команда консоли	Описание
<code>qos map dscp-queue список_dscp to идентификатор_очереди</code>	Изменяет привязку DSCP к CoS.
<code>show qos map [dscp-queue tcp-port-queue udp-port-queue dscp-policed dscp-mutation]</code>	Отображает все привязки для QoS.

Далее приведен пример команд консоли.

```
console(config)# qos map dscp-queue 33 40 41 to 1
```

```
Console(config)# exit
```

```
console# show qos map dscp-queue
```

Dscp-queue Map

d1: d2 0 1 2 3 4 5 6 7 8 9

0: 01 01 01 01 01 01 02 02

1: 02 02 02 02 02 03 03 03

2: 03 03 03 04 04 04 04 04

3: 04 04 05 05 05 05 05 05

4: 06 06 06 06 06 06 07 07

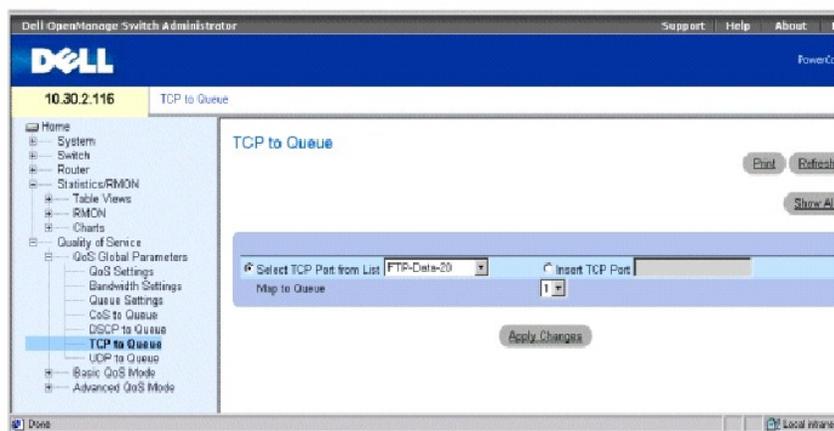
5: 07 07 07 07 08 08 08 08

6: 08 08 08 08

Определение привязки QoS TCP к очереди

На странице QoS TCP to Queue (Привязка QoS TCP к очереди) можно выполнить привязку порта TCP к очереди. Чтобы открыть эту страницу, выберите Quality of Service (Качество обслуживания) → QoS Global Parameters (Общие параметры QoS) → TCP to Queue (Привязка TCP к очереди) на панели дерева.

Рис. 10-8. Страница QoS TCP to Queue (Привязка QoS TCP к очереди)



Select TCP Port from List (Выбор порта TCP в списке) - выбирает известный порт TCP для привязки к очереди.

Insert TCP Port (Добавить порт TCP) - позволяет вручную ввести порт TCP для привязки к очереди.

Map to Queue (Привязка к очереди) - определяет очередь, к которой привязан указанный порт TCP.

Привязка известного порта TCP к очереди

1. Откройте страницу **TCP to Queue** (Привязка TCP к очереди).
2. Выберите параметр **Select TCP Port from List** (Выбор порта TCP в списке).
3. Выберите порт TCP.
4. Выберите очередь в списке **Map to Queue** (Привязка к очереди).
5. Нажмите кнопку **Apply Changes** (Применить изменения).

Порт TCP будет привязан к указанной очереди, а устройство обновлено.

Привязка неуказанного порта TCP к очереди

1. Откройте страницу **QoS TCP to Queue** (Привязка QoS TCP к очереди).
2. Выберите параметр **Insert TCP Port** (Добавить порт TCP).
3. Введите номер порта TCP и его описание в поле **Insert TCP Port** (Добавить порт TCP).
4. Выберите очередь в списке **Map to Queue** (Привязка к очереди).
5. Нажмите кнопку **Apply Changes** (Применить изменения).

Порт TCP будет привязан к указанной очереди, а устройство обновлено.

Удаление привязки порта TCP к очереди

1. Откройте страницу **QoS TCP to Queue** (Привязка QoS TCP к очереди).
2. Нажмите кнопку **Show All** (Показать все), чтобы отобразить страницу **TCP to Queue Mapping Table** (Таблица привязки TCP к очереди).
3. Установите флажок **Remove** (Удалить) для каждого порта TCP, для которого необходимо удалить привязку к очереди.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Определение привязки портов TCP к очереди командами консоли

Таблица 10-7. Команды консоли для привязки портов TCP к очереди

Команда консоли	Описание
<code>qos map tcp-port- queue порт1 ... порт 8 к идентификатору_очереди</code>	Изменяет привязку порта TCP к очереди.
<code>show qos map [dscp- queue tcp-port- queue udp-port- queue dscp-policed dscp-mutation]</code>	Отображает все привязки для QoS.

Далее приведен пример команд консоли.

```
console(config)# qos map tcp-port-queue 2000 80 to 2
```

```
console(config)# exit
```

```
console# show qos map tcp-port-queue
```

```
Tcp port - queue map
```

```
Port queue
```

```
-----
```

```
6000 1
```

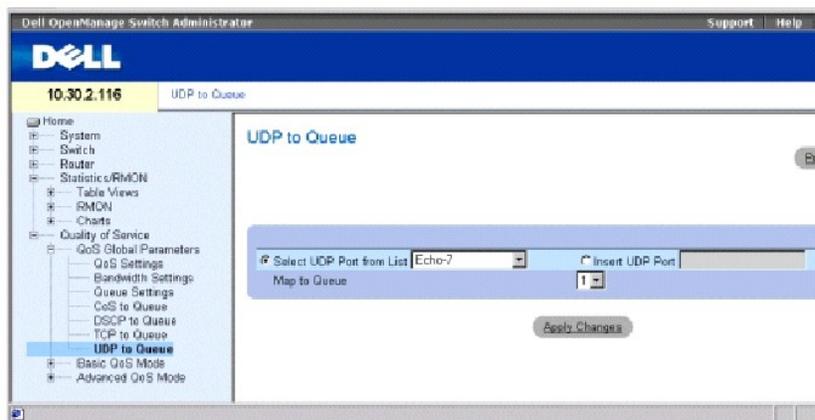
```
6001 2
```

```
6002 3
```

Определение привязки QoS UDP к очереди

На странице QoS UDP to Queue (Привязка QoS UDP к очереди) можно выполнить привязку порта UDP к очереди. Чтобы открыть эту страницу, выберите Quality of Service (Качество обслуживания) → QoS Global Parameters (Общие параметры QoS) → UDP to Queue (Привязка UDP к очереди) на панели дерева.

Рис. 10-9. Страница UDP to Queue (Привязка UDP к очереди)



Select UDP Port from List (Выбор порта UDP в списке) - выбирает известный порт UDP для привязки к очереди.

Insert UDP Port (Добавить порт UDP) - позволяет вручную ввести порт UDP для привязки к очереди.

Map to Queue (Привязка к очереди) - определяет очередь, к которой привязан указанный порт UDP.

Привязка известного порта UDP к очереди

1. Откройте страницу UDP to Queue (Привязка порта UDP к очереди).
2. Выберите параметр Select UDP Port from List (Выбор порта UDP в списке).

3. Выберите порт UDP.
4. Выберите очередь в списке **Map to Queue** (Привязка к очереди).
5. Нажмите кнопку **Apply Changes** (Применить изменения).

Порт UDP будет привязан к указанной очереди, а устройство обновлено.

Привязка неуказанного порта UDP к очереди

1. Откройте страницу **UDP to Queue** (Привязка порта UDP к очереди).
2. Выберите параметр **Insert UDP Port** (Добавить порт UDP).
3. Введите номер порта UDP в поле **Insert UDP Port** (Добавить порт UDP).
4. Выберите очередь в списке **Map to Queue** (Привязка к очереди).
5. Нажмите кнопку **Apply Changes** (Применить изменения).

Порт UDP будет привязан к указанной очереди, а устройство обновлено.

Удаление привязки порта UDP к очереди

1. Откройте **страницу UDP to Queue** (Привязка порта UDP к очереди).
2. Нажмите кнопку **Show All** (Показать все), чтобы отобразить страницу **UDP to Queue Mapping Table** (Таблица привязки UDP к очереди).
3. Установите флажок **Remove** (Удалить) для каждого из портов UDP, для которых необходимо удалить привязку очереди.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Определение привязки портов UDP к очереди командами консоли

Таблица 10-8. Команды консоли для привязки портов UDP к очереди

Команда консоли	Описание
<code>qos map udp-port-queue порт1 ...порт 8 к идентификатору_очереди</code>	Изменяет привязку порта UDP к очереди.
<code>show qos map [dscp-queue tcp-port-queue udp-port-queue dscp-policed dscp-mutation]</code>	Отображает все привязки для QoS.

Далее приведен пример команд консоли.

```
console(config)# qos map udp-port-queue 68 to 1
```

```
console(config)# exit
```

```
console# show qos map udp-port-queue
```

```
Udp port-queue map:
```

```
Port queue
```

```
-----
```

8000 1

8001 2

Настройка основного режима QoS

На странице **Basic QoS Mode** (Основной режим QoS) приведены ссылки на страницы QoS, на которых настраивается режим доверия и перезапись DSCP. Чтобы открыть страницу **Basic QoS Mode** (Основной режим QoS), выберите **Quality of Service** (Качество обслуживания) → **Basic QoS Mode** (Основной режим QoS) на панели дерева.

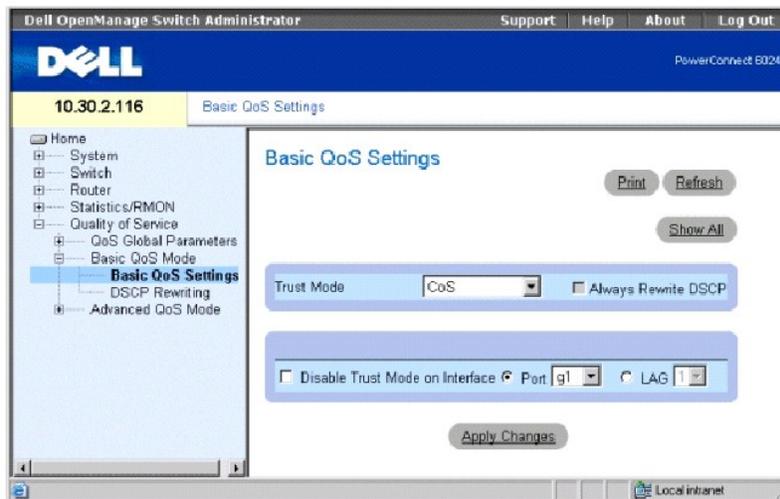
Определение основных параметров основного режима QoS

Для настройки общего режима доверия, который устанавливается для указанных интерфейсов, используйте страницу **Basic QoS Settings** (Параметры основного режима QoS). Пакеты, поступающие в домен QoS, классифицируются на границе домена QoS. При классификации пакетов на границе можно настроить режим доверия для портов.

Значения DSCP можно перезаписать на административной границе домена QoS. Если два домена QoS имеют различные определения DSCP, можно перезаписать значения DSCP. Карта DSCP применяется только для входящих портов, которых настроен режим доверия DSCP.

Чтобы открыть страницу **Basic QoS Settings** (Параметры основного режима QoS), выберите **Quality of Service** (Качество обслуживания) → **Basic QoS Mode** (Основной режим QoS) → **Basic QoS Settings** (Параметры основного режима QoS) на панели дерева.

Рис. 10-10. Страница Basic QoS Settings (Параметры основного режима QoS)



Trust Mode (Режим доверия) - выбирает режим доверия. Если метка CoS, метка DSCP и привязки TCP/UDP пакета сопоставлены с другими очередями, то **Trust Mode** (Режим доверия) определяет очередь, в которую определяется пакет. Возможные значения:

CoS - устанавливает значение CoS для режима доверия на устройстве. Привязка CoS определяет очередь пакетов.

DSCP - устанавливает значение DSCP для режима доверия на устройстве. Привязка DSCP определяет очередь пакетов.

TCP/UDP Port (Порт TCP/UDP) - устанавливает порт TCP/UDP для режима доверия на устройстве. Привязка порта TCP/UDP определяет очередь пакетов.

Always Rewrite DSCP (Всегда перезаписывать DSCP) - перезаписывает метку DSCP пакета в соответствии с настройкой перезаписи DSCP для QoS. Параметр **Always Rewrite DSCP** (Всегда перезаписывать DSCP) можно выбрать только в том случае, если для параметра **Trust Mode** (Режим доверия) установлено значение **DSCP**.

Disable Trust Mode on Interface (Отключить режим доверия для интерфейса) - отключает режим доверия для выбранного порта или группы LAG.

Interface (Интерфейс) - порт или группа LAG, для которого отключен режим доверия.

Установка режима доверия

1. Откройте страницу **Basic QoS Settings** (Параметры основного режима QoS).
2. Выберите **Trust Mode** (Режим доверия).
3. Если для параметра **Trust Mode** (Режим доверия) установлено значение **DSCP**, выберите параметр **Always Rewrite DSCP** (Всегда перезаписывать DSCP), чтобы все метки DSCP перезаписывались как привязанные.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Будет выбран режим доверия, а устройство обновлено.

Отключение режима доверия для интерфейса:

1. Откройте страницу **Basic QoS Settings** (Параметры основного режима QoS).
2. Нажмите кнопку **Show All** (Показать все), чтобы отобразить страницу **Basic QoS Settings Table** (Таблица параметров интерфейса QoS).
3. Выберите параметр **Disable Trust Mode** (Отключить режим доверия) для всех интерфейсов, для которых необходимо отключить режим доверия.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Определение параметров основного режима QoS с помощью команд консоли

Таблица 10-9. Команды консоли для определения параметров основного режима QoS

Команда консоли	Описание
<code>qos trust cos dscp tcp-udp-port</code>	В глобальном контексте эта команда используется для настройки основного режима системы и переключение ее в доверенное состояние.
<code>qos trust</code>	В контексте настройки интерфейса эта команда используется для включения доверенного состояния каждого порта.
<code>qos dscp-mutation</code>	Применяет карту изменений DSCP для доверенного порта DSCP системы (всегда перезаписывает DSCP для этого порта).

Далее приведен пример команд консоли.

```
console(config)# qos trust dscp
```

```
console(config)# qos dscp-mutation
```

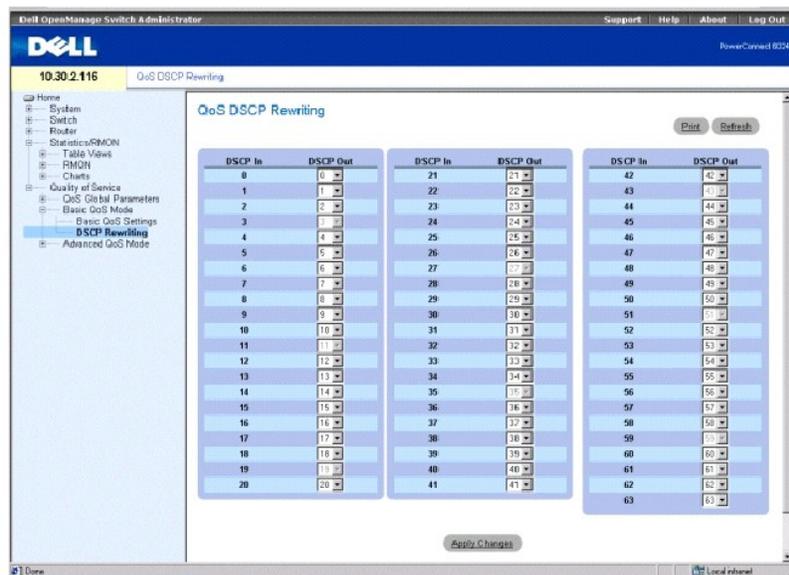
```
Console (config)# interface ethernet g5
```

Console (config-if) qos trust

Определение параметров перезаписи QoS DSCP

Для настройки метода перезаписи меток DSCP используйте страницу QoS DSCP Rewriting (Перезапись DSCP для QoS). Чтобы открыть эту страницу, выберите Quality of Service (Качество обслуживания) → Basic QoS Settings (Параметры основного режима QoS) → DSCP Rewriting (Перезапись DSCP) на панели дерева.

Рис. 10-11. Страница QoS DSCP Rewriting (Перезапись DSCP для QoS)



DSCP In (DSCP входящего пакета) - метка DSCP во входящем пакете.

DSCP Out (DSCP исходящего пакета) - метка DSCP в исходящих пакетах.

Настройка перезаписи DSCP

1. Откройте страницу QoS DSCP Rewriting (Перезапись DSCP для QoS).
2. Для каждой из меток DSCP In (DSCP входящего пакета) выберите значение DSCP Out (DSCP исходящего пакета) в раскрывающемся списке.
3. Нажмите кнопку Apply Changes (Применить изменения).

Перезапись DSCP будет настроена, а устройство обновлено.

Настройка перезаписи DSCP с помощью команд консоли

Таблица 10-10. Команды консоли для настройки перезаписи DSCP

Команда консоли	Описание
	Изменяет карту изменений DSCP в DSCP.

```
qos map dscp- mutation dscp_входящего пакета to dscp_исходящего пакета
```

Далее приведен пример команд консоли для определения карты изменений DSCP:

```
console(config)# qos map dscp-mutation 1 2 4 5 6 to 63
```

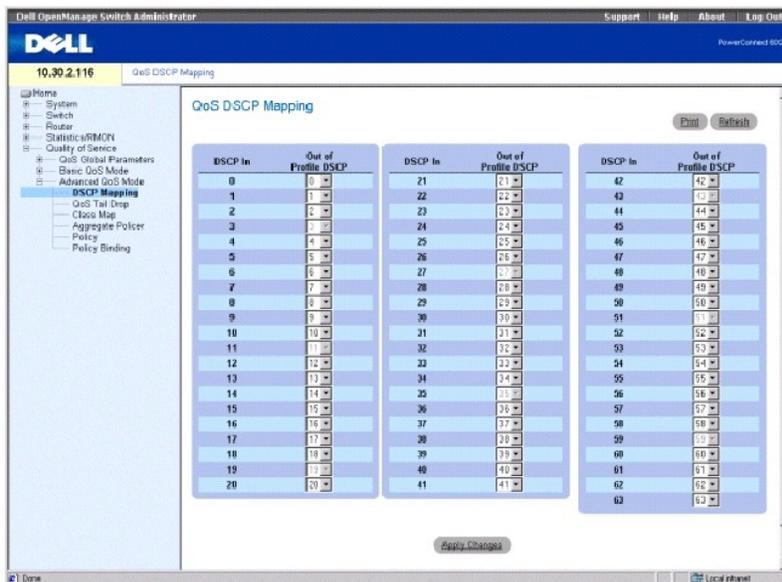
Настройка расширенного режима QoS

На странице **Advanced QoS Mode** (Расширенный режим QoS) приведены ссылки на страницы QoS для настройки расширенных параметров. Чтобы открыть эту страницу, выберите **Quality of Service** (Качество обслуживания) → **Advanced QoS Mode** (Расширенный режим QoS) на панели дерева.

Определение параметров привязки QoS DSCP

Когда трафик превысит ограничения, установленные пользователем, воспользуйтесь страницей **QoS DSCP Mapping** (Привязка QoS DSCP) для настройки метки DSCP, которая должна использоваться вместо меток входящих пакетов DSCP. Чтобы открыть эту страницу, выберите **Quality of Service** (Качество обслуживания) → **Advanced QoS Mode** (Расширенный режим QoS) → **DSCP Mapping** (Привязка DSCP) на панели дерева.

Рис. 10-12. Страница QoS DSCP Mapping (Привязка QoS DSCP)



DSCP In (DSCP входящего пакета) - метка DSCP во входящем пакете.

Out of Profile DSCP (Внепрофильный DSCP) - устанавливает новую метку DSCP для входящей метки.

Настройка привязки DSCP

1. Откройте страницу **QoS DSCP Mapping** (Привязка QoS DSCP).
2. Выберите значение в раскрывающемся меню **Out of Profile DSCP** (Внепрофильный DSCP).

Это значение заменить значение метки DSCP In (DSCP входящего пакета).

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

Привязка DSCP будет настроена, а устройство обновлено.

Настройка привязки DSCP с помощью команд консоли

Таблица 10-11. Команды консоли для привязки DSCP

Команда консоли	Описание
<code>qos map policed- dscp список_dscp to dscp_с_разметкой</code>	Изменяет определенную карту DSCP для повторной маркировки.

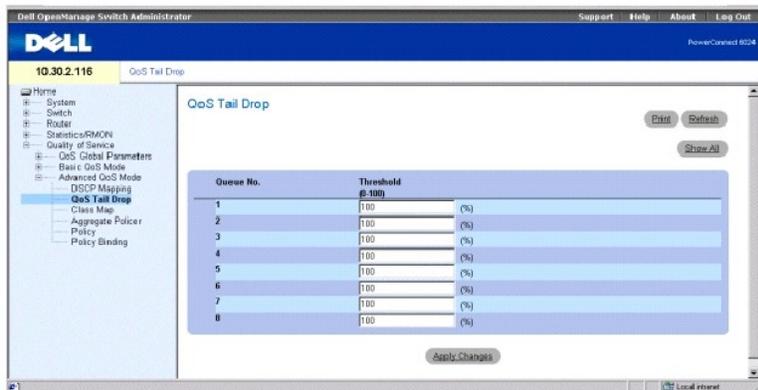
Далее приведен пример команд консоли для сопоставления значений DSCP 12 и 18 значению 56 при попадании за пределы профиля:

```
console(config)# qos map policed-dscp 12 18 to 56
```

Определение параметров отбрасывания конца очереди QoS

Отбрасывание конца очереди возникает при переполнении буфера последовательностью пакетов. Несколько последних пакетов в последовательности отбрасываются вследствие ограниченного места в буфере. Для определения параметров отбрасывания конца очереди для каждой очереди используйте страницу **QoS Tail Drop** (Отбрасывание конца очереди QoS). Чтобы открыть страницу **QoS Tail Drop** (Отбрасывание конца очереди QoS), выберите **Quality of Service** (Качество обслуживания) → **Advanced QoS Mode** (Расширенный режим QoS) → **QoS Tail Drop** (Отбрасывание конца очереди QoS) на панели дерева.

Рис. 10-13. Страница QoS Tail Drop (Отбрасывание конца очереди QoS)



Queue No. (Номер очереди) - указывает очередь, для которой применяются параметры отбрасывания конца очереди.

Threshold (1-100) (Пороговое значение (1-100)) - пороговое значение отбрасывания конца очереди в процентах. При поступлении пакета выполняется сравнение с этим значением и, если оно превышено, пакеты отбрасываются до тех пор, пока снова значение не будет ниже порогового.

Настройка порогового значения отбрасывания конца очереди

1. Откройте страницу **QoS Tail Drop** (Отбрасывание конца очереди QoS).

2. Выберите пороговое значение для каждой очереди.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Будет настроено пороговое значение отбрасывания конца очереди, а устройство обновлено.

Настройка параметров отбрасывания конца очереди для интерфейса

1. Откройте страницу **QoS Tail Drop** (Отбрасывание конца очереди QoS).
2. Нажмите кнопку **Show All** (Показать все), чтобы отобразить страницу **Tail Drop Table** (Отбрасывание конца очереди QoS).
3. Выберите состояние для каждого интерфейса.
4. Нажмите кнопку **Apply Changes** (Применить изменения).
5. Состояние отбрасывания конца очереди будет определено для интерфейсов.

Определение параметров отбрасывания конца очереди QoS с помощью команд консоли

Таблица 10-12. Команды консоли для настройки параметров отбрасывания конца очереди

Команда консоли	Описание
<code>qos wrr-queue threshold идентификатор_очереди пороговое_значение_в_процентах</code>	Присваивает пороговые значения для отбрасывания конца очереди.

Далее приведен пример команд консоли для определения параметров отбрасывания конца очереди:

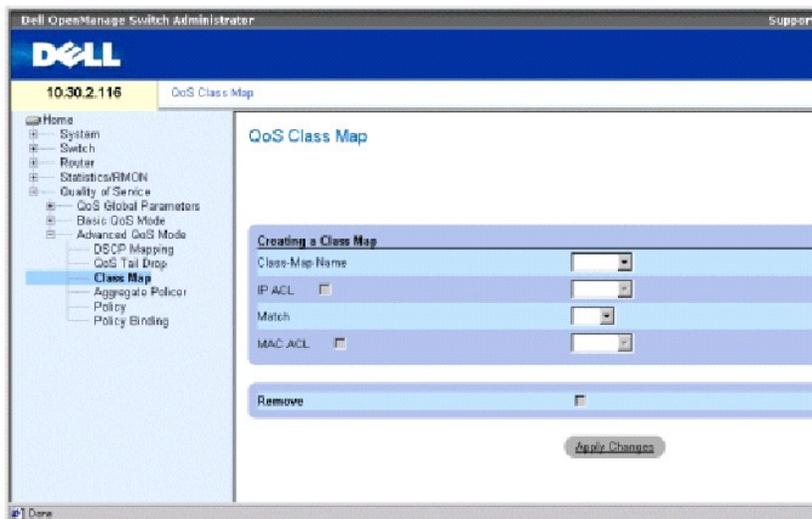
```
console(config)# qos wrr-queue threshold 8 80
```

Определение таблицы классов QoS

Список ACL, основанный на IP-адресах, и список ACL, основанный на MAC-адресах, образуют таблицу классов. Таблицы классов настраиваются в соответствии с критериями пакета и сопоставляются с пакетами на основе схемы первого совпадения. Например, таблица классов A назначается для пакетов на основе только списка ACL, основанного на IP-адресах, или списка ACL, основанного на MAC-адресах. Таблица классов B назначается для пакетов на основе списков ACL, основанных как на IP-, так и на MAC-адресах.

Для определения и редактирования таблицы классов используйте страницу **QoS Class Map** (Таблица классов QoS). Чтобы открыть эту страницу, выберите **Quality of Service (Качество обслуживания) → Advanced QoS Mode (Расширенный режим QoS) → Class Map (Таблица классов)** на панели дерева.

Рис. 10-14. Страница QoS Class Map (Таблица классов QoS)



Class-Map Name (Имя таблицы классов) - определенное пользователем имя таблицы классов.

IP ACL - список ACL на основе IP-адресов из списка управления доступом (ACL) на основе IP. Дополнительную информацию об определении списков ACL на основе IP-адресов см. в разделе [«Определение списков ACL, основанных на IP-адресах»](#).

Match (Соответствие) - критерии используются для сопоставления IP-адресов и/или MAC-адресов с адресом списка ACL. Возможные значения:

And (И) - должно выполняться соответствие как со списком ACL на основе MAC-адреса, так и со списком ACL на основе IP-адреса.

Or (Или) - должно выполняться соответствие как со списком ACL на основе MAC-адреса, так и со списком ACL на основе IP-адреса.

MAC ACL - список MAC ACL из списка управления доступом на основе MAC-адреса. Информацию об определении списков ACL на основе MAC-адресов см. в разделе [«Определение списков ACL, основанных на MAC-адресах»](#).

Remove (Удалить) - когда установлен этот флажок, таблица классов удаляется из таблицы классов.

Добавление таблицы классов

1. Откройте страницу **QoS Class Map** (Таблица классов QoS).
2. Нажмите кнопку **Add** (Добавить), чтобы отобразить страницу **Add a Class-Map** (Добавление таблицы классов).
3. Введите имя таблицы классов (не более 16 символов) в поле **Class-Map Name** (Имя таблицы классов).
4. Выполните одно из следующих действий.
 1. Для подключения списка ACL на основе IP-адресов к таблице классов установите флажок **IP ACL** и выберите список IP ACL в раскрывающемся меню.
 1. Для подключения списка ACL на основе MAC-адресов к таблице классов установите флажок **MAC ACL** и выберите список MAC ACL в раскрывающемся меню.
5. Выберите параметр **And (И)** или **Or (Или)** в раскрывающемся меню **Match** (Соответствие), если установлены оба флажка: **IP ACL** и **MAC ACL**.
6. Нажмите кнопку **Apply Changes** (Применить изменения).

Таблица классов будет создана, а устройство обновлено.

Изменение таблицы классов

1. Откройте страницу **QoS Class Map** (Таблица классов QoS).
2. Выберите таблицу классов в **раскрывающемся** меню **Class-Map Name** (Имя таблицы классов).
3. Измените необходимые поля на этой странице.
4. Нажмите кнопку **Apply Changes** (Применить изменения).
5. Таблица классов будет изменена, а устройство обновлено.

Удаление таблицы классов

1. Откройте страницу **QoS Class Map** (Таблица классов QoS).
2. Выберите таблицу классов в раскрывающемся меню **Class-Map Name** (Имя таблицы классов).
3. Установите флажок **Remove** (Удалить).
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Таблица классов будет удалена, а устройство обновлено.

Отображение таблицы классов

1. Откройте страницу **QoS Class Map** (Таблица классов QoS).
2. Нажмите кнопку **Show All** (Показать все), чтобы отобразить страницу **Class Map Table** (Таблица классов).

Определение таблицы классов QoS с помощью команд консоли

Таблица 10-13. Команды консоли для таблицы классов QoS

Команда консоли	Описание
<code>class-map class-map-name [match-all match-any]</code>	Создает таблицу классов и включает режим ее настройки.
<code>match access-group acl-name</code>	Определяет критерии соответствия для классификации трафика; активна только в режиме настройки таблицы классов.
<code>show class-map [class-map-name]</code>	Отображает все таблицы классов.

Далее приведен пример команд консоли.

```
console(config)# class-map class1 match-all
```

```
console(config-cmap)# match access-group dell
```

```
console(config-cmap)# exit
```

```
console(config)# exit
```

```
console> show class-map class1
```

Class Map match-all class1 (id4)

Определение общих ограничителей скорости QoS

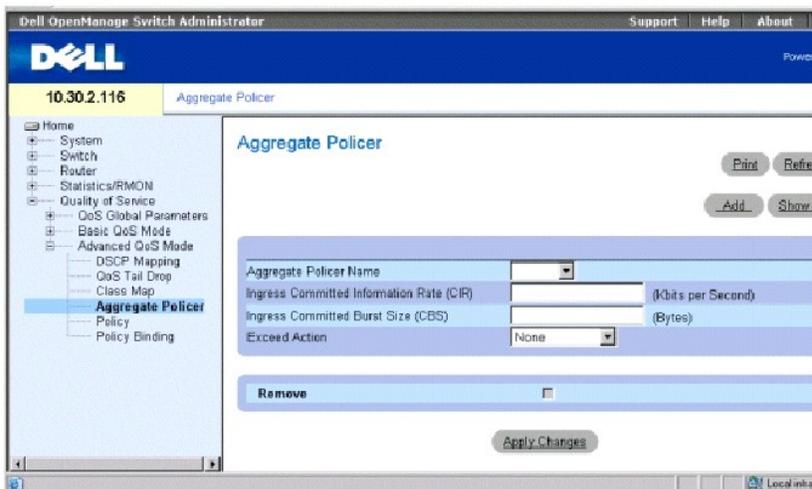
После классификации пакета начинается процесс ограничения скорости. Ограничитель скорости определяет ограничение полосы пропускания для входящего трафика на классифицированном потоке, также определяются действия для пакетов, превышающих эти ограничения. К таким действиям относятся пересылка пакетов, отбрасывание пакетов или повторная пометка пакетов с использованием нового значения DSCP.

Коммутатор поддерживает ограничители скорости для отдельных потоков и общие ограничители.

Общие ограничители устанавливают ограничения на группу потоков. Общий ограничитель скорости нельзя удалить, если он используется в карте политики. Сначала удалите общий ограничитель скорости из всех карт политики с помощью команды `no police aggregate`, прежде чем использовать команду `no qos aggregate-policer`.

Используйте страницу QoS Aggregate Policer (Общий ограничитель скорости QoS) для указания ограничений полосы пропускания и определения действий с пакетами, которые не удовлетворяют требованиям. Чтобы открыть эту страницу, выберите Quality of Service (Качество обслуживания) → Advanced QoS Mode (Расширенный режим QoS) → Aggregate Policer (Общий ограничитель скорости) на панели дерева.

Рис. 10-15. Страница QoS Aggregate Policer (Общий ограничитель скорости QoS)



Aggregate Policer Name (Имя общего ограничителя скорости) - определяет имя общего ограничителя скорости.

Ingress Committed Information Rate (CIR) (Гарантированная скорость передачи данных на входе) - CIR в битах в секунду.

Ingress Committed Burst Size (CBS) (Гарантированный объем данных на входе) - CBS в байтах в секунду.

Exceed Action (Действие при превышении) - назначенное действие в случае превышения ограничений входящим трафиком. Возможные значения:

Drop (Отбросить) - пакеты, превышающие ограничения, отбрасываются.

Remark DSCP (Повторно пометить DSCP) - пакеты, превышающие ограничения, пересылаются повторно или отмечаются с новым значением DSCP.

None (Нет) - пакеты, превышающие ограничение, пересылаются.

Remove (Удалить) - когда установлен этот флажок, общий ограничитель скорости удаляется из Aggregate Policer Table (Таблицы общего ограничителя скорости).

Добавление общего ограничителя скорости

1. Откройте страницу **QoS Aggregate Policer** (Общий ограничитель скорости QoS).
2. Нажмите кнопку **Add** (Добавить), чтобы отобразить страницу **Add Aggregate Policer** (Добавление общего ограничителя скорости).
3. Введите значения в полях диалогового окна и нажмите кнопку **Apply Changes** (Применить изменения).

Будет создан общий ограничитель скорости, а устройство обновлено.

Удаление общего ограничителя скорости

1. Откройте страницу **QoS Aggregate Policer** (Общий ограничитель скорости QoS).
2. Выберите общий ограничитель скорости в раскрывающемся меню.
3. Установите флажок **Remove** (Удалить) и нажмите кнопку **Apply Changes** (Применить изменения).

Общий ограничитель скорости будет удален, а устройство обновлено.

Изменение общего ограничителя скорости

1. Откройте страницу **QoS Aggregate Policer** (Общий ограничитель скорости QoS).
2. Нажмите кнопку **Show All** (Показать все), чтобы отобразить страницу **Aggregate Policer Table** (Таблица общего ограничителя скорости).
3. Измените данные в таблице для необходимых ограничителей скорости.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Определение общих ограничителей скорости с помощью команд консоли

Таблица 10-14. Команды консоли для определения общих ограничителей скорости

Команда консоли	Описание
<code>qos aggregate- policer имя_общего_ограничителя_скорости гарантированная_скорость_бит/с превышение_в_байтах exceed-action {drop policed-dscp- transmit}</code>	Определяет параметры ограничителя скорости, которые можно применить для нескольких классов трафика внутри одной таблицы политики.
<code>show qos aggregate police [имя_общего_ограничителя_скорости]</code>	Отображает параметр общего ограничителя скорости.

Далее приведен пример команд консоли.

```
console# qos aggregate policer policer1 124000 96000 exceed-action drop
```

```
console> show qos aggregate police policer1
```

```
aggregate-policer policer1 96000 4800 exceed-action drop
```

not used by any policy map

Определение политик

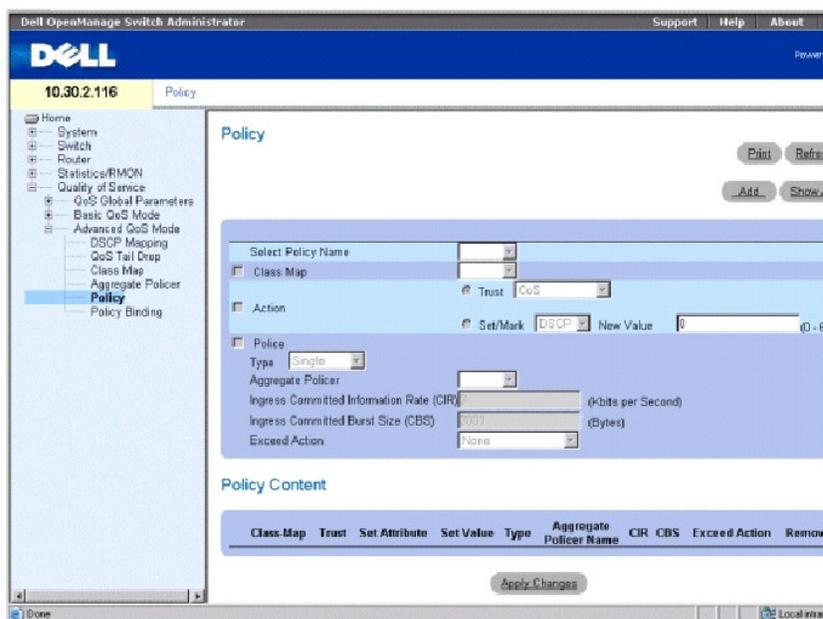
Политика - это совокупность классов, каждый из которых является сочетанием таблицы классов и действия QoS, которое применяется к соответствующему трафику. Классы применяются по методу первого подходящего.

Перед настройкой политик для классов, удовлетворяющих критериям, определенным в таблице классов, необходимо определить таблицу классов или указать таблицу политики, которую необходимо создать, изменить или в которую необходимо добавить эту таблицу. Политики классов можно настраивать в таблице политик только в том случае, если определенные классы удовлетворяют критериям.

Общий ограничитель скорости можно применять для нескольких классов в одной таблице политик, однако, общий ограничитель скорости нельзя использовать для различных карт политик. Общий ограничитель скорости определяется в том случае, если он используется одновременно для нескольких классов. Ограничители скорости на одном порту не могут использоваться вместе с другими ограничителями скорости на другом устройстве. Трафик с двух различных портов можно объединять с целью ограничения скорости.

Чтобы открыть страницу QoS Policy (Политика QoS), выберите Quality of Service (Качество обслуживания) → Advanced QoS Mode (Расширенный режим QoS) → Policy (Политика) на панели дерева.

Рис. 10-16. Страница QoS Policy (Политика QoS)



Select Policy Name (Выбор имени политики) - выбирает имя политики.

Class Map (Таблица классов) - выбирает таблицу классов для классов.

Action (Действие) - дополнительное действие для класса. Возможные значения:

Trust (Доверие) - включает режим доверия для класса. Эта команда используется для определения режима доверия QoS для заданного трафика. Если заданный тип является доверенным, механизм QoS назначает пакет в очередь, используя полученное значение или значение по умолчанию и соответствующую таблицу, как определено на странице QoS Global Parameters (Общие параметры QoS). Выбрав режим доверия, можно определить доверие только входящему трафику с определенными значениями DSCP.

Set/Mark (Задать/пометить) - настройка доверия вручную.

New Value (Новое значение) - значение для выбранного метода **Set/Mark** (Задать/пометить).

Police Type (Тип ограничителя) - тип ограничителя для класса. Возможные значения:

Aggregate (Общий) - настраивает использование для класса определенного общего ограничителя скорости, выбранного в раскрывающемся меню. Общий ограничитель скорости определяется в том случае, если он используется одновременно для нескольких классов. Трафик с двух различных портов можно объединять с целью ограничения скорости. Общий ограничитель скорости можно применять для нескольких классов в одной таблице политик, однако, его нельзя использовать для различных таблиц политик.

Single (Одиночный) - настраивает использование для класса вручную настроенных скоростей передачи данных и действий в случае превышения ограничений.

Aggregate Policer (Общий ограничитель скорости) - определяемые пользователем общие ограничители скорости.

Ingress Committed Information Rate (CIR) (Гарантированная скорость передачи данных на входе) - CIR в битах в секунду. Это поле используется только в том случае, если для параметра **Police** (Ограничитель) указано значение **Single** (Одиночный).

Ingress Committed Burst Size (CBS) (Гарантированный объем данных на входе) - CBS в байтах в секунду. Это поле используется только в том случае, если для параметра **Police** (Ограничитель) указано значение **Single** (Одиночный).

Exceed Action (Действие при превышении) - действие, назначаемое для входящих пакетов при превышении CIR. Это поле используется только в том случае, если для параметра **Police** (Ограничитель) указано значение **Single** (Одиночный). Возможные значения:

Drop (Отбросить) - пакеты, превышающие определенное значение CIR, отбрасываются.

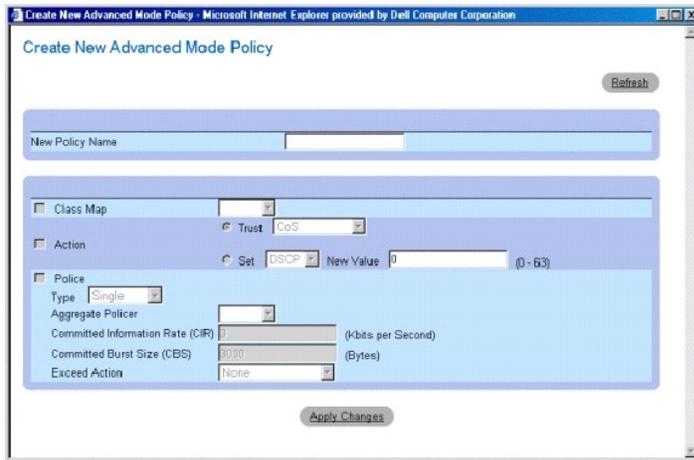
Remark DSCP (Повторно пометить DSCP) - пакеты, превышающие определенное значение CIR, помечаются новым значением DSCP.

None (Нет) - пакеты, превышающие определенное значение CIR, пересылаются.

Добавление политики и ее первого класса

1. Откройте страницу **QoS Policy** (Политика QoS).
2. Нажмите кнопку **Add** (Добавить), чтобы отобразить страницу **Create New Advanced Mode Policy** (Создание новой политики расширенного режима).

Рис. 10-17. Страница Create New Advanced Mode Policy (Создание новой политики расширенного режима)



3. Введите имя для политики в поле **New Policy Name** (Имя новой политики).
4. Выполните одно из следующих действий.
 - 1 Для настройки таблицы для класса щелкните **Class Map** (Таблица классов) и выберите таблицу классов в раскрывающемся меню.
 - 1 Чтобы настроить действие доверия для класса, щелкните **Action** (Действие), выберите **Trust** (Доверие), а затем выберите метод доверия в раскрывающемся меню.
 - 1 Чтобы настроить действия Set/Mark (Задать/пометить), щелкните **Set** (Задать), выберите метод в раскрывающемся меню и введите значение в поле **New Value** (Новое значение).
5. Если требуется настроить ограничение скорости для класса, щелкните **Police** (Ограничитель) и выберите тип ограничения скорости в раскрывающемся меню.
 - 1 Для общего ограничителя скорости выберите общий ограничитель скорости в раскрывающемся меню **Aggregate Policer** (Ограничитель скорости).
 - 1 Для одиночного ограничителя скорости введите данные в полях **Committed Information Rate (CIR)** (Гарантированная скорость передачи данных), **Committed Burst Size (CBS)** (Гарантированный объем данных) и **Exceed Action** (Действие при превышении).
6. Нажмите кнопку **Apply Changes** (Применить изменения).

Будет создана политика и ее первый класс, а устройство обновлено.

Добавление класса

1. Откройте страницу **QoS Policy** (Политика QoS).
2. Выберите политику в раскрывающемся списке.
3. Измените информацию в полях на странице и нажмите кнопку **Apply Changes** (Применить изменения).

Класс будет добавлен в политику, а устройство обновлено.

Удаление политик.

1. Откройте страницу **QoS Policy** (Политика QoS).
2. Нажмите кнопку **Show All** (Показать все), чтобы отобразить страницу **Policy Table** (Таблица политик).
3. Установите флажок **Remove** (Удалить) для каждой политики, которую необходимо удалить, а затем нажмите кнопку **Apply Changes** (Применить изменения).

Политики будут удалены из системы, а устройство обновлено.

Определение политик с помощью команд консоли

Таблица 10-15. Команды консоли для политики

Команда консоли	Описание
<code>policy-map имя_таблицы_политики</code>	Создает таблицу политики и включает режим настройки таблицы политики.
<code>class имя_таблицы_классов [access-group имя_acl]</code>	Определяет классификацию трафика и включает режим настройки таблицы политики класса.
<code>trust [cos dscp tcp-udp-port]</code>	Настраивает состояние доверия, которое выбирает значение, используемое QoS в качестве источника для внутреннего значения DSCP.
<code>set {dscp новое_dscp queue идентификатор_очереди cos новое_cos}</code>	Устанавливает новые значения в IP-пакетах. Примечание. Эта команда и команда <code>trust</code> являются взаимоисключающими.
<code>police гарантированная_скорость_бит/с гарантированная_последовательность_в_байтах [exceed-action {drop policed- dscp- transmit}]</code>	Определяет одиночный ограничитель скорости для классифицируемого трафика.
<code>qos aggregate-policer имя_общего_ограничителя_скорости гарантированная_скорость_бит/с превышение_в_байтах exceed-action {drop policed-dscp-transmit}</code>	Определяет параметры ограничителя скорости, которые можно применить для нескольких классов трафика внутри одной таблицы политики.

Далее приведен пример команд консоли.

```
console(config)# policy map policy1
```

```
console(config-pmap)# class class1 access-group dell
```

```
console(config-pmap)# trust cos
```

```
console(config-pmap)# set dscp 56
```

```
console(config-pmap)# police 124000 96000 exceed-action drop
```

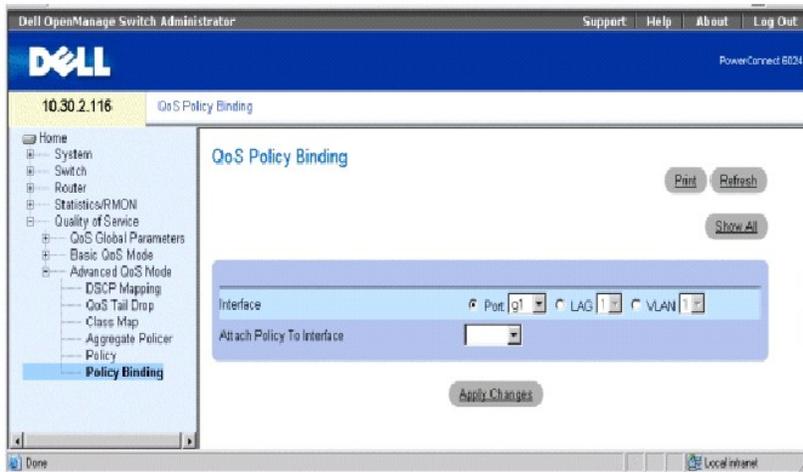
```
console(config-pmap)# exit
```

```
console(config)# qos aggregate-policer policer1 124000 96000 exceed-action drop
```

Определение политики для интерфейса

Используйте страницу [QoS Policy Binding](#) (Привязка политики QoS) для реализации политик для интерфейсов. Чтобы открыть эту страницу, выберите **Quality of Service** (Качество обслуживания) → **Advanced QoS Mode** (Расширенный режим QoS) → **Policy Binding** (Привязка политики) на панели дерева.

Рис. 10-18. Страница QoS Policy Binding (Привязка политики QoS)



Interface (Интерфейс) - выбор интерфейса.

Attach Policy to Interface (Привязка политики к интерфейсу) - привязка политики к интерфейсу.

ПРИМЕЧАНИЕ. Таблица политик, содержащая команду настройки класса set или trust policy-map или имеющая классификацию ACL, которую нельзя добавить для входного интерфейса.

Привязка политики к интерфейсу

1. Откройте страницу **QoS Policy Binding** (Привязка политики QoS).
2. Выберите тип интерфейса.

Для интерфейса поддерживается только одна таблица политики. Однако одна и та же таблица политики может быть назначена для нескольких интерфейсов и направлений.

3. Выберите порт, номер группы LAG или VLAN в соответствующем раскрываемом списке.
4. Выберите политику в раскрываемом меню **Attach Policy to Interface** (Привязка политики к интерфейсу).
5. Нажмите кнопку **Apply Changes** (Применить изменения).

Выбранная политика будет применена для выбранного интерфейса, а устройство обновлено.

Удаление политики из интерфейсов

1. Откройте страницу **QoS Policy Binding** (Привязка политики QoS).
2. Нажмите кнопку **Show All** (Показать все), чтобы отобразить страницу **PTI Reference Table** (Справочная таблица PTI).
3. Установите флажок **Remove** (Удалить) для каждого интерфейса, из которого необходимо удалить политику, и нажмите кнопку **Apply Changes** (Применить изменения).

Политика будет удалена из порта, но останется в системе.

Назначение политики для интерфейсов с помощью команд консоли

Таблица 10-16. Команды консоли для назначения политики для интерфейса

Команда консоли	Описание
-----------------	----------

```
service-policy input имя_таблицы_политики
```

Назначает таблицу политики соответствующему входному или выходному интерфейсу.

Далее приведен пример команд консоли.

```
console(config-if)# service-policy input policy1
```

[Назад на страницу Содержание](#)

Настройка коммутатора

Системы Dell™ PowerConnect™ 6024/6024F

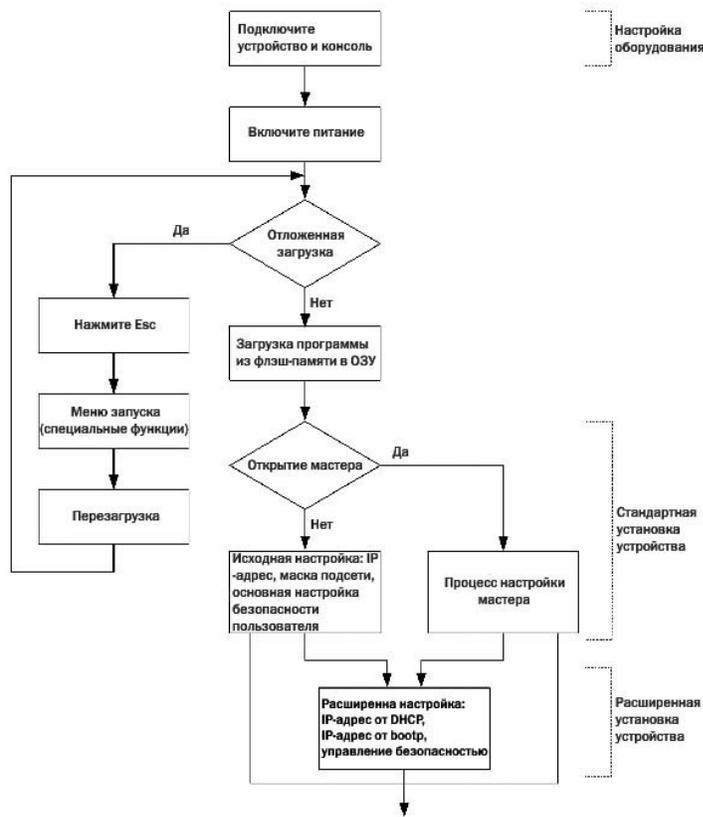
- [Общая информация по настройке](#)
- [Прочие требования к настройке](#)
- [Загрузка коммутатора](#)
- [Обзор настройки](#)
- [Начальная настройка](#)
- [Расширенная настройка](#)
- [Загрузка программного обеспечения и перезагрузка](#)
- [Пример процесса настройки](#)
- [Функции меню Startup \(Запуск\)](#)
- [Порт управления вне диапазона](#)

В этом разделе описывается первоначальная настройка устройства.

После выполнения всех внешних соединений к устройству должен быть подключен терминал для контроля загрузки и других процедур. Порядок процедур установки и настройки показан на [рис. 5-1](#). В качестве начальной настройки выполняется стандартная настройка устройства. Можно выполнить другие функции, однако при этом процесс установки длится дольше и может потребоваться перезагрузка системы. Выполнение других операций описано позже в этом разделе.

🔔 **ВНИМАНИЕ.** Перед дальнейшими действиями прочтите примечания к выпуску для этого продукта. Примечания к выпуску можно загрузить с веб-узла support.dell.com.

Рис. 5-1. Процесс установки и настройки



Общие сведения о настройке

Коммутатор поставляется с предварительно определенными функциями и настройкой.

Автоматическое согласование

Автоматическое согласование позволяет устройству сообщать о режимах работы и обмениваться информацией с другим устройством, которое использует совместно с ним двухточечный сегмент линии связи. При этом оба устройства автоматически настраиваются для наиболее эффективного использования их возможностей.

Автоматическое согласование полностью выполняется на физических уровнях во время установления связи без дополнительной настройки MAC или протоколов более высоких уровней. Автоматическое согласование позволяет портам выполнять следующие действия.

- 1 сообщать о своих характеристиках;
- 1 подтверждать прием и распознавание общих режимов работы, которые используются обоими устройствами;
- 1 отвергать использование режимов работы, которые не являются общими для этих двух устройств;
- 1 настраивать наиболее производительный (из числа поддерживаемых обоими портами) режим работы для каждого порта.

Если порт коммутатора подсоединен к контроллеру сетевого интерфейса (NIC) рабочей станции или сервера, который не поддерживает или не настроен на автосогласование, коммутируемый порт и NIC необходимо настроить вручную с помощью Web-браузера или команд консоли на одинаковую скорость передачи и дуплексный режим.

 **ВНИМАНИЕ.** Если станция на противоположной стороне канала попытается выполнить автосогласование с портом, для которого вручную настроен полнодуплексный режим, то в результате автосогласования вызывающая станция будет переведена в полудуплексный режим. Это несоответствие может привести к существенным потерям кадров. Такие ситуации характерны для стандарта автосогласования.

Настройки по умолчанию для коммутируемых портов

В следующей таблице приведены описания настроек по умолчанию для переключаемых портов.

Таблица 5-1. Настройки порта по умолчанию

Функция	Настройка по умолчанию
Скорость и режим работы порта	1000M Автоматическое согласование
Состояние пересылки пакетов для порта	Включено
Защита от блокировки очереди	On (Включено)
Управление потоком	Выключено
Обратное давление	Выключено

Ниже приведен пример изменения скорости порта g1 с использованием команд консоли:

```
Console(config)# interface ethernet g1

Console (config-if)# speed 100
```

Далее приведен пример включения управления потоком g1 для порта с помощью команд консоли:

```
Console(config)# interface ethernet g1
```

```
Console (config-if)# flowcontrol on
```

Далее приведен пример включения для порта обратного давления g1 с использованием команд консоли. Обратное давление работает только режима работы 10 Мбит/с.

```
Console(config)# interface ethernet g1
```

```
Console (config-if)# speed 10
```

```
Console(config-if)# back pressure (обратное давление)
```

Настройка подключения терминала

Для коммутатора необходимо указать следующие параметры подключения терминала:

- 1 без контроля четности
- 1 1 стоповый бит
- 1 8 битов данных

Скорость передачи данных

Для скоростей передачи может быть задано вручную одно из следующих значений:

- 1 2400
- 1 4800
- 1 9600
- 1 19200
- 1 115200

 **ПРИМЕЧАНИЕ.** Скорость передачи данных по умолчанию: 115200.

 **ПРИМЕЧАНИЕ.** При закрытии устройства не восстанавливается значение скорости передачи по умолчанию. Скорость необходимо специально настроить.

 **ПРИМЕЧАНИЕ.** Скорость передачи, установленная для консоли, не сохраняется в файле общих настроек коммутатора. Она сохраняется непосредственно в постоянной памяти коммутатора.

Далее приведен пример настройки для изменения скорости передачи данных по умолчанию с помощью команд консоли:

```
console# configure
```

```
console(config)# line console
```

```
console(config-line)# speed 11520 0
```

Прочие требования к настройке

Для загрузки встроенного программного обеспечения и настройки устройства необходимы следующие компоненты.

- 1 ASCII-терминал (или его эмуляция), подключенный (с помощью перекрестного кабеля) к последовательному порту на задней панели устройства.
- 1 Назначенный для коммутатора IP-адрес для дистанционного управления коммутатором с помощью Telnet, SSH и т. п.

 **ПРИМЕЧАНИЕ.** Процесс настройки определяет только один порт.

Загрузка коммутатора

При включении питания с подключенным локальным терминалом коммутатор выполняет процедуру проверки при включении питания (POST). Процедура POST выполняется каждый раз при инициализации устройства. Во время этой процедуры выполняется проверка компонентов оборудования и определяется полная работоспособность устройства перед окончательным запуском.

В случае обнаружения критической ошибки, выполнение программы прекращается. В случае успешной проверки POST в память ОЗУ загружается действующий образ исполняемого файла.

На терминале отображаются сообщения POST, которые показывают успешное или неудачное выполнение процедуры.

Чтобы загрузить коммутатор, выполните следующие действия.

1. Убедитесь, что кабель ASCII подсоединен к терминалу.
2. Подсоедините источник питания к коммутатору.
3. Включите питание.

При загрузке коммутатора в ходе выполнения теста определяется объем доступной памяти устройства, а затем продолжается загрузка. Далее приведен пример экрана теста POST:

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

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

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

```
Testing CPU PCI Bus Device Configuration.....PASS
```

```
BOOT Version 1.0.0.13 Date 13-Aug-2003 Time 15:28:31
```

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

Процесс загрузки длится около 30 секунд.

Сообщение автозагрузки, которое появляется в конце процедуры POST (на последних строках), указывает, что при загрузке проблем не обнаружено.

Во время загрузки можно воспользоваться меню **Startup** (Запуск), если необходимо выполнить специальные процедуры. Для входа в меню **Startup** (Запуск) необходимо нажать клавишу <Esc> или <Enter> в течение первых двух секунд после появления сообщения автозагрузки. Информацию о меню **Startup** (Запуск) см. в разделе «[Функции меню Startup \(Запуск\)](#)».

Если не прерывать загрузку системы нажатием клавиши <Esc> или <Enter>, то система продолжит распаковку и загрузку программного кода в ОЗУ. Программный код запускается из оперативной памяти и отображается список доступных системных портов и их состояние (включен или выключен).

 **ПРИМЕЧАНИЕ.** Следующий экран содержит пример настройки. Фактические адреса, номера версий и даты для разных устройств могут отличаться.

Preparing to decompress...

Decompressing SW from image-1

d04000

OK

Running from RAM...

** Running SW Ver. 1.0.1.06 Date 15-Sep-2003 Time 17:48:07 **

HW version is 00.01.64

Base Mac address is: 00:00:b0:16:00:00

Dram size is : 256M bytes

Dram first block size is : 235520K bytes

Dram first PTR is : 0x1800000

Dram second block size is : 1984K bytes

Dram second PTR is : 0xFE00000

Flash size is: 16M

Tuning File info. Ver: 0.2.80 Creation date: Aug 20 2003 11:20:13

PowerConnect 6024

Tapi Version: v1.1a1-P18

Core Version: v1.1a1-P18

18-May-2003 16:24:41 %INIT-I-InitCompleted: Initialization task is completed

Start the sync process between devices 0 - 1

Sync OK

18-May-2003 16:24:41 %Box-W-PS-STAT-CHNG: PS# 1 status changed - not operational

.

18-May-2003 16:24:41 %Box-I-PS-STAT-CHNG: PS# 2 status changed - operational.

18-May-2003 16:24:41 %Box-W-FAN-STAT-CHNG: FAN# 1 status changed - operational.

18-May-2003 16:24:41 %Box-I-FAN-STAT-CHNG: FAN# 2 status changed - operational.

console> 18-May-2003 16:24:41 %DELL-I-STATUS: The product global status has chan

ged from ok to non-critical at time 900.

18-May-2003 16:24:42 %LINK-W-Down: g1

18-May-2003 16:24:42 %LINK-W-Down: g2

После успешной загрузки коммутатора появится системное приглашение (console>), и можно начинать процесс настройки коммутатора с помощью локального терминала. Однако перед настройкой коммутатора необходимо убедиться, что на устройстве установлена последняя версия программного обеспечения. Если установлена не последняя версия, загрузите и установите последнюю версию. См. раздел [«Загрузка программного обеспечения и перезагрузка»](#).

Обзор настройки

Коммутатор поддерживает 10/100 Мбит/с порт управления Ethernet вне диапазона (OOB), который напрямую соединен с устройством. Этот порт поддерживает выполнение задач администратора по управлению системой. Порт вне диапазона обрабатывается как обычный IP-интерфейс для системы, и через него доступны все интерфейсы системы. Порт вне диапазона не поддерживает трафик пользователя. С портов из диапазона (порт Ethernet, отличный от порта вне диапазона) не выполняется коммутация или маршрутизация пакетов на порт вне диапазона.

Перед настройкой устройства необходимо получить у администратора сети следующую информацию:

- 1 IP-адрес порта вне диапазона;
- 1 IP-маска подсети для сети;
- 1 шлюз по умолчанию (маршрутизатор ближайшего узла) - IP-адрес для настройки маршрута по умолчанию.

Существует два типа настройки. При начальной настройке определяются базовые функции конфигурации с основными настройками системы безопасности. При расширенной настройке выполняется настройка динамических IP-адресов и дополнительные параметры системы безопасности.

- 🔔 **ВНИМАНИЕ.** После внесения любых изменений в настройку необходимо сохранить новую настройку перед перезагрузкой устройства. Чтобы сохранить настройку, введите следующую команду:

```
console# copy running-config startup-config
```

Начальная настройка

Выполнять начальную настройку можно с помощью мастера настройки или команд консоли. Если файл настройки устройства пустой, мастер настройки вводится автоматически. Можно активизировать команды консоли, нажав комбинацию клавиш [ctrl+z].

В руководстве дается информация о том, как использовать мастера настройки для начальной настройки устройства. Мастер настройки настраивает следующие поля.

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

По завершении проверки POST и загрузки устройства отобразятся следующие сообщения.

```
Welcome to Dell Easy Setup Wizard
```

```
The Setup Wizard guides you through the initial switch configuration, and gets you up and running easily and quickly. You can also skip the setup wizard, and enter CLI mode to manually configure the switch if you prefer.
```

```
You can exit the Setup Wizard at any time by entering [ctrl+Z].
```

```
The system will prompt you with a default answer; by pressing enter, you accept the default.
```

```
After you configure basic settings using the Setup Wizard, you can manage the device from the Out-of-band management port.
```

```
Would you like to enter the setup wizard? [Y/N] Y
```

1. При вводе [N] мастер настройки закрывается. Если ответа на запрос не будет в течение 60 секунд, мастер настройки закрывается автоматически, и отобразится приглашение консоли. При вводе [Y] мастер настройки будет осуществлять интерактивное руководство начальной настройкой устройства.

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

🔍 **ПРИМЕЧАНИЕ.** Можно в любой момент закрыть мастер настройки, нажав комбинацию клавиш [ctrl+z].

Шаг мастера 1

При вводе [Y] отобразится 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:

- 1 Setup the initial SNMP version 2 account now.
- 1 Return later and setup the SNMP version 2 account. (For more information on setting up a SNMP version 2 account, see the user documentation).

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

2. Введите [N], чтобы пропустить шаг 2, или введите [Y], чтобы продолжить работу мастера настройки. При вводе [Y] отобразятся следующие сообщения.

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 other management interfaces to change this setting later, and to add additional management system later. 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:

Please enter the Management System IP address(A.B.C.D) or wildcard (0.0.0.0) to manage from any Management Station:

3. Введите следующие сведения.
 - o Строку сообщества SNMP пользователя, например «MYSETUPWIZARD»
 - o IP-адрес системы управления, например «0.0.0.0».
4. Нажмите клавишу Enter.

Шаг мастера 2

Отобразится следующее:

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:

Please enter the user name:

Please enter the user password:

Please reenter the user password:

5. Введите следующие сведения.
 - o Имя пользователя, например «admin»
 - o Пароль и подтверждение пароля.

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

6. Нажмите клавишу Enter.

Шаг мастера 3

7. Отобразятся следующие сообщения.

Next, an IP address is setup. The IP address is defined on the OOB port. 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 device IP address(A.B.C.D):

Please enter the IP subnet mask (A.B.C.D or /nn):

8. Введите IP-адрес и IP-маску подсети, например 192.168.1.100, в качестве IP-адреса, а также 255.255.255.0 в качестве IP-маски подсети.

 **ПРИМЕЧАНИЕ.** Каждый элемент IP-адреса должен начинаться с цифры, отличной от 0. Например, IP-адреса 001.100.192.6 и 192.001.10.3 являются недопустимыми.

9. Нажмите клавишу Enter.

Шаг мастера 4

Отобразится следующее:

Finally, setup the default gateway. Please enter the gateway IP address from which this network is reachable (e.g. 192.168.1.1):

10. Введите шлюз по умолчанию.
11. Нажмите клавишу Enter. Отобразятся следующие сообщения (в каждом примере описаны разные параметры).

This is the configuration information that has been collected:

SNMP Interface = MYSETUPWIZARD@0.0.0.0

User Account setup = admin

Password = *****

Management IP address = 192.168.1.100 255.255.255.0

Default Gateway = 192.168.1.1

Шаг мастера 5

Отобразится следующее:

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]

12. Введите [N], чтобы не перезагружать мастер настройки, или введите [Y], чтобы завершить работу мастера настройки. При вводе [Y] отобразятся следующие сообщения.

```
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.
```

Шаг мастера 6

Отобразится приглашение команд консоли.

Теперь можно выполнять управление устройством либо через подключенный порт консоли, который уже подключен, либо удаленно через интерфейс вне диапазона, определенный во время начальной конфигурации.

Расширенная настройка

Этот раздел содержит информацию о динамическом выделении IP-адресов и управлении системой безопасности на основе механизма AAA (authentication, authorization, accounting - проверка подлинности, авторизация и учет).

При настройке/получении IP-адресов с использованием протоколов DHCP и BOOTP от этих серверов передается IP-адрес, а также может передаваться маска подсети и шлюз по умолчанию.

Получение IP-адреса от сервера DHCP

Если для получения IP-адреса используется протокол DHCP, то устройство работает как DHCP-клиент.

Чтобы получить IP-адрес от сервера DHCP, необходимо выполнить следующие действия:

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

```
console# configure
```

```
Console (config)# interface ethernet g 1
```

```
console(config-if)# ip address dhcp hostname <string>
```

```
Console (config-if) # ex it
1 Назначение динамических IP-адресов (для порта вне диапазона)
```

```
console# configure
```

```
console(config)# interface out-of-band-eth
```

```
console(config-oob)# ip address dhcp hostname dell
```

```
console(config-oob)# exit
```

```
console(config)# exit
```

Интерфейс получает IP-адрес автоматически.

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

```
console#show ip interface
```

```
IP Address I/F Type Directed Broadcast
```

```
-----
```

```
100.1.1.1/24 vlan 1 static disable
```

```
OoB ip interfaces
```

```
Gateway IP Address Activity status
```

```
-----
```

```
10.6.12.1 active
```

```
IP Address I/F Type
```

```
-----
```

```
10.6.12.20/24 Oob-eth 1 dhcp
```

 **ПРИМЕЧАНИЕ.** Чтобы получить IP-адрес от сервера DHCP, не нужно удалять настройку устройства.

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

Получение IP-адреса от сервера BOOTP

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

Чтобы получить IP-адрес от сервера BOOTP:

1. Выберите и подсоедините любой порт к серверу BOOTP или к подсети, в которой имеется такой сервер, чтобы получить IP-адрес.
2. В командной строке системы введите команду `delete startup configuration` (удалить конфигурацию запуска), чтобы удалить запускаемую настройку из флэш-памяти.

Устройство перезагружается без настройки и через 60 секунд начинает посылать запросы BOOTP.

Устройство получает IP-адрес автоматически.

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

Этот процесс показан в следующем примере:

```
console> enable

console# delete startup-config

Startup file was deleted

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 для устройства настроен IP-адрес.

Управление системой безопасности и настройка паролей

Безопасность системы обеспечивается механизмом AAA (authentication, authorization, accounting - проверка подлинности, авторизация и учетные записи), который управляет правами доступа и привилегиями пользователей, а также способами администрирования. AAA использует как локальные,

так и удаленные пользовательские базы данных. Шифрование данных производится посредством механизма SSH.

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

Настройка паролей системы безопасности

Можно настроить пароли системы безопасности для следующих служб:

- 1 Console
- 1 Telnet
- 1 SSH
- 1 HTTP
- 1 HTTPS

 **ПРИМЕЧАНИЕ.** Пароли определяются пользователем.

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

Настройка первоначального пароля консоли

Для настройки первоначального пароля консоли 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
```

1 Во время первоначальной регистрации в устройстве через сеанс консоли в ответ на приглашение ввести пароль введите `george`.

1 При установке режима устройства «включено» 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
```

- 1 При первоначальной регистрации в устройстве через сеанс Telnet введите пароль bob.
- 1 При установке режима устройства «включено» введите bob.

Настройка первоначального пароля SSH

Для настройки начального пароля SSH введите следующие команды:

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

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

```
console(config)# line ssh
```

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

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

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

- 1 При первоначальной регистрации в устройстве через сеанс SSH введите пароль jones.
- 1 При установке режима устройства «включено» введите jones.

Настройка первоначального пароля HTTP

Для настройки первоначального пароля HTTP введите следующие команды:

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

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

Настройка первоначального пароля HTTPS:

Для настройки первоначального пароля HTTPS введите следующие команды:

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

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

 **ПРИМЕЧАНИЕ.** При каждом обновлении (установке новой версии) приложения программы управления устройством следует создавать новый сертификат crypto.

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

В программе обозревателя включите отображение на странице данных SSL 2.0 и последующих версий.

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

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

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

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

Загрузка программного обеспечения и перезагрузка

Загрузка программного обеспечения через XModem

В этом разделе содержатся инструкции для загрузки программного обеспечения (системного и загрузочного образа) с помощью XModem, который является протоколом передачи данных для обновления резервных файлов настройки.

Для загрузки загрузочного файла с помощью XModem:

1. Введите команду `console# xmodem: boot`.

Коммутатор готов к приему файлов по протоколу XModem и на экране появится следующий текст:

```
console# copy xmodem: boot
```

```
Please download program using XMODEM.
```

```
console#
```

2. Укажите путь для исходного файла в течение 20 секунд.

Если путь не будет указан в течение 20, истечет время ожидания команды.

Для загрузки файла образа программы с помощью XModem:

1. Введите команду `console# xmodem: image`.

Коммутатор готов к приему файлов по протоколу XModem.

2. Для запуска процесса передачи укажите путь к исходному файлу.

Далее приведен пример отображаемой на экране информации:

```
console# copy xmodem: image
```

```
Please download program using XMODEM.
```

```
console#
```

Загрузка программного обеспечения через сервер TFTP

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

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

При следующей загрузке коммутатор распаковывает и запускает текущий активный образ системы, если не указано иначе.

Для загрузки образа через сервер TFTP:

1. Убедитесь, что IP-адрес настроен для одного из портов устройства, и проверьте соединение с сервером TFTP с помощью команды ping.
2. Убедитесь, что файл, который нужно загрузить, сохранен на сервере TFTP (файл DOS).
3. Чтобы проверить номер версии программного обеспечения, запущенного на устройстве, введите команду `console# show version`.

Далее приведен пример отображаемой на экране информации:

```
console# show version
SW version 3.31.42 (date 22-Jul-2003 time 13:42:41)
Boot version 1.31.03 (date 01-Jun-2003 time 15:12:20)
HW version
```

4. Чтобы узнать, какой образ системы активен, введите команду `console# show bootvar`. Далее приведен пример отображаемой на экране информации:

```
console# show bootvar
Images currently available on the Flash
Image-1 active (selected for next boot)
Image-2 not active
console#
```

5. Чтобы скопировать образ системы на устройство, введите команду `console# copy tftp://{tftp address}/{file name} image`.

При загрузке нового образа он сохраняется в другой области, выделяемой для следующей копии образа системы (image-2, как указано в данном примере). Далее приведен пример отображаемой на экране информации:

```
console# copy tftp://176.215.31.3/file1 image
Accessing file file1 on 176.215.31.3...
```

```
Loading file1 from
176.215.31.3: !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Copy took 00:01:11 [hh:mm:ss]
```

Знаки восклицания указывают, что процесс не завершен. Точка указывает, что истекло время ожидания для процесса копирования. Несколько точек в строке показывают, что возникла ошибка в процессе копирования.

Пример процесса настройки

В этом разделе представлены основные шаги, необходимые для установления удаленного сетевого соединения для администрирования с коммутатором. В этом разделе не поясняются различные возможные настройки коммутатора или соответствующие команды.

В этом разделе также описан первоначальный доступ к коммутатору при заводских настройках и определениях. Если после ранее введенной конфигурации возникают проблемы, то необходимо удалить файл загрузки настройки при включении питания устройства и перезагрузить устройство. См. раздел «[Настройки устройства по умолчанию](#)».

Требования для настройки устройства

Для этого примера необходимы следующие компоненты:

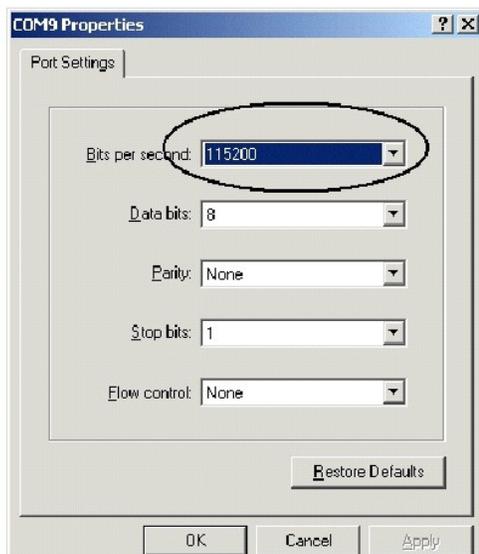
- 1 Коммутатор PowerConnect 6024/6024F
- 1 Рабочая станция, на которой установлены:
 - o сетевой адаптер;
 - o приложение терминала ASCII (например, Microsoft(r) Windows(r) HyperTerminal или Procomm Plus Terminal);
 - o приложение обозревателя.
- 1 Один кабель нуль-модема F2F.
- 1 Кабель (кабели) UTP (категории 5) с прямым или перекрестным соединением

Первоначальное соединение

1. Для подключения коммутатора к рабочей станции используйте порт RS-232.
2. Установите для терминала ASCII следующие параметры и выберите соответствующий COM-порт.

В следующем примере показан экран программы HyperTerminal.

Рис. 5-2. Окно свойств HyperTerminal



ПРИМЕЧАНИЕ. Скорость передачи данных для нового устройства по умолчанию составляет 115200 бод. Устройство может быть настроено на другую скорость передачи. Если использование при скорости передачи 115200 бод изображение терминала устройства не появляется, попробуйте другие установки скорости передачи.

3. Для подключения рабочей станции к коммутатору используйте нуль-модемный кабель F2F.
4. Подключите кабель питания к устройству и включите устройство.

Появится следующий экран.

```
*****
```

```
***** SYSTEM RESET *****
```

```
*****
```

Booting...

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

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

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

```
Testing CPU PCI Bus Configuration.....PASS
```

```
BOOT Version 1.0.0.13 Date 13-Aug-2003 Time 15:28:31
```

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

На этом этапе, если необходимо, можно войти в меню **Startup** (Запуск), чтобы выполнить специальные процедуры. Если не входить в меню **Startup** (Запуск), система продолжает операцию распаковки и загрузки программного кода в ОЗУ. Программный код запускается из оперативной памяти, и отображается список доступных номеров портов и их состояние (включен или выключен).

 **ПРИМЕЧАНИЕ.** Следующий экран содержит пример настройки. Фактические адреса, номера версий и даты для разных устройств могут отличаться.

```
Preparing to decompress...
```

```
Decompressing SW from image-1
```

```
d04000
```

```
OK
```

Running from RAM...

*** Running SW Ver. 1.0.1.06 Date 15-Sep-2003 Time 17:48:07 ***

HW version is 00.01.64

Base Mac address is: 00:00:b0:16:00:00

Dram size is : 256M bytes

Dram first block size is : 235520K bytes

Dram first PTR is : 0x1800000

Dram second block size is : 1984K bytes

Dram second PTR is : 0xFE00000

Flash size is: 16M

Tuning File info. Ver: 0.2.80 Creation date: Aug 20 2003 11:20:13

PowerConnect 6024

Tapi Version: v1.1a1-P18

Core Version: v1.1a1-P18

18-May-2003 16:24:41 %INIT-I-InitCompleted: Initialization task is completed

Start the sync process between devices 0 - 1

Sync OK

18-May-2003 16:24:41 %Box-W-PS-STAT-CHNG: PS# 1 status changed - not operational

.

18-May-2003 16:24:41 %Box-I-PS-STAT-CHNG: PS# 2 status changed - operational.

18-May-2003 16:24:41 %Box-W-FAN-STAT-CHNG: FAN# 1 status changed - operational.

18-May-2003 16:24:41 %Box-I-FAN-STAT-CHNG: FAN# 2 status changed - operational.

console> 18-May-2003 16:24:41 %DELL-I-STATUS: The product global status has chan

ged from ok to non-critical at time 900.

18-May-2003 16:24:42 %LINK-W-Down: g1

18-May-2003 16:24:42 %LINK-W-Down: g2

Устройство готово к настройке.

Настройки устройства по умолчанию

Для восстановления настроек устройства по умолчанию введите команду `delete startup-config` в приглашении привилегированного режима (`#`) и перезагрузите устройство. После перезагрузки устройства для него будут восстановлены настройки по умолчанию.

console>

console> enable

console# delete startup-config

Startup file was deleted

console# reload

This command will reset the whole system and disconnect your current

session. Do you want to continue (y/n) [n]?

y

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

.

.

.

.

Включение удаленного администрирования

1. Введите с консоли команду `enable` (включить), чтобы войти в режим экрана Privileged EXEC, как показано далее:

```
console> enable
```

```
console#
```

2. Подключите станцию управления (ПК) к устройству через один из портов Ethernet или через подключенную к устройству сеть с помощью кабеля CAT5.

В данном примере используется порт g1.

3. Проверьте (на терминале ASCII), что состояние интерфейса изменилось на «up» (включено), а STP находится в состоянии передачи (через 30 секунд), как показано далее:

```
Console#
```

```
01-Jan-2000 01:43:03 %LINK-I-Up: Vlan 1
```

```
01-Jan-2000 01:43:03 %LINK-I-Up: g1
```

```
01-Jan-2000 01:43:34 %STP-I-PORTSTATUS: Port g1: STP status Forwarding
```

4. Введите с консоли команду `config`, чтобы войти в режим экрана Configuration (Настройка), следующим образом:

```
console# config
```

5. Введите с консоли команду `interface vlan`, чтобы войти в режим экрана VLAN Configuration (Настройка VLAN) через VLAN 1 по умолчанию (метка = 1), следующим образом:

```
console(config)#interface vlan 1
```

```
console (config-if)#
```

6. **Задайте IP-адрес для устройства, указав IP-адрес (в этом примере 50.1.1.1) группы VLAN, содержащей интерфейс, который подключен к станции управления. Если станция управления подключена напрямую к интерфейсу, то IP-адрес для VLAN должен иметь ту же подсеть, что и станция управления.**

```
console(config)#
```

```
console(config-if)# ip address 50.1.1.1 225.0.0. 0
```

```
console (config-if) #
```

7. **Если станция управления входит в удаленную сеть и не подключена непосредственно к интерфейсу, настройте статическую маршрутизацию.**

Настроенный IP-адрес должен принадлежать к той же подсети, что и один из IP-интерфейсов устройства. В этом примере статический адрес 50.1.1.100.

```
Console (config-if) # ex it
```

```
console(config)# ip route 0.0.0.0.0.0.0 50.1.1.100
```

```
console(config)#
```

8. **Введите команду ping с коммутатора, чтобы проверить соединение со станцией управления.**

Перед отправкой команды ping для проверки соединения станции управления подождите 30 секунд, чтобы порт перешел в состояние пересылки STP. IP-адрес станции управления (в этом примере) 50.1.1.2:

```
console(config)#
```

```
console(config)# exit
```

```
console# ping 50.1.1. 2
```

```
64 bytes from 50.1.1.2: icmp_seq=1. time=0 ms
```

```
64 bytes from 50.1.1.2: icmp_seq=2. time=0 ms
```

```
64 bytes from 50.1.1.2: icmp_seq=3. time=0 ms
```

```
64 bytes from 50.1.1.2: icmp_seq=4. time=0 ms
```

```
----50.1.1.2 PING Statistics----
```

```
4 packets transmitted, 4 packets received, 0% packet loss
```

```
round-trip (ms) min/avg/max = 0/0/0
```

```
console#
```

9. Определите имя пользователя и пароль для разрешения полного (уровень привилегий 15) доступа к устройству для удаленного пользователя (по протоколу HTTP и HTTPS).

В этом примере имя пользователя «Dell», пароль «Dell» и уровень привилегий 15. Уровень привилегий изменяется от 1 до 15, где 15 - самый высокий уровень. Доступ к веб-интерфейсу предоставляется только на уровне 15.

```
console# config
```

```
console(config)# username Dell password Dell privilege 15
```

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

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

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

```
Generating RSA private key, 1024 bit long modulus
```

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

10. Определите имя пользователя и пароль, чтобы разрешить локальному пользователю доступ к консоли, Telnet или Web-серверу.

В этом примере имя пользователя и пароль «Dell», а уровень привилегий - 15.

```
console(config)# username Dell password Dell privilege 15
```

```
console(config)#
```

```
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 tom
```

```
console(config-line)# exit
```

```
console(config)# line telnet
```

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

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

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

```
console(config-line)# exit
```

```
console(config)# line ssh
```

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

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

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

```
console(config-line)# exit
```

11. Сохраните файл `running-config` в файл `startup-config`.

это позволит сохранить выполненную конфигурацию после перезагрузки устройства.

```
console(config-line)# exit
```

```
console(config)# exit
```

```
console# copy running-config startup-config
```

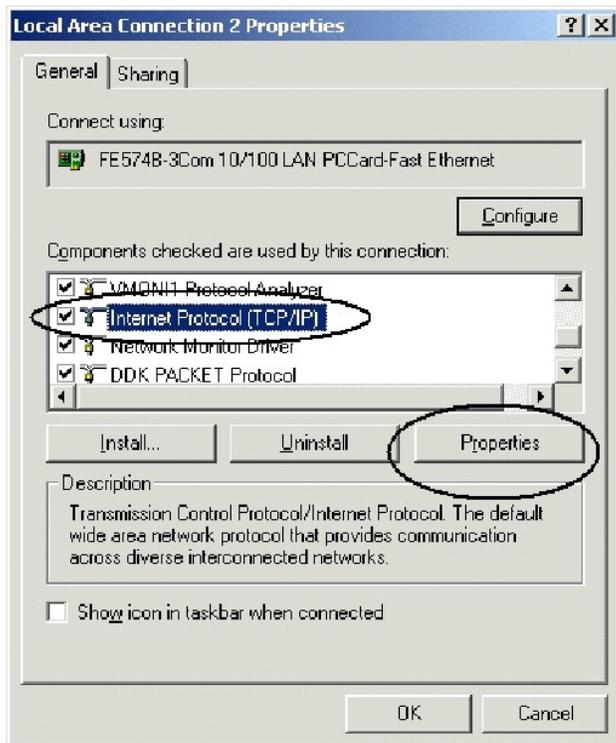
Устройство настроено и может управляться через Telnet, веб-интерфейс и другими способами.

Установка IP-адреса станции управления

1. На станции управления выберите **Start** (Пуск) → **Settings** (Настройка) → **Network and Dial-up Connections** (Сетевые подключения).
2. Щелкните правой кнопкой мыши на сетевом соединении, которое используется для управления, и выберите пункт **Properties** (Свойства).

Появится окно свойств подключения.

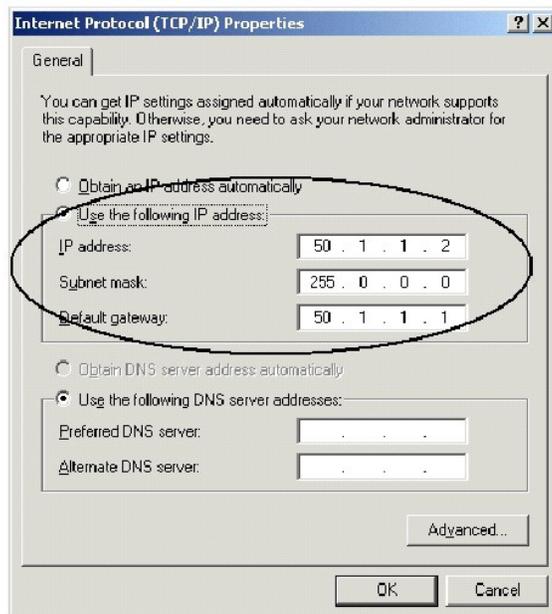
Рис. 5-3. Окно свойств подключения к локальной сети



3. Выберите Internet Protocol (TCP/IP) (Протокол Интернета (TCP/IP)), а затем нажмите кнопку Properties (Свойства).

Появится окно Internet Protocol (TCP/IP) Properties (Свойства протокола Интернета (TCP/IP)).

Рис. 5-4. Окно «Свойства протокола Интернета (TCP/IP)»



4. Выберите Use the following IP address (Использовать следующий IP-адрес).
5. Введите соответствующие адреса для станции управления в полях IP address (IP-адрес), Subnet mask (Маска подсети) и Default gateway (Основной шлюз).

 **ПРИМЕЧАНИЕ.** Если станция управления подключена к маршрутизатору, а не напрямую к коммутатору 6024/6024F, основной шлюз должен соответствовать IP-адресу интерфейса маршрутизатора, подключенного к рабочей станции, который ведет к коммутатору 6024/6024F.

Включение доступа через Telnet

Для доступа к устройству через Telnet используйте режим командной строки Windows/DOS или приложение Telnet. Не забудьте вести соответствующий пароль. Соединение производится с адресом IP, определенным на устройстве.

После предоставления доступа использование команд аналогично непосредственному управлению устройством:

1. На станции управления выберите **Start** (Пуск)→ **Run** (Выполнить).
2. В окне **Run** (Выполнить) введите `cmd` и нажмите кнопку **OK**.

Отобразится стандартный интерфейс командной строки Windows.

3. Введите команду **Telnet** и IP-адрес устройства, как показано далее:

```
Microsoft Windows 2000 [Version 5.00.2195]
```

```
(C) Copyright 1985-2000 Microsoft Corp.
```

```
C:\>telnet 50.1.1.1
```

```
11-Aug-20 03 11:14:06 %MSCM-I-NEWTERM: New TELNET connection from 50.1.1.2
```

```
Password:***
```

```
console> enable
```

```
Password:***
```

```
console#show ip interface
```

```
Proxy ARP is disabled
```

```
IP Address I/F Type Directed Broadcast
```

```
-----
```

```
100.1.1.1/24 vlan 1 static disable
```

```
OOB ip interfaces
```

Gateway IP Address Activity status

10.6.12.1 active

IP Address I/F Type

10.6.12.20/24 Oob-eth 1 dhcp

Коммутатор отобразит состояние сеанса Telnet:

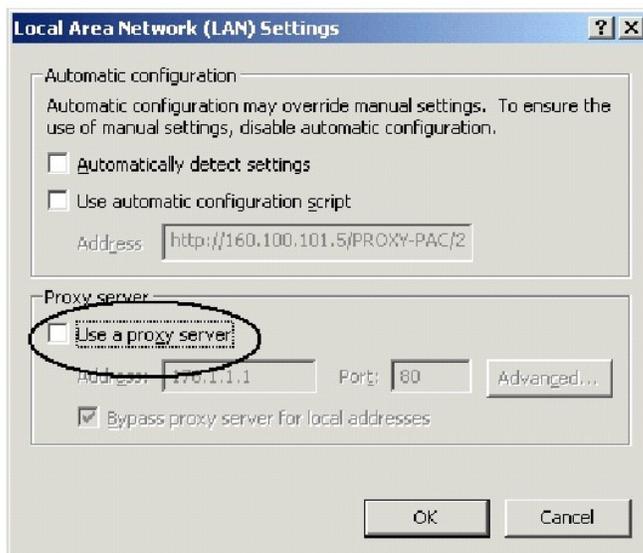
```
console> 01-Jan-2000 02:39:04 %MSCM-I-NEWTERM: New TELNET connection from 50.1.1.2
```

```
01Jan-2000 02:39:11 %MSCM-I-TERMTERMINATED: TELNET connection from 50.1.1.2 terminated
```

Включение доступа через веб-интерфейс (сервер HTTP)

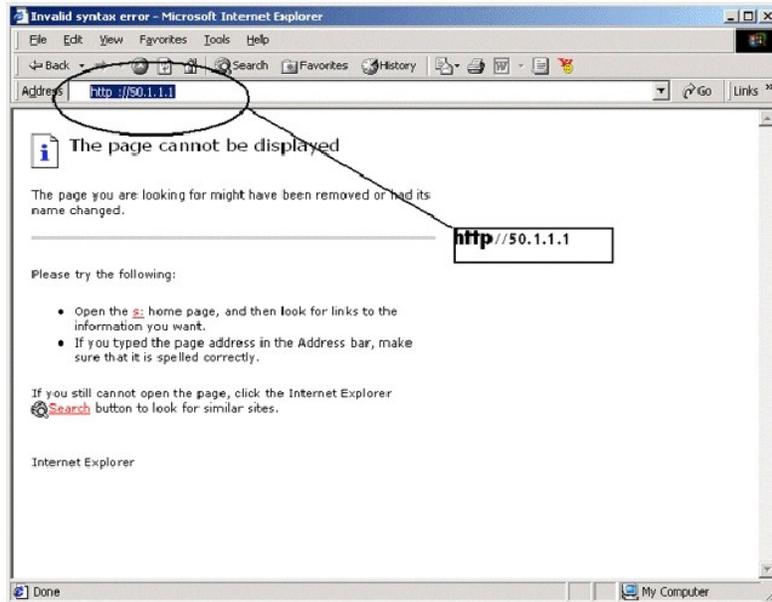
1. Чтобы предотвратить проблемы, которые могут возникать при использовании прокси-сервера HTTP, отключите настройку прокси-сервера (снимите флажок) в обозревателе.
 - a. В Microsoft Internet Explorer выберите **Сервис** → **Свойства обозревателя**.
 - b. Откройте вкладку **Подключение** и нажмите кнопку **Настройка сети**, чтобы открыть окно **Настройка локальной сети**.
 - c. Снимите флажок **Использовать прокси-сервер** и нажмите кнопку **OK**.

Рис 5-5. Окно «Настройка локальной сети»



- d. Нажмите кнопку **OK**, чтобы закрыть окно **Свойства обозревателя**.
2. В окне обозревателя введите IP-адрес, ранее настроенный на устройстве (с префиксом http:// или без него).

Рис 5-6. Вход в веб-интерфейс



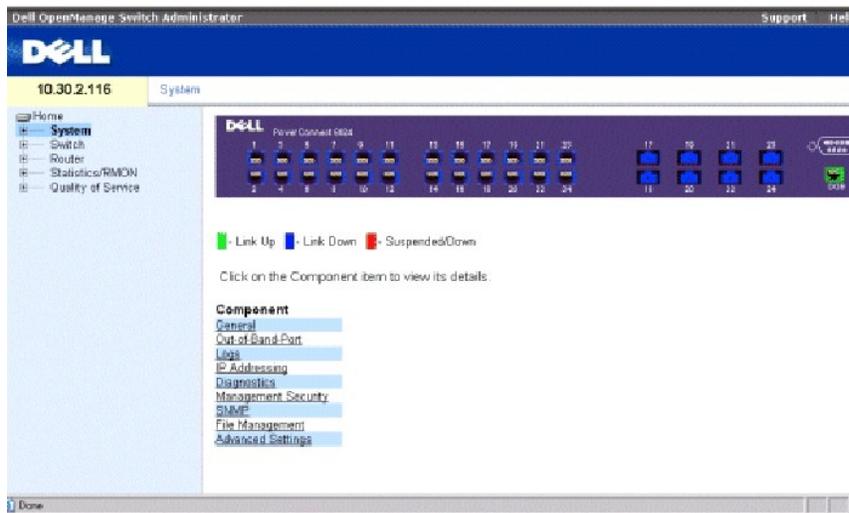
Отобразится окно ввода пароля.

3. Введите имя пользователя и пароль.

Отобразится страница Dell OpenManage Switch Administrator.

ПРИМЕЧАНИЕ. Если пароль не определен, допустим любой пароль.

Рис. 5-7. Страница Dell OpenManage Switch Administrator



Настройка безопасного доступа для управления (HTTPS)

При безопасном управлении с помощью стандартного обозревателя используется протокол безопасного соединения SSL (Secure Socket Layer).

Для безопасного управления устройством с помощью стандартного обозревателя выполните следующие действия:

1. Настройте коммутатор, разрешив использование сервера HTTPS, и создайте ключ защиты, используя команды `ip https server` и `crypto certificate generate key-generate`:

```
console# configure
```

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

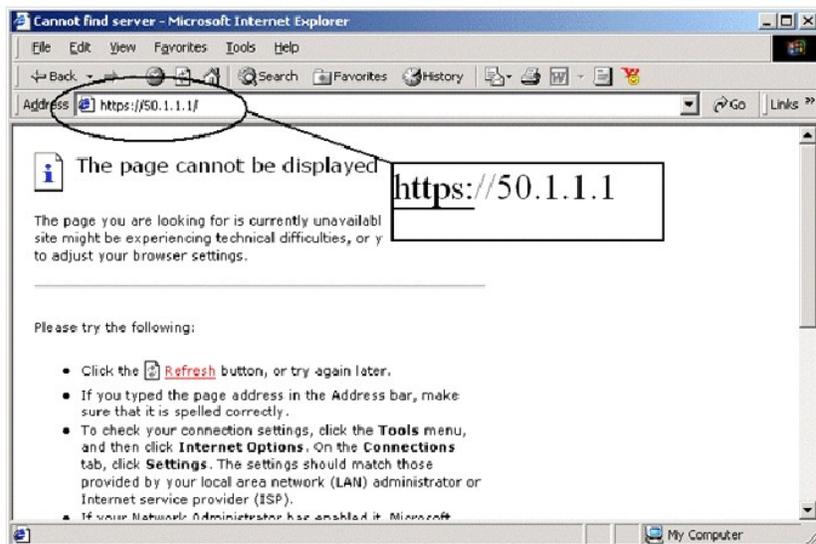
```
console(config)# crypto certificate generate key-generate
```

```
Generating RSA private key, 1024 bit long modulus
```

```
console(config)#
```

2. Настройте станцию управления точно так же, как и для обычного соединения HTTP (см. раздел [»Включение доступа через веб-интерфейс \(сервер HTTP\)»](#)).
3. Установите соединение устройств по протоколу HTTPS, введя адрес `https://<ip-адрес>` устройства в окне обозревателя (необходимо использовать `https`):

Рис. 5-8. Вход в веб-интерфейс с использованием безопасного соединения



Отобразится окно **Предупреждение безопасности**.

4. Нажмите кнопку **Да**, чтобы принять сертификат безопасности (если проверка подлинности не выполняется третьей стороной).
5. Появится окно **Введите пароль доступа** к сети.
6. Введите имя пользователя и пароль.

Отобразится страница Dell OpenManage Switch Administrator для устройства.

Функции меню Startup (Запуск)

В меню Startup можно выполнить дополнительные настройки.

Чтобы отобразить меню Startup (Запуск):

1. Во время процесса загрузки, после завершения первой части POST, нажмите <Esc> или <Enter> в течение первых двух секунд после появления следующего сообщения:

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

Отобразится меню Startup (Запуск), содержащее следующие функции настройки:

```
[1] Download Software (Загрузка программного обеспечения)
```

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

```
[3] Erase Flash Sectors (Удаление данных в секторах флэш-памяти)
```

```
[4] Password Recovery Procedure ((Процедура восстановления пароля))
```

```
[5] Enter Diagnostic Mode (Запуск режима диагностики)
```

```
[6] Back Enter your choice or press 'ESC' to exit: (Введите нужный вариант или нажмите клавишу ESC для закрытия:)
```

В следующих разделах описаны параметры меню Startup (Запуск). Если в течение 25 секунд (по умолчанию) не будет выбран ни один из пунктов меню, истечет время ожидания команды.

Только персонал службы технической поддержки может выполнять операции в режиме Diagnostics (Диагностика). По этой причине параметры пункта Enter Diagnostic Mode (Перейти в режим диагностики) меню Startup (Запуск) не описаны в этом руководстве.

Download Software (Загрузка программного обеспечения)

Используйте этот пункт, когда необходима загрузка новой версии программного обеспечения для замены поврежденных файлов или обновления системного программного обеспечения.

Чтобы загрузить программное обеспечение из меню Startup (Запуск).

1. в меню Startup (Запуск) нажмите <1>.

Отобразится следующая строка:

```
Загрузка кода с помощью XMODEM
```

2. При использовании HyperTerminal нажмите Transfer (Передача) в строке меню HyperTerminal.

3. В меню **Transfer** (Передача) выберите **Send File** (Отправить файл).

Появится окно **Send File** (Отправить файл).

4. Введите путь для файла, который должен быть загружен.
5. Убедитесь, что протокол определен как **Xmodem**.
6. Нажмите кнопку **Send** (Отправить).

Начнется загрузка программного обеспечения. Загрузка программного обеспечения занимает несколько минут. Приложение эмуляции терминала, например **HyperTerminal**, может отображать состояние процесса загрузки.

После загрузки программного обеспечения устройство перезагружается автоматически.

Удаление файла флэш-памяти

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

Чтобы удалить настройку устройства:

1. В меню **Startup** (Запуск) нажмите **<2>** на 6 секунд, чтобы удалить файл флэш-памяти.

Появится следующее сообщение:

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

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

2. Нажмите клавишу **<Y>**.

 **ПРИМЕЧАНИЕ.** Не нажимайте **<Enter>**.

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** в качестве имени файла флэш-памяти.

Настройка удалится, а устройство перезагрузится.

4. Выполните начальную настройку коммутатора.

Удаление данных в секторах флэш-памяти

Для устранения неполадок может потребоваться удалить данные в секторах флэш-памяти. В случае удаления данных во флэш-памяти все файлы программного обеспечения необходимо загрузить и установить заново.

Чтобы удалить данные во флэш-памяти:

1. В меню **Startup** (Запуск) нажмите <3> на 6 секунд.

Появится следующее сообщение:

```
Warning! About to erase Flash Memory! FLASH size = 16252928. blocks = 64 Are you sure (Y/N)
```

2. Подтвердите, нажав <Y>.

Появится следующее сообщение:

```
Enter First flash block (1 - 63):
```

3. Введите первый блок флэш-памяти, который необходимо очистить, и нажмите клавишу <Enter>.

Можно ввести значения от 1 до 64. Появится следующее сообщение:

```
Enter Last flash block (1 - 63):
```

4. Введите последний блок флэш-памяти, который необходимо очистить, и нажмите клавишу <Enter>.
5. Появится следующее сообщение:

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

6. Подтвердите, нажав <Y>.

Появится следующее сообщение:

```
Erasing flash blocks 1 - 63: Done.
```

Восстановление пароля

Если пароль потерян, используйте пункт **Password Recovery** (Восстановление пароля) в меню **Startup** (Запуск). Эта процедура позволяет пользователю один раз войти в устройство без пароля.

Восстановление пароля возможно только с локального терминала:

1. В меню **Startup** (Запуск) выберите **[4]** и нажмите <Enter>.

Пароль будет удален.

2. Чтобы обеспечить безопасность устройства, заново настройте пароли для соответствующих методов управления.

Поддержка порта для управления вне диапазона

Порт управления вне диапазона (OOB) - 10/100 Мбит/с порт Ethernet, который можно использовать для прямого подключения к коммутатору с целью выполнения функций администратора по управлению системой. Порт описывается как обычный IP-интерфейс для системы, и через него доступны все интерфейсы

системы.

Никакие интерфейсы внутри диапазона недоступны через порт OOB. Порт вне диапазона также недоступен ни через один из портов внутри диапазона. Поскольку функции управления сетью можно выполнять с помощью порта вне диапазона, порт вне диапазона следует использовать для выполнения всех функций по управлению сетью, включая веб-администрирование, загрузку/передачу настройку образа и настроек, Telnet; управление SNMP и т.д.

В отличие от портов внутри диапазона, порт вне диапазона не используется для маршрутизации и коммутации. Использование для управления сетью порта OOB вместо порта внутри диапазона гарантирует, что дополнительный 1-гигабитный порт внутри диапазона останется активным для маршрутизации.

В следующих разделах приведены примеры команд OOB.

Назначение динамических IP-адресов (для порта вне диапазона)

```
console#configure
```

```
console(config) #interface out-of-band-eth
```

```
console(config-oob) #ip address dhcp hostname dell
```

```
console(config-oob) #exit
```

```
console(config) #exit
```

```
console#
```

Назначение статических IP-адресов (для порта вне диапазона)

```
console> enable
```

```
console# configure
```

```
console(config) #interface out-of-band-eth
```

```
console(config-oob)#ip address 10.1.1.1 255.0.0.0
```

```
console(config-oob)#exit
```

```
console(config)#ip default-gateway 10.1.1.10
```

```
Console(config)# exit
```

```
console#
```

Назначение IP-адреса для шлюза по умолчанию

```
console>
```

```
console> enable
```

```
console# configure
```

```
console(config) #interface out-of-band-eth
```

```
console(config-oob)#ip address 10.0.0.1 /8
```

```
console(config-oob)#ip default-gateway 10.1.1.1
```

```
console(config-oob)#
```

Проверка соединения путем передачи команды ping через порт вне диапазона

```
console#ping oob/ 10.6.12.25
```

Копирование образа/загрузка

```
copy tftp://oob/10.6.12.25/ves_115.dos image
```

```
copy tftp://oob/10.6.12.25/boot_013.rfb boot
```

Установка для шлюза IP по умолчанию значения вне диапазона

```
console# configure
```

```
console(config)# interface out-of-band-eth
```

```
console(config-oob)#ip default-gateway 10.1.1.10
```

Дополнительная информация

Дополнительную информацию о настройке портов управления вне диапазона см. в разделе «[Настройка портов управления вне диапазона \(OOB\)](#)».

[Назад на страницу Содержание](#)

Получение справки

Системы Dell™ PowerConnect™ 6024/6024F

- [Техническая поддержка](#)
 - [Корпоративное обучение и сертификация Dell](#)
 - [Проблемы с заказом](#)
 - [Информация по продуктам](#)
 - [Возврат изделий для гарантийного ремонта или в счет кредита](#)
 - [Прежде чем позвонить](#)
 - [Обращение в Dell](#)
-

Техническая поддержка

Для получения помощи в решении технических проблем см. инструкции по установке компонентов и поиску, устранению неисправностей в интерактивной справке на веб-узле технической поддержки Dell Support по адресу support.dell.com. Подробнее см. в разделе «Обслуживание, осуществляемое в интерактивном режиме».

Если проблему не удастся решить с помощью обслуживания в интерактивном режиме, обратитесь в Dell по телефону для получения технической поддержки. См. раздел [«Обращение в Dell»](#).

ПРИМЕЧАНИЕ. Позвоните в службу технической поддержки с телефона, расположенного недалеко от системы, чтобы сотрудники службы технической поддержки могли помочь вам с выполнением любых необходимых процедур.

ПРИМЕЧАНИЕ. Система обслуживания клиентов Dell через экспресс-код техобслуживания может быть недоступна в некоторых странах.

Когда автоматическая служба приема звонков Dell выдаст запрос на ввод кода экспресс-обслуживания, введите его, чтобы ваш звонок был переадресован нужному специалисту службы технической поддержки. Если не имеется экспресс-кода техобслуживания, откройте папку Dell Accessories (Сопутствующие средства Dell), дважды щелкните на пиктограмме Express Service Code (Экспресс-код техобслуживания) и далее следуйте инструкциям на экране.

Инструкции по работе со службой технической поддержки см. в разделе [«Техническая поддержка»](#) и [«Прежде чем позвонить»](#).

ПРИМЕЧАНИЕ. Некоторые из этих служб могут быть недоступны за пределами континентальной части США. Информацию о доступных справочных средствах можно получить в местном представительстве корпорации Dell.

Службы в Интернете

Веб-сайт службы технической поддержки Dell находится по адресу: support.euro.dell.com. Чтобы получить доступ к справочной информации и инструментам, на странице WELCOME TO DELL SUPPORT выберите свой регион и укажите необходимые сведения.

Связаться с Dell по электронным каналам связи можно по следующим адресам.

1 Интернет

www.dell.com/

www.dell.com/ap/ (только для стран азиатско-тихоокеанского региона)

www.dell.com/jp (только для Японии)

www.euro.dell.com (только для стран Европы)

www.dell.com/la (только для стран Латинской Америки)

www.dell.ca (только для Канады)

- 1 Анонимный протокол передачи данных (FTP)

ftp.dell.com/

В качестве имени пользователя используйте `user:anonymous`, а в качестве пароля используйте ваш адрес электронной почты.

- 1 Электронная служба поддержки

support@us.dell.com

apsupport@dell.com (только для стран азиатско-тихоокеанского региона)

support.jp.dell.com (только Япония)

support.euro.dell.com (только для стран Европы)

- 1 Электронная служба распространения

sales@dell.com

apmarketing@dell.com (только для стран азиатско-тихоокеанского региона)

sales_canada@dell.com (только для Канады)

- 1 Электронная информационная служба

info@dell.com

Служба AutoTech

Автоматизированная служба технической поддержки компании Dell—AutoTech—предоставляет записанные ответы на наиболее часто задаваемые вопросы клиентов компании по поводу их переносных и настольных компьютеров.

Для звонков в службу AutoTech пользуйтесь телефоном с кнопочным тональным набором, чтобы можно было выбирать темы, связанные с вашими вопросами.

Служба AutoTech работает круглосуточно без выходных. Доступ к ней можно получить также с помощью службы технической поддержки. См. контактную информацию для своего региона.

Автоматическая система отслеживания заказа

Чтобы проверить состояние заказа по продуктам Dell, можно посетить веб-узел support.euro.dell.com или позвонить в автоматическую систему отслеживания заказа. Вам будет задано несколько вопросов, записанных на магнитофонную ленту, чтобы служба могла идентифицировать ваш заказ и выдать информацию о его исполнении. См. контактную информацию для своего региона.

Служба технической поддержки

Служба технической поддержки корпорации Dell доступна для обращения круглосуточно и без выходных. Она дает ответы на вопросы своих клиентов по любым аппаратным средствам Dell. Для предоставления быстрых и точных ответов на вопросы персонал службы технической поддержки использует компьютерную диагностику.

Чтобы обратиться в службу технической поддержки компании Dell, обратитесь к разделу [«Прежде чем позвонить»](#), а затем см. контактную информацию для своего региона.

Корпоративное обучение и сертификация Dell

Информацию о корпоративном обучении и сертификации Dell можно найти в Интернете по адресу www.dell.com/training. Эти услуги могут быть доступны не во всех регионах.

Проблемы с заказом

Если при получении заказа возникают проблемы, например недостающие или незаказанные детали, ошибки в счете и т.д., свяжитесь с корпорацией Dell для их устранения. Во время звонка нужно иметь под рукой свой счет или упаковочный лист. См. контактную информацию для своего региона.

Информация по продуктам

Если потребуется узнать информацию о других продуктах, которые можно приобрести у Dell, или сделать заказ, посетите веб-сайт корпорации Dell по адресу: www.dell.com. Номер телефона, по которому можно связаться со специалистом по продажам, см. в списке контактных номеров для своего региона.

Возврат изделий для гарантийного ремонта или в счет кредита

Прежде чем возвращать изделия для гарантийного ремонта или в счет кредита, выполните следующие действия.

1. Обратитесь в корпорацию Dell, чтобы получить номер разрешения на возврат материала, и запишите его на наружной стороне коробки.

Соответствующий номер телефона см. в разделе контактной информации для своего региона.

2. Вложите в посылку копию счета и письмо с описанием причины возврата изделия.
3. Приложите копию, содержащую диагностическую информацию.
4. Если возврат осуществляется для обмена, приложите все дополнительные принадлежности, относящиеся к возвращаемому изделию (кабели питания, такие носители информации, как компакт-диски и дискеты, руководства и т.п.).
5. Для отправки оборудования используйте оригинальную или аналогичную упаковку.

Доставка производится за счет пользователя. Пользователь также сам должен страховать все возвращаемые изделия и принимать на себя риск потери посылки во время доставки в корпорацию Dell. Пакеты, отправляемые наложенным платежом (C.O.D.), не принимаются.

Изделия, не удовлетворяющие какому-либо из указанных выше требований, не принимаются и будут возвращены отправителю.

Перед тем, как позвонить

ПРИМЕЧАНИЕ. Прежде чем позвонить, подготовьте свой Express Service Code (Экспресс-код техобслуживания). С помощью этого кода автоматическая телефонная служба поддержки сможет быстро соединить вас с нужным специалистом.

Перед звонком в службу технической поддержки Dell следует включить компьютер и во время разговора находиться рядом с ним. Вас могут попросить ввести некоторые команды с клавиатуры, передать подробную информацию о ретрансляции во время выполнения действий или выполнить другие действия для устранения неполадок, которые можно выполнить только в самой компьютерной системе. Документация по системе также должна быть под рукой.

⚠ ПРЕДУПРЕЖДЕНИЕ. Перед обслуживанием любых компонентов внутри компьютера см. *Информационное руководство по системе для ознакомления с важной информацией о безопасности.*

Как связаться с корпорацией Dell

Связаться с Dell по электронным каналам связи можно на следующих веб-сайтах.

- 1 www.dell.com
- 1 support.euro.dell.com (техническая поддержка)
- 1 premiersupport.dell.com (техническая поддержка для образовательных, правительственных и медицинских учреждений, среднего и крупного бизнеса, включая клиентов категории Premier, Platinum и Gold)

Веб-адреса для вашей страны содержатся в соответствующем разделе таблицы.

ПРИМЕЧАНИЕ. Бесплатные номера предназначены для использования только в тех странах, для которых они указаны.

Для обращения в корпорацию Dell пользуйтесь электронными адресами, кодами и телефонами, указанными в таблице. Чтобы выяснить, какие коды следует использовать, обратитесь к оператору местной или международной телефонной службы.

Страна (город) Код международного доступа и код страны Код города	Название отделения или регион обслуживания, веб-сайт и адрес электронной почты	Региональные коды, местные номера и бесплатные номера
Австралия (Сидней) Код выхода на международную линию: 0011 Код страны: 61 Код города: 2	Электронная почта (Австралия): au_tech_support@dell.com	
	Электронная почта (Новая Зеландия): nz_tech_support@dell.com	
	Малые предприятия и ИЧП	1-300-65-55-33
	Правительственные заказы и бизнес	бесплатно: 1-800-633-559
	Отдел привилегированных клиентов (ОПК)	бесплатно: 1-800-060-889
	Обслуживание клиентов	бесплатно: 1-800-819-339
	Отдел продаж для крупных предприятий	бесплатно: 1-800-808-385
	Отдел торговых операций	бесплатно: 1-800-808-312
Факс	бесплатно: 1-800-818-341	
Австрия (Вена) Код выхода на международную линию: 900 Код страны: 43 Код города: 1	Веб-узел: support.euro.dell.com	
	Электронная почта: tech_support_central_europe@dell.com	
	Отдел продаж для домашних пользователей/малых предприятий	0820 240 530 00
	Факс для домашних пользователей/малых предприятий	0820 240 530 49
	Отдел обслуживания домашних пользователей/малых предприятий	0820 240 530 14
	Работа с клиентами для привилегированных счетов/корпоративных клиентов	0820 240 530 16
	Техническая поддержка для малых предприятий	0820 240 530 14
	Привилегированные клиенты/корпорации: техническая поддержка	0660 8779
Коммутатор	0820 240 530 00	
Антигуа и Барбуда	Отдел поддержки по общим вопросам	1-800-805-5924
Ангилла	Отдел поддержки по общим вопросам	бесплатно: 800-335-0031
Антильские острова	Отдел поддержки по общим вопросам	001-800-882-1519
Аргентина (Буэнос-Айрес) Код выхода на международную линию: 00 Код страны: 54	Веб-узел: www.dell.com.ar	
	Отдел технической поддержки и обслуживания клиентов	бесплатный номер: 0-800-444-0733
	Отдел продаж	0-810-444-3355
	Факс отдела технической поддержки	11 4515 7139

Код города: 11	Факс отдела обслуживания	11 4515 7138
Аруба	Отдел поддержки по общим вопросам	бесплатно:800 -1578
Багамы	Отдел поддержки по общим вопросам	бесплатно: 1-866-278-6818
Барбадос	Отдел поддержки по общим вопросам	1-800-534-3066
Бельгия (Брюссель)	Веб-узел: support.euro.dell.com	
Код выхода на международную линию: 00	Электронная почта: tech_be@dell.com	
Код страны: 32	Электронная почта для переписки на французском языке: support.euro.dell.com/be/fr/emaiddell/	
Код города: 2	Техническая поддержка	02 481 92 88
	Обслуживание клиентов	02 481 91 19
	Отдел продаж для крупных предприятий	02 481 91 00
	Факс	02 481 92 99
	Коммутатор	02 481 91 00
Бермудские о-ва	Отдел поддержки по общим вопросам	1-800-342-0671
Боливия	Отдел поддержки по общим вопросам	бесплатно:800-10-0238
Бразилия	Веб-узел: www.dell.com/br	
Код выхода на международную линию: 00	Поддержка покупателей и техническая поддержка	0800 90 3355
Код страны: 55	Факс отдела технической поддержки	51 481 5470
Код города: 51	Факс отдела обслуживания	51 481 5480
	Отдел продаж	0800 90 3390
Бруней	Техническая поддержка клиентов (Пенанг, Малайзия)	604 633 4966
Код страны: 673	Обслуживание клиентов (Пенанг, Малайзия)	604 633 4949
	Сделки по продаже (Пенанг, Малайзия)	604 633 4955
Великобритания (Брэнкнелл)	Веб-узел: support.euro.dell.com	
Код выхода на международную линию: 00	Веб-узел по обслуживанию пользователей: support.euro.dell.com/uk/en/ECare/Form/Home.asp	
Код страны: 44	Электронная почта: dell_direct_support@dell.com	
Код города: 1344	Техническая поддержка (корпоративные/привилегированные клиенты/ОПК [более 1000 сотрудников])	0870 908 0500
	Техническая поддержка (непосредственная поддержка/ОПК и поддержка по общим вопросам)	0870 908 0800
	Глобальные клиенты: обслуживание покупателей	01344 373 186
	Отдел обслуживания домашних пользователей и малых предприятий	0870 906 0010
	Поддержка корпоративных клиентов	01344 373 185
	Привилегированные клиенты (500-5000 сотрудников): обслуживание покупателей	0870 906 0010
	Отдел обслуживания центрального правительства	01344 373 193
	Отдел обслуживания местных органов управления и образования	01344 373 199
	Отдел обслуживания медицинских учреждений	01344 373 194
	Отдел продаж для домашних пользователей и малых предприятий	0870 907 4000
	Отдел продаж корпоративного/государственного сектора	01344 860 456
	Факс отдела по работе с домашними пользователями и малыми предприятиями	0870 907 4006
Венесуэла	Отдел поддержки по общим вопросам	8001-3605
Виргинские о-ва (Великобритания)	Отдел поддержки по общим вопросам	бесплатно: 1-866-278-6820
Виргинские о-ва (США)	Отдел поддержки по общим вопросам	1-877-673-3355
Гайана	Отдел поддержки по общим вопросам	бесплатно: 1-877-270-4609
Гватемала	Отдел поддержки по общим вопросам	1-800-999-0136
Германия (Ланген)	Веб-узел: support.euro.dell.com	
Код выхода на международную линию: 00	Электронная почта: tech_support_central_europe@dell.com	
Код страны: 49	Техническая поддержка	06103 766-7200
Код города: 6103	Отдел обслуживания домашних пользователей/малых предприятий	0180-5-224400
	Отдел обслуживания клиентов в глобальных масштабах	06103 766-9570
	Привилегированные клиенты: обслуживание покупателей	06103 766-9420
	Привилегированные клиенты: обслуживание покупателей	06103 766-9560
	Клиенты-бюджетники: обслуживание покупателей	06103 766-9555
	Коммутатор	06103 766-7000
Гонконг	Веб-узел: support.ap.dell.com	
Код выхода на международную линию: 001	Электронная почта: ap_support@dell.com	
	Техническая поддержка (Dimension™ и Inspiron™)	2969 3189

Код страны: 852	Техническая поддержка (OptiPlex™, Latitude™ и Dell Precision™)	2969 3191
	Техническая поддержка (PowerApp™ и PowerVault™)	2969 3196
	Горячая линия Gold Queue EEC	2969 3187
	Отдел защиты потребителей	3416 0910
	Крупные корпоративные клиенты	3416 0907
	Программы обслуживания клиентов во всем мире	3416 0908
	Отдел по работе со средними предприятиями	3416 0912
	Отдел по работе с домашними пользователями и малыми предприятиями	2969 3105
Гренада	Отдел поддержки по общим вопросам	бесплатно: 1-866-540-3355
Код выхода на международную линию: 00 Код страны: 30	Греция Веб-узел: support.euro.dell.com	
	Электронная почта: support.euro.dell.com/gr/en/emalldell/	
	Техническая поддержка	080044149518
	Техническая поддержка клиентов из категории Gold	08844140083
	Коммутатор	2108129800
	Отдел продаж	2108129800
	Факс	2108129812
Код выхода на международную линию: 00 Код страны: 45	Дания (Копенгаген) Веб-узел: support.euro.dell.com	
	Отдел поддержки по электронной почте (переносные компьютеры): den_nbk_support@dell.com	
	Отдел поддержки по электронной почте (настольные компьютеры): den_support@dell.com	
	Эл. почта для поддержки серверов: Nordic_server_support@dell.com	
	Техническая поддержка	7023 0182
	Отдел обслуживания клиентов (сопутствующее)	7023 0184
	Отдел обслуживания домашних пользователей/малых предприятий	3287 5505
	Коммутатор (сопутствующее обслуживание)	3287 1200
	Факс-коммутатор (сопутствующее обслуживание)	3287 1201
	Коммутатор для домашних пользователей и малых предприятий	3287 5000
Факс-коммутатор (домашние пользователи/малые предприятия)	3287 5001	
Доминика	Отдел поддержки по общим вопросам	бесплатно: 1-866-278-6821
Доминиканская Республика	Отдел поддержки по общим вопросам	1-800-148-0530
Каймановы о-ва	Отдел поддержки по общим вопросам	1-800-805-7541
Код выхода на международную линию: 011	Канада (Норт-Йорк, Онтарио) Состояние интерактивного заказа: www.dell.ca/ostatus	
	Автоматическая служба технической поддержки AutoTech	бесплатно: 1-800-247-9362
	Служба TechFax	бесплатно: 1-800-950-1329
	Обслуживание домашних пользователей и малых предприятий	бесплатно: 1-800-847-4096
	Обслуживание средних и крупных предприятий, государственных учреждений	бесплатно: 1-800-326-9463
	Техническая поддержка для домашних пользователей и малых предприятий	бесплатно: 1-800-847-4096
	Техническая поддержка для средних и крупных предприятий, государственных учреждений	бесплатно: 1-800-387-5757
	Отдел продаж для домашних пользователей и малых предприятий	бесплатно: 1-800-387-5752
	Отдел продаж для средних и крупных предприятий, государственных учреждений	бесплатно: 1-800-387-5755
	Отдел продаж запасных частей и отдел оказания дополнительных услуг	1 866 440 3355
Код страны: 86 Код города: 592	Китай (Сямынь) Веб-узел технической поддержки: support.ap.dell.com/china	
	Адрес электронной почты отдела технической поддержки: cn_support@dell.com	
	Факс отдела технической поддержки	818 1350
	Техническая поддержка для домашних пользователей и малых предприятий	бесплатно: 800 858 2437
	Корпоративные клиенты: техническая поддержка	бесплатно: 800 858 2333
	Отдел работы с клиентами	бесплатно: 800 858 2060
	Малые предприятия и ИЧП	бесплатно: 800 858 2222
	Отдел привилегированных клиентов	бесплатно: 800 858 2557
	Крупные корпоративные клиенты: GCP	бесплатно: 8008582055
	Крупные корпоративные клиенты: ключевые клиенты	бесплатно: 800 858 2628
	Крупные корпоративные клиенты, север	бесплатно: 800 858 2999
	Крупные корпоративные клиенты: правительственные организации и образовательные учреждения, север	бесплатно: 800 858 2955
	Крупные корпоративные клиенты: восток	бесплатно: 800 858 2020
	Крупные корпоративные клиенты: правительственные организации и образовательные учреждения, восток	бесплатно: 800 858 2669
	Крупные корпоративные клиенты: группа очередников	бесплатно: 800 858 2222

	Крупные корпоративные клиенты, юг	бесплатно: 800 858 2355
	Крупные корпоративные клиенты: запад	бесплатно: 800 858 2811
	Крупные корпоративные клиенты: комплектующие	бесплатно: 800 858 2621
Колумбия	Отдел поддержки по общим вопросам	980-9-15-3978
Коста-Рика	Отдел поддержки по общим вопросам	0800-012-0435
Индия	Техническая поддержка	1600 33 8045
	Отдел продаж	1600 33 8044
Ирландия (Черривуд) Код выхода на международную линию: 16 Код страны: 353 Код города: 1	Веб-узел: support.euro.dell.com	
	Электронная почта: dell_direct_support@dell.com	
	Техническая поддержка	1850 543 543
	Техническая поддержка в Великобритании (звонок только из Великобритании)	0870 908 0800
	Отдел обслуживания домашних пользователей	01 204 4014
	Отдел обслуживания малых предприятий	01 204 4014
	Отдел обслуживания клиентов в Великобритании (звонок только из Великобритании)	0870 906 0010
	Поддержка корпоративных клиентов	1850 200 982
	Отдел обслуживания корпоративных клиентов (звонок только из Великобритании)	0870 907 4499
	Отдел продаж в Ирландии	01 204 4444
	Отдел продаж в Великобритании (звонок только из Великобритании)	0870 907 4000
	Факс/Факс отдела продаж	01 204 0103
	Коммутатор	01 204 4444
Испания (Мадрид) Код выхода на международную линию: 00 Код страны: 34 Код города: 91	Веб-узел: support.euro.dell.com	
	Электронная почта: support.euro.dell.com/es/es/emaildell/	
	Домашние пользователи и малые предприятия	
	Техническая поддержка	902 100 130
	Отдел обслуживания клиентов	902 118 540
	Отдел продаж	902 118 541
	Коммутатор	902 118 541
	Факс	902 118 539
	Работа с корпоративными клиентами	
	Техническая поддержка	902 100 130
	Отдел обслуживания клиентов	902 118 546
	Коммутатор	91 722 92 00
	Факс	91 722 95 83
Италия (Милан) Код выхода на международную линию: 00 Код страны: 39 Код города: 02	Веб-узел: support.euro.dell.com	
	Электронная почта: support.euro.dell.com/it/it/emaildell/	
	Домашние пользователи и малые предприятия	
	Техническая поддержка	02 577 826 90
	Обслуживание клиентов	02 696 821 14
	Факс	02 696 821 13
	Коммутатор	02 696 821 12
	Работа с корпоративными клиентами	
	Техническая поддержка	02 577 826 90
	Обслуживание клиентов	02 577 825 55
	Факс	02 575 035 30
	Коммутатор	02 577 821
	Корея (Сеул) Код выхода на международную линию: 001 Код страны: 82 Код города: 2	Техническая поддержка
Отдел продаж		бесплатно: 080-200-3600
Отдел обслуживания клиентов (Сеул, Корея)		бесплатно: 080-200-3800
Отдел обслуживания клиентов (Пинанг, Малайзия)		604 633 4949
Факс		2194-6202
Коммутатор		2194-6000
Латинская Америка	Техническая поддержка покупателей (Остин, Техас, США)	512 728-4093
	Отдел обслуживания клиентов (Остин, Техас, США)	512 728-3619
	Факс (техническая поддержка и обслуживание покупателей) (Остин, Техас, США)	512 728-3883
	Отдел продаж (Остин, Техас, США)	512 728-4397
	Факс отдела продаж (Остин, Техас, США)	512 728-4600
		или 512 728-3772

Люксембург	Веб-узел: support.euro.dell.com		
Код выхода на международную линию: 00 Код страны: 352	Электронная почта: tech_be@dell.com		
	Техническая поддержка (Брюссель, Бельгия)	3420808075	
	Отдел продаж для домашних пользователей/малых предприятий (Брюссель, Бельгия)	бесплатно: 080016884	
	Отдел продаж для крупных предприятий (Брюссель, Бельгия)	02 481 91 00	
	Отдел обслуживания клиентов (Брюссель, Бельгия)	02 481 91 19	
	Факс (Брюссель, Бельгия)	02 481 92 99	
	Коммутатор (Брюссель, Бельгия)	02 481 91 00	
Макао	Техническая поддержка	бесплатно: 0800 582	
Код страны: 853	Отдел обслуживания клиентов (Пинанг, Малайзия)	604 633 4949	
	Сделки по продаже	бесплатно: 0800 581	
Малайзия (Пинанг)	Техническая поддержка	бесплатно: 1 800 888 298	
Код выхода на международную линию: 00 Код страны: 60	Отдел обслуживания клиентов	04 633 4949	
	Сделки по продаже	бесплатно: 1 800 888 202	
Код города: 4	Отдел продаж для крупных предприятий	бесплатно: 1 800 888 213	
Мексика	Техническая поддержка клиента	001-877-384-8979 или 001-877-269-3383	
Код выхода на международную линию: 00 Код страны: 52	Отдел продаж	50-81-8800 или 01-800-888-3355	
	Отдел обслуживания клиентов	001-877-384-8979 или 001-877-269-3383	
	Основной	50-81-8800 или 01-800-888-3355	
Монсеррат	Отдел поддержки по общим вопросам	бесплатно: 1-866-278-6822	
Нидерланды (Амстердам)	Веб-узел: support.euro.dell.com		
Код выхода на международную линию: 00 Код страны: 31 Код города: 20	Эл. почта (техническая поддержка): (Для предприятий): nl_server_support@dell.com (Latitude): nl_latitude_support@dell.com (Inspiron): nl_inspiron_support@dell.com (Dimension): nl_dimension_support@dell.com (OptiPlex): nl_optiplex_support@dell.com (Dell Precision): nl_workstation_support@dell.com		
	Техническая поддержка	020 674 45 00	
	Техническая поддержка: факс	020 674 47 66	
	Отдел обслуживания домашних пользователей/малых предприятий	020 674 42 00	
	Отдел обслуживания клиентов (сопутствующее)	020 674 4325	
	Отдел продаж для домашних пользователей/малых предприятий	020 674 55 00	
	Отдел сопутствующих продаж	020 674 50 00	
	Факс отдела продаж для домашних пользователей/малых предприятий	020 674 47 75	
	Факс отдела продаж	020 674 47 50	
	Коммутатор	020 674 50 00	
	Факс коммутатора	020 674 47 50	
	Никарагуа	Отдел поддержки по общим вопросам	001-800-220-1006
	Новая Зеландия	Электронная почта (Новая Зеландия): nz_tech_support@dell.com	
	Код выхода на международную линию: 00 Код страны: 64	Электронная почта (Австралия): au_tech_support@dell.com	
Домашние пользователи и малые предприятия		0800 446 255	
Правительственные заказы и бизнес		0800 444 617	
Отдел продаж		0800 441 567	
	Факс	0800 441 566	
Норвегия (Люсакер)	Веб-узел: support.euro.dell.com		
Код выхода на международную линию: 00	Отдел поддержки по электронной почте (переносные компьютеры): nor_nbk_support@dell.com		

Код страны: 47	Отдел поддержки по электронной почте (настольные компьютеры): nor_support@dell.com	
	Отдел поддержки по электронной почте (серверы): Nordic_server_support@dell.com	
	Техническая поддержка	671 16882
	Сопутствующая работа с клиентами	671 17514
	Отдел обслуживания домашних пользователей/малых предприятий	23162298
	Коммутатор	671 16800
	Факс-коммутатор	671 16865
Острова Теркс и Кайкос	Отдел поддержки по общим вопросам	бесплатно: 1-866-540-3355
Панама	Отдел поддержки по общим вопросам	001-800-507-0962
Перу	Отдел поддержки по общим вопросам	0800-50-669
Код выхода на международную линию: 011 Код страны: 48 Код города: 22	Веб-узел: support.euro.dell.com	
	Электронная почта: pl_support@dell.com	
	Телефон отдела обслуживания клиентов	57 95 700
	Отдел обслуживания клиентов	57 95 999
	Отдел продаж	57 95 999
	Факс отдела обслуживания клиентов	57 95 806
	Факс приемной	57 95 998
Коммутатор	57 95 999	
Код выхода на международную линию: 00 Код страны: 351	Веб-узел: support.euro.dell.com	
	Электронная почта: support.euro.dell.com/pt/en/emaildell/	
	Техническая поддержка	707200149
	Отдел обслуживания клиентов	800 300 413
	Отдел продаж	800 300 410 или 800 300 411 или 800 300 412 или 21 422 07 10
Факс	21 424 01 12	
Пуэрто-Рико	Отдел поддержки по общим вопросам	1-800-805-7545
Сальвадор	Отдел поддержки по общим вопросам	01-899-753-0777
Сент- Винсент и Гренадины	Отдел поддержки по общим вопросам	бесплатно: 1-877-270-4609
Сент- Китс и Невис	Отдел поддержки по общим вопросам	бесплатно: 1-877-441-4731
Сент- Люсия	Отдел поддержки по общим вопросам	1-800-882-1521
Код выхода на международную линию: 005 Код страны: 65	Техническая поддержка	бесплатно: 800 6011 051
	Отдел обслуживания клиентов (Пинанг, Малайзия)	6046334949
	Сделки по продаже	бесплатно: 800 6011 054
Отдел продаж для крупных предприятий		бесплатно: 800 6011 053
Страны Юго-Восточной Азии и Тихоокеанского региона	Техническая поддержка, обслуживание покупателей и продажи (Пинанг, Малайзия)	604 633 4810
Код выхода на международную линию: 011 Код страны: 1	Автоматическая система отслеживания заказа	бесплатно: 1-800-433-9014
	Автоматическая служба технической поддержки AutoTech (для портативных и настольных компьютеров)	бесплатно: 1-800-247-9362
	Клиент (дом и домашний офис)	
	Техническая поддержка	бесплатно: 1-800-624-9896
	Обслуживание клиентов	бесплатно: 1-800-624-9897
	Отдел обслуживания и поддержки (DellNet™)	бесплатно: 1-877-Dellnet (1-877-335-5638)
	Программа оказания помощи в покупке сотрудникам фирмы (EPP)	бесплатно: 1-800-695-8133
	Веб-узел финансовой службы: www.dellfinancialservices.com	
	Финансовые услуги (аренда/кредиты)	бесплатно: 1-877-577-3355
	Финансовые услуги (Привилегированные клиенты Dell [DPA])	бесплатно: 1-800-283-2210
	Предприятия	
	Обслуживание покупателей и техническая поддержка	бесплатно: 1-800-822-8965
	Отдел поддержки программы покупки сотрудниками (EPP)	бесплатно: 1-800-695-8133
	Техническая поддержка проекторов	бесплатно: 1-877-459-7298
	Государственные (правительство, образование и здравоохранение)	
	Техническая поддержка и обслуживание покупателей	бесплатно: 1-800-456-3355
Отдел поддержки программы покупки сотрудниками (EPP)	бесплатно: 1-800-234-1490	
Продажи Dell	бесплатно: 1-800-289-3355	

		или бесплатно: 1-800-879-3355
	Фирменный магазин Dell (восстановленные компьютеры Dell)	бесплатно: 1-888-798-7561
	Продажа программ и периферийных устройств	бесплатно: 1-800-671-3355
	Отдел продаж запасных частей	бесплатно: 1-800-357-3355
	Отдел реализации дополнительных услуг и гарантий	бесплатно: 1-800-247-4618
	Факс	бесплатно: 1-800-727-8320
	Отдел по обслуживанию клиентов с нарушениями слуха и речи	бесплатно: 1-877-DELLTY (1-877-335-5889)
Таиланд	Техническая поддержка	бесплатно: 0880 060 07
Код выхода на международную линию: 001	Отдел обслуживания клиентов (Пинанг, Малайзия)	604 633 4949
Код страны: 66	Отдел продаж	бесплатно: 0880 060 09
Тайвань	Техническая поддержка для портативных и настольных компьютеров	бесплатно: 00801 86 1011
Код выхода на международную линию: 002	Техническая поддержка (серверы)	бесплатно: 0080 60 1256
Код страны: 886	Сделки по продаже	бесплатно: 0080 651 228
	Отдел продаж для крупных предприятий	бесплатно: 0080 651 227
Тринидад и Тобаго	Отдел поддержки по общим вопросам	1-800-805-8035
Уругвай	Отдел поддержки по общим вопросам	бесплатно: 000-413-598-2521
Финляндия (Хельсинки)	Веб-узел: support.euro.dell.com	
Код выхода на международную линию: 990	Электронная почта: fin_support@dell.com	
Код страны: 358	Эл. почта для поддержки серверов: Nordic_support@dell.com	
Код города: 9	Техническая поддержка	09 253 313 60
	Техническая поддержка: факс	09 253 313 81
	Сопутствующая работа с клиентами	09 253 313 38
	Отдел обслуживания домашних пользователей/малых предприятий	09 693 791 94
	Факс	09 253 313 99
	Коммутатор	09 253 313 00
Франция (Париж) (Монпелье)	Веб-узел: support.euro.dell.com	
Код выхода на международную линию: 00	Электронная почта: support.euro.dell.com/be/fr/emaildell/	
Код страны: 33	Домашние пользователи и малые предприятия	
Коды города: (1) (4)	Техническая поддержка	0825 387 270
	Обслуживание клиентов	0825 823 833
	Коммутатор	0825 004 700
	Коммутатор (для клиентов, находящихся за пределами Франции)	04 99 75 40 00
	Отдел продаж	0825 004 700
	Факс	0825 004 701
	Факс (для клиентов, находящихся за пределами Франции)	04 99 75 40 01
	Работа с корпоративными клиентами	
	Техническая поддержка	0825 004 719
	Обслуживание клиентов	0825 338 339
	Коммутатор	01 55 94 71 00
	Отдел продаж	01 55 94 71 00
	Факс	01 55 94 71 01
Чехия (Прага)	Веб-узел: support.euro.dell.com	
Код выхода на международную линию: 00	Электронная почта: czech_dell@dell.com	
Код страны: 420	Техническая поддержка	02 2186 27 27
Код города: 2	Обслуживание клиентов	02 2186 27 11
	Факс	02 2186 27 14
	Служба TechFax	02 2186 27 28
	Коммутатор	02 2186 27 11
Чили (Сантьяго)	Продажи, поддержка покупателей и техническая поддержка	бесплатно: 1230-020-4823
Код страны: 56		
Код города: 2		
Швейцария (Женева)	Веб-узел: support.euro.dell.com	
Код выхода на международную линию: 00	Электронная почта: swisstech@dell.com	
Код страны: 41	Адрес электронной почты для клиентов HSB и корпоративных клиентов, говорящих на французском языке: support.euro.dell.com/ch/fr/emaildell/	
	Техническая поддержка (домашние пользователи и малые предприятия)	0844 811 411

Код города: 22	Техническая поддержка (для корпоративных клиентов)	0844 822 844
	Отдел обслуживания клиентов (домашние пользователи и малые предприятия)	0848 802 202
	Отдел обслуживания клиентов (корпоративные клиенты)	0848 821 721
	Факс	022 799 01 90
	Коммутатор	022 799 01 01
Швеция (Уппландс, Васбю)	Веб-узел: support.euro.dell.com	
Код выхода на международную линию: 00	Электронная почта: swe_support@dell.com	
	Эл. почта для поддержки Latitude и Inspiron: Swe-nbk_kats@dell.com	
Код страны: 46	Эл. почта для поддержки OptiPlex: Swe_kats@dell.com	
Код города: 8	Эл. почта для поддержки серверов: Nordic_server_support@dell.com	
	Техническая поддержка	08 590 05 199
	Сопутствующая работа с клиентами	08 590 05 642
	Отдел обслуживания домашних пользователей/малых предприятий	08 587 70 527
	Отдел поддержки программы покупки сотрудниками (EPP)	20 140 14 44
	Факс отдела технической поддержки	08 590 05 594
	Отдел продаж	08 590 05 185
	Эквадор	Отдел поддержки по общим вопросам
ЮАР (Йоханнесбург)	Веб-узел: support.euro.dell.com	
Код выхода на международную линию:	Электронная почта: dell_zs_support@dell.com	
	Техническая поддержка	011 709 7710
09/091	Обслуживание клиентов	011 709 7707
	Отдел продаж	011 709 7700
Код страны: 27	Факс	011 706 0495
Код города: 11	Коммутатор	011 709 7700
Ямайка	Отдел поддержки по общим вопросам (звонок только из Ямайки)	1-800-682-3639
Япония (Кавасаки)	Веб-узел: support.jp.dell.com	
Код выхода на международную линию: 001	Техническая поддержка для серверов	бесплатно: 0120-198-498
	Техническая поддержка за пределами Японии (серверы)	81-44-556-4162
Код страны: 81	Техническая поддержка (Dimension™ и Inspiron™)	бесплатно: 0120-198-226
	Техническая поддержка за пределами Японии (Dimension и Inspiron)	81-44-520-1435
Код города: 44	Техническая поддержка (Dell Precision™, OptiPlex™ и Latitude™)	бесплатно: 0120-198-433
	Техническая поддержка за пределами Японии (Dell Precision, OptiPlex и Latitude)	81-44-556-3894
	Техническая поддержка (Axim™)	бесплатно: 0120-981-690
	Техническая поддержка за пределами Японии (Axim)	81-44-556-3468
	Служба Faxbox	044-556-3490
	Круглосуточная автоматическая служба заказов	044-556-3801
	Отдел обслуживания клиентов	044-556-4240
	Отдел продаж для предприятий (до 400 сотрудников)	044-556-1465
	Отдел продаж привилегированным клиентам (более 400 сотрудников)	044-556-3433
	Отдел продаж крупным корпоративным клиентам (более 3500 сотрудников)	044-556-3430
	Отдел продаж бюджетных организаций (правительственные организации, образовательные и медицинские учреждения)	044-556-1469
	Глобальный сегмент, Япония	044-556-3469
	Индивидуальные пользователи	044-556-1760
Коммутатор	044-556-4300	

[Назад на страницу Содержание](#)

[Назад на страницу Содержание](#)

Использование Dell OpenManage Switch Administrator

Системы Dell™ PowerConnect™ 6024/6024F

- [Запуск приложения](#)
 - [Элементы интерфейса](#)
 - [Использование кнопок программы Switch Administrator](#)
 - [Определение полей](#)
 - [Доступ к коммутатору с помощью команд консоли](#)
 - [Использование режима командной строки](#)
-

Запуск приложения

1. Откройте веб-браузер.
2. Введите в строке адреса IP-адрес коммутатора (как определено в консоли) и нажмите клавишу <Enter>.

Для получения сведений о назначении IP-адреса для коммутатора см. раздел «[Начальная настройка](#)».

3. Когда отобразится окно Enter Network Password (Ввод сетевого пароля), введите имя пользователя и пароль.

 **ПРИМЕЧАНИЕ.** Для коммутатора не настроен пароль по умолчанию, поэтому настройка коммутатора без ввода пароля невозможна. Для получения сведений о восстановлении утраченного пароля см. раздел «[Восстановление пароля](#)».

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

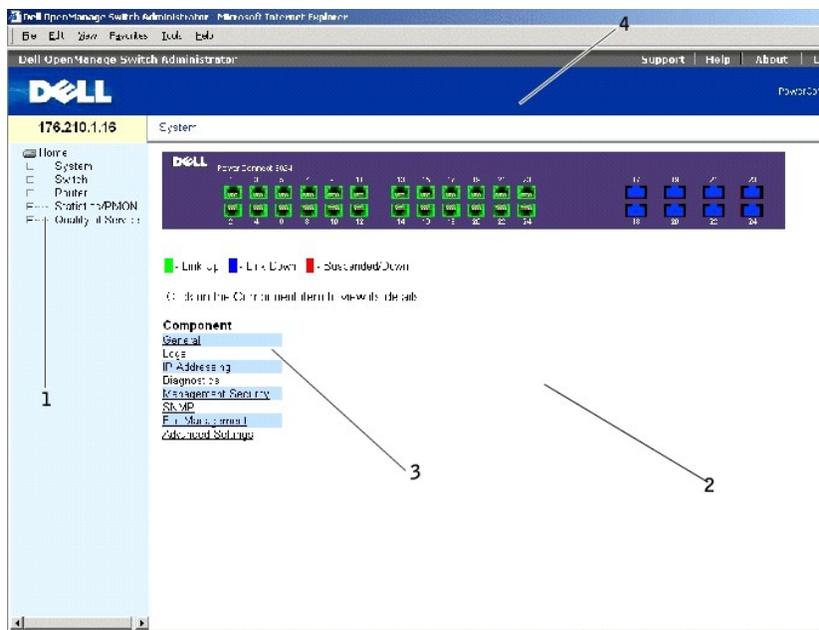
4. Нажмите кнопку ОК.
 5. Откроется домашняя страница Dell OpenManage Switch Administrator.
-

Элементы интерфейса

Домашняя страница (см. [рис. 4-1](#)) содержит следующие панели.

1. Панель дерева расположена в левой части домашней страницы и представляет собой разворачиваемое дерево параметров и их компонентов.
1. Панель устройства - расположена с правой стороны домашней страницы и отображает вид устройства, информационную или табличную область и инструкции по настройке.

Рис. 4-1. Компоненты программы Switch Administrator



В [таблице 4-1](#) приведен список компонентов интерфейса с соответствующими номерами.

Таблица 4-1. Компоненты интерфейса

Компонент	Название
1	Панель дерева содержит список различных параметров устройства. Ветви дерева можно раскрывать для просмотра всех компонентов параметра или сворачивать, скрывая эти компоненты. Чтобы расширить панель дерева для просмотра полного названия компонента, перетащите вертикальную полосу вправо.
2	На панели устройства приведены сведения о портах устройства, текущей настройке и состоянии устройства, табличная информация и компоненты параметров. Цвет порта показывает, активен ли порт в настоящий момент. Зеленый цвет означает, что порт включен, красный показывает, что произошла ошибка с портом, а синий - что соединение отключено. ПРИМЕЧАНИЕ. Индикаторы не отображаются на панели устройства. Состояние индикаторов можно определить на самом коммутаторе. Дополнительную информацию об индикаторах см. в разделе « Описания индикаторов ». В зависимости от выбранного параметра, в нижней области панели устройства отображается прочая информация об устройстве и диалоговые окна для настройки параметров.
3	В списке компонентов приведен список компонентов параметров. Компоненты также можно просмотреть, раскрыв параметр на панели дерева.
4	Информационные кнопки предоставляют доступ к сведениям о коммутаторе, а также доступ на веб-узел поддержки Dell. Дополнительную информацию см. в разделе « Информационные кнопки ».

Использование дерева кнопок программы Switch Administrator

Информационные кнопки

Таблица 4-2. Информационные кнопки

--	--

Кнопка	Описание
Support (Поддержка)	Открывает страницу службы поддержки Dell support.dell.com
Help (Справка)	Интерактивная справка, содержащая сведения, помогающие при настройке и управлении коммутатором. Страницы интерактивной справки напрямую связаны со страницами. Например, если открыта страница IP Addressing (IP-адресация), то при нажатии кнопки Help (Справка) отображается раздел справки для этой страницы.
About (О компьютере)	Содержит номер версии и сборки, а также информацию об авторских правах Dell.
Log Out (Выход)	Завершает работу приложения и закрывает окно браузера.

Кнопки управления устройством

Таблица 4-3. Кнопки управления устройством

Кнопка	Описание
Apply Changes (Применить изменения)	Применяет заданные изменения для устройства.
Add (Добавить)	Добавляет информацию в таблицы или диалоговые окна.
Telnet	Запускает сеанс Telnet.
Query (Запрос)	Запрашивает таблицы.
Show All (Показать все)	Отображает таблицы устройств.
Стрелка влево и стрелка вправо	Перемещает информацию между списками.
Refresh (Обновить)	Обновляет информацию об устройстве.
Reset All Counters (Сбросить все счетчики)	Сбрасывает статистические счетчики.
Print (Печать)	Распечатывает страницу Network Management System (Система сетевого управления) и табличную информацию.
Show Neighbor's Info (Показать сведения о соседних компонентах)	Отображает Neighbors List (Список соседних компонентов) из страницы Neighbors Table (Таблица соседних компонентов).
Draw (Нарисовать)	Быстро создает статистические диаграммы.
Clear Log (Очистить журнал)	Удаляет сообщения из буфера журнала.
Reset (Сброс)	Сбрасывает коммутатор.
Test Now (Тестировать)	Запускает диагностический тест для медных кабелей.

Определение полей

Поля, определенные пользователем, могут содержать от 1 до 159 символов, если на странице Dell OpenManage Switch Administrator не указано иное.

Можно использовать любые символы, за исключением следующих:

```

1 \
1 /
1 :
1 *
1 ?
1 <
1 >
1 |

```

Доступ к коммутатору с помощью команд консоли

Коммутатором можно управлять через прямое соединение с портом консоли или через соединение Telnet. Для получения сведений о портах

управления, находящихся вне диапазона, см. раздел [«Порт управления вне диапазона»](#).

Использование режима командной строки аналогично вводу команд в системе Linux. Если доступ осуществляется через соединение Telnet, убедитесь, что устройство имеет определенный IP-адрес и рабочая станция, используемая для доступа к устройству, подключена к нему до начала использования команд консоли.

Для получения сведений о настройке начального IP-адреса см. раздел [«Начальная настройка»](#).

 **ПРИМЕЧАНИЕ.** Перед использованием консоли убедитесь, что клиент загружен.

Подключение консоли

1. Включите питание коммутатора и дождитесь завершения запуска.
2. Когда появится приглашение консоли Console> введите команду enable и нажмите <Enter>.
3. Настройте устройство и введите необходимые команды для выполнения нужных задач.
4. По окончании выйдите из сеанса с помощью команды quit или exit.

 **ПРИМЕЧАНИЕ.** Если в систему войдет другой пользователь в режиме Privilege EXEC, то текущий пользователь будет отключен от системы, а в нее войдет новый пользователь.

Подключение Telnet

Telnet - это протокол TCP/IP эмуляции терминала. Терминалы ASCII 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.

Коммутатор поддерживает одновременно до четырех сеансов Telnet. Во время сеанса Telnet можно использовать все команды консоли.

Чтобы запустить сеанс Telnet:

1. Щелкните Пуск > Выполнить.
2. В окне **Запуск** программы введите telnet <IP-адрес> в поле **Открыть**.
3. Нажмите кнопку **ОК**, чтобы начать сеанс Telnet.

Использование режима командной строки

Обзор режима командной строки

Режим командной строки подразделяется на несколько командных режимов. Каждый из них имеет свой собственный набор команд. При вводе знака вопроса в строке консоли отображается список команд, доступных для данного командного режима.

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 консоли, и используется для доступа к подсистемам настройки, таким как режим командной строки (CLI). Для перехода на следующий уровень (Privileged EXEC) необходимо ввести пароль (если настроен).

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

Режим Global Configuration управляет настройкой устройства на глобальном уровне.

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

Режим User EXEC

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

```
console>
```

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

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

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

Режим Privileged EXEC

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

Чтобы получить доступ к командам режима Privileged EXEC:

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

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

```
console#
```

Чтобы отобразить список команд режима Privileged EXEC, введите знак вопроса в командной строке и нажмите клавишу <Enter>.

Для возврата из режима Privileged EXEC Mode в режим User EXEC Mode используйте любую из следующих команд: `disable`, `exit/end` или `<Ctrl><Z>`.

Следующий пример иллюстрирует переход в режим privileged EXEC и возврат в режим User EXEC:

```
console> enable
```

```
Enter Password: *****
```

```
console#
```

```
console# disable
```

```
console>
```

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

Режим Global Configuration

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

Для перехода в режим Global Configuration в командной строке режима Privileged EXEC введите команду `configure` и нажмите клавишу `<Enter>`. В режиме Global Configuration отображается имя хоста устройства, за которым следует символ решетки `#` и `(config)`.

```
console(config)#
```

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

Для возврата из режима Global Configuration в режим Privileged EXEC введите команду `exit` или используйте команду `<Ctrl><Z>`.

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

```
console#  
  
console#configure  
  
console(config)#exit  
  
console#
```

Режим Interface Configuration

Команды режима Interface configuration изменяют специальные настройки IP-интерфейса, включая группу мостов, описание и т.д. Существуют следующие режимы Interface Configuration (Настройки интерфейса).

- 1 **VLAN** - содержит команды для создания и настройки сети VLAN в целом, например для создания сети VLAN и применения IP-адреса к сети VLAN.
- 1 **Port Channel** - содержит команды для настройки групп LAG (Link Aggregation Groups).
- 1 **IP** - содержит команды для управления IP-интерфейсами.
- 1 **Out-of-Band-Ethernet** - содержит команды для управления и настройки управляющих соединений.

Примеры команд консоли

Команды консоли предоставляются как примеры настройки. Для получения полного описания команд консоли с примерами см. Справочник по командам консоли коммутатора.

[Назад на страницу Содержание](#)

[Назад на страницу Содержание](#)

Описание аппаратного обеспечения

Системы Dell™ PowerConnect™ 6024/6024F

- [Описание портов](#)
- [Компоненты оборудования](#)
- [Описания индикаторов](#)

В этом разделе содержится информация о характеристиках устройства и настройках аппаратного обеспечения модуля.

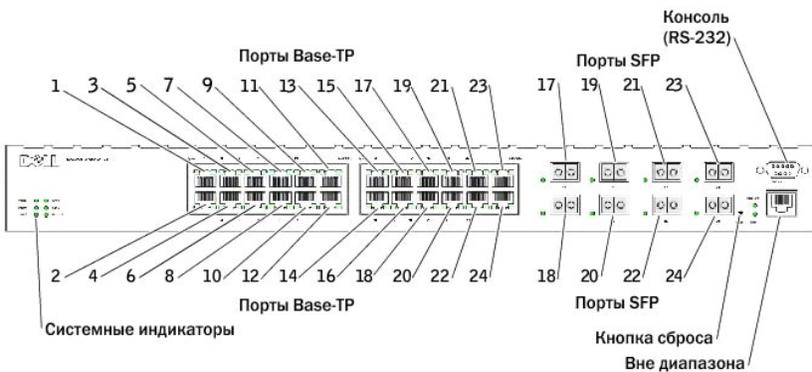
Описание портов

Коммутатор PowerConnect 6024

Порты 1-16 назначены как порты 10/100/1000, а порты 17-24 - как комбинированные порты. Номера портов показаны на следующем рисунке.

Комбинированный порт представляет собой один логический порт, имеющий два физических подключения - подключение RJ-45 и подключение SFP. Когда разъем вставлен в порт SFP, порт SFP будет активен до тех пор, пока не будет подключен медный разъем порта Base-T с тем же самым номером и не будет установлено соединение.

Рис. 2-1. Коммутатор PowerConnect 6024 с 24 портами 10/100/1000 Base-T



Коммутатор автоматически обнаруживает, какой кабель подключен к портам RJ-45 - перекрестный кабель или кабель прямого подключения. Порты SFP поддерживают модули SX и LX.

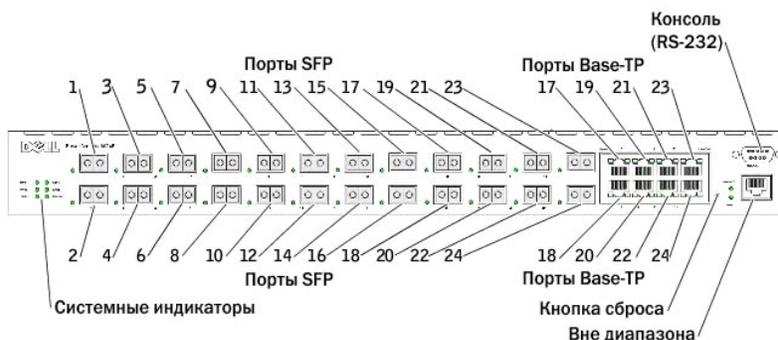
Порты RJ-45 поддерживают дуплексный и полудуплексный режимы 10/100/1000 Мбит/с.

Коммутатор PowerConnect 6024F

Порты PowerConnect 6024F отличаются от портов PowerConnect 6024 только назначением: Порты 1-16 назначены как порты SFP, а порты 17-24 назначены как комбинированные порты. Номера портов показаны на следующем рисунке.

Информацию о функциях портов см. в разделе описания портов для PowerConnect 6024.

Рис. 2-2. Коммутатор PowerConnect 6024F с 24 портами SFP



Поддержка порта для управления вне диапазона

Порт управления вне диапазона (OOB) - 10/100 Мбит/с порт Ethernet, который можно использовать для прямого подключения к коммутатору для выполнения задач администратора по управлению системой. Порт вне диапазона описывается как обычный IP-интерфейс для системы, и через него доступны все интерфейсы системы.

Дополнительную информацию о настройке портов управления вне диапазона см. в разделе [«Порт управления вне диапазона»](#).

Порт консоли (RS-232)

Порт консоли (RS-232) используется только для управления через последовательный интерфейс. Этот порт предоставляет прямое подключение к коммутатору и используется для доступа к консоли с терминала, подключенного к порту EIA/TIA-232.

Порт консоли поддерживает синхронную передачу данных (восемь битов данных, один стоповый бит, без контроля четности). Скорость передачи данных по умолчанию 115200 бод.

Компоненты оборудования

Фактические размеры

Коммутатор имеет следующие физические размеры:

- 1 440 x 460 x 44 мм (Ш x Г x В).
- 1 17,32 x 18,11 x 1,73 дюйма (Ш x Г x В).

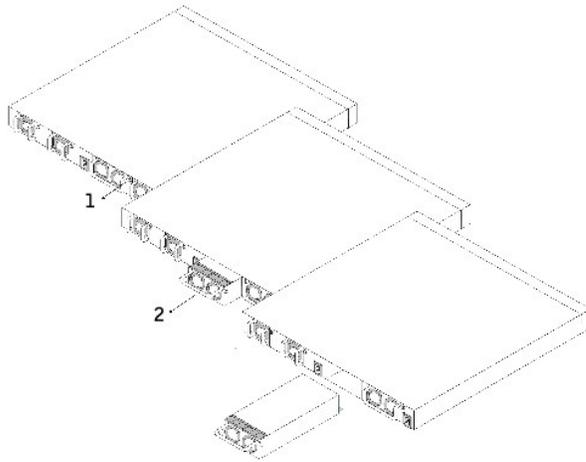
Источники питания

Коммутатор поставляется с двумя внутренними источниками питания. Проверить их работу можно с помощью индикаторов. Дополнительную информацию см. в разделе [«Системные индикаторы»](#).

Чтобы заменить источник питания:

1. Выверните винты на задней панели и выньте неисправный источник питания.
2. Установите новый источник питания в слот и убедитесь, что он полностью вставлен внутрь коммутатора.

Рис 2-3. Установка источника питания



3. Установите винты и приверните источник питания.
4. Подключите каждый источник питания к отдельному внешнему источнику питания.

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

Кнопка Reset (Сброс)

На передней панели коммутатора расположена кнопка сброса, предназначенная для сброса коммутатора вручную.

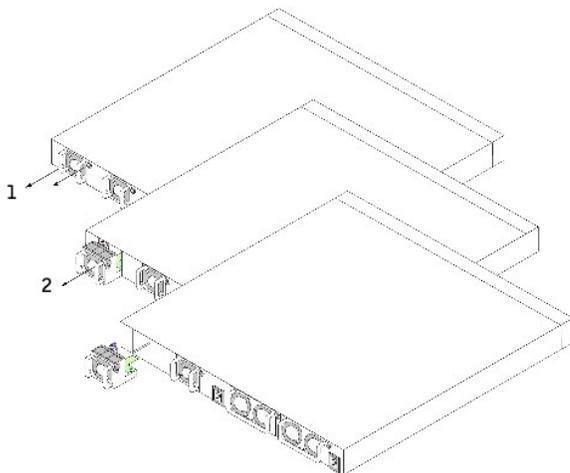
Система вентиляции

В системе установлены два вентилятора. Проверить их работу можно с помощью индикаторов. Дополнительную информацию см. в разделе [«Системные индикаторы»](#).

Чтобы заменить вентилятор:

1. Отверните два винта и осторожно извлеките неисправный вентилятор.
2. Аккуратно вставьте новый вентилятор в отсек.

Рис. 2-4. Установка или замена вентилятора



3. Установите винты и приверните вентилятор.

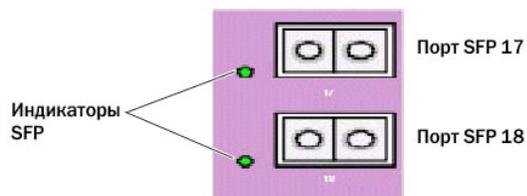
Описания индикаторов

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

Индикаторы порта SFP

На рис. 2-5 показаны индикаторы порта SFP, которые находятся рядом с каждым портом SFP.

Рис. 2-5. Индикаторы порта SFP



В таблице 2-1 приведено описание индикаторов для порта SFP.

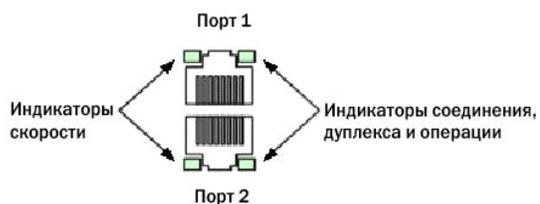
Таблица 2-1. Описание индикаторов для порта SFP

Индикатор	Цвет	Описание
SFP	Зеленый	Связь с портом установлена.
	Мигает зеленым	Порт получает и/или принимает сетевой трафик.
	Не горит	Связь с портом не установлена.

Индикаторы порта 10/100/1000 Base-T

У каждого порта 10/100/1000 Base-T имеется два индикатора. Индикатор скорости расположен слева от порта, а индикатор связь/дуплекс/активность расположен с правой стороны. На следующем рисунке показаны индикаторы порта 10/100/100 Base-T:

Рис. 2-6. Индикаторы порта 10/100/1000 Base-T



В [таблице 2-2](#) приведено описание индикаторов для порта 10/100/1000 Base-T.

Таблица 2-2. Описание порта 10/100/1000 Base-T

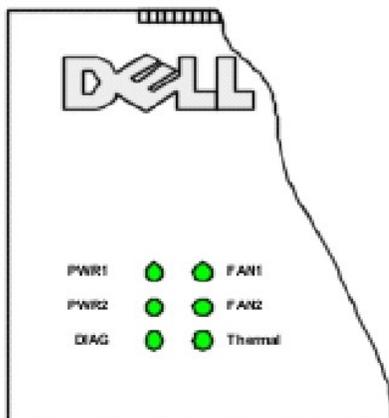
Индикатор	Цвет	Описание
Скорость		
	Зеленый	Порт работает на скорости 1000 Мбит/с.
	Оранжевый	Порт работает на скорости 100 Мбит/с.
	Не горит	Порт работает на скорости 10 Мбит/с.
Соединение		
	Зеленый	Порт работает и функционирует в дуплексном режиме.
	Мигает зеленым	Порт получает и посылает пакеты, работает в дуплексном режиме.
	Оранжевый	Порт работает в полудуплексном режиме.
	Мигает оранжевым	Порт получает и посылает пакеты, работает в полудуплексном режиме.
	Не горит	Связь с портом не установлена.

Системные индикаторы

Системные индикаторы, расположенные с левой стороны передней панели, предоставляют информацию об источниках питания, вентиляторах, температурных условиях и диагностическую информацию.

На [рис. 2-7](#) изображены системные индикаторы.

Рис. 2-7. Системные индикаторы



В [таблице 2-3](#) приведено описание системных индикаторов.

Таблица 2-3. Описание системных индикаторов

Индикатор	Цвет	Описание
Fan 1 (Вентилятор 1)		
	Горит зеленым	Вентилятор 1 установлен и работает.
	Горит красным	Вентилятор 1 установлен, но не работает.
	Не горит	Вентилятор 1 не установлен.
Fan 2 (Вентилятор 2)		
	Горит зеленым	Вентилятор 2 установлен и работает.
	Горит красным	Вентилятор 2 установлен, но не работает.
	Не горит	Вентилятор 2 не установлен.
PWR1		
	Горит зеленым	Источник питания 1 установлен и работает.
	Горит красным	Источник питания 1 установлен, но не работает.
	Не горит	Источник питания 1 не установлен.
PWR2		
	Горит зеленым	Источник питания 2 установлен и работает.
	Горит красным	Источник питания 2 установлен, но не работает.
	Не горит	Источник питания 2 не установлен.
Dia (Диагностика)		
	Мигает зеленым	Выполняется диагностический тест.
	Горит зеленым	Диагностический тест успешно завершен.
	Горит красным	Ошибка во время выполнения диагностического теста.
Thermal (Тепловое состояние)		
	Горит красным	Температура системы достигла максимально допустимого значения.
	Не горит	Температура системы в норме.

[Назад на страницу Содержание](#)

Введение

Системы Dell™ PowerConnect™ 6024/6024F

- [Коммутатор PowerConnect 6024](#)
- [Коммутатор PowerConnect 6024F](#)
- [Документация по командам консоли](#)
- [Функции](#)

ВНИМАНИЕ. Перед дальнейшими действиями прочтите примечания к выпуску для этого продукта. Примечания к выпуску можно загрузить с веб-узла support.dell.com.

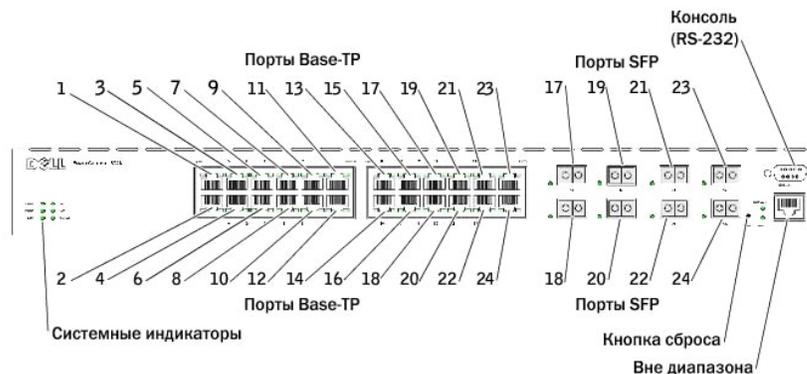
Устройство Dell™ PowerConnect™ 6024/6024F представляет собой автономный коммутатор уровня Layer 3, дополняющий серию сетевых коммутаторов Dell PowerConnect. Коммутатор имеет следующие особенности.

- 1 Корпус форм-фактора 1U, спроектированный для монтажа в стойку.
- 1 Порт управления вне диапазона для подключения к разъемам RJ-45 и RS-232.
- 1 Поддерживает все требования по обмену данными для многоуровневых коммутаторов, включая полный набор функций Layer 2, Layer 3+, безопасности и управления.
- 1 Возможность горячей замены источников питания и вентиляторов охлаждения.

Коммутатор PowerConnect 6024

Коммутатор PowerConnect 6024 содержит 24 порта 10/100/1000 Base-T RJ-45 с восьмью комбинированными портами SFP, поддерживающими режим автоматического определения скорости, управление потоком и дуплексный режим. Трансиверы SFP поставляются отдельно.

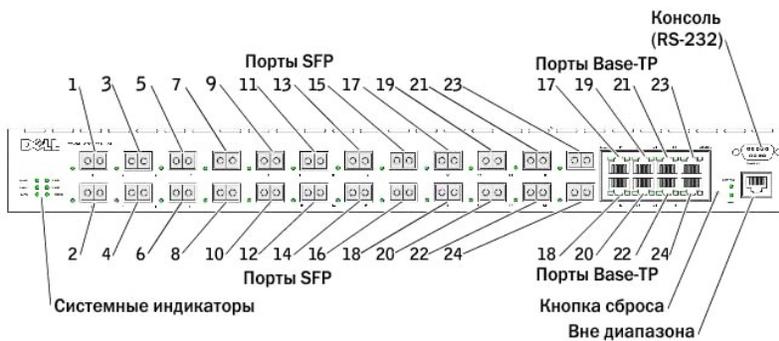
Рис. 1-1. Коммутатор PowerConnect 6024



Коммутатор PowerConnect 6024F

Коммутатор PowerConnect 6024F содержит 24 порта SFP с 8 комбинированными портами 10/100/1000 Base-T RJ-45, поддерживающими режим автоматического определения скорости, управление потоком и дуплексный режим. Трансиверы SFP поставляются отдельно.

Рис. 1-2. Коммутатор PowerConnect 6024F



Документация по

команд консоль

Справочное руководство по командам консоли содержит сведения о командах консоли, используемых для настройки коммутатора. В документе приведено описание командной строки, синтаксис и значения по умолчанию.

Функциональные возможности

В этом разделе описаны функции коммутатора, настраиваемые пользователем. Для получения списка всех функций см. примечания к выпуску программного обеспечения.

Функции портов

Виртуальное тестирование кабеля (VCT)

VCT определяет потенциальные проблемы связи при использовании медных кабелей, таких как обрыв или замыкание проводов кабеля, и отображает отчет по результатам.

Поддержка больших кадров

Большие кадры позволяют передавать данные меньшим числом пакетов, что уменьшает объем служебной информации, время обработки и перерывы.

Поддержка MDI/MDIX

Коммутатор автоматически обнаруживает, какой кабель подключен - перекрестный кабель или кабель прямого подключения.

MDI (Media-Dependent Interface) - это стандарт кабелей для конечных станций, а стандарт кабелей для концентраторов и коммутаторов называется MDIX (Media-Dependent Interface with Crossover).

Дополнительную информацию о настройке MDI/MDI для портов или объединенных групп каналов (LAG) см. в разделе [«Определение конфигурации порта»](#) или [«Определение конфигурации LAG»](#).

Аппаратная поддержка функции «Watchdog»

Коммутатор использует аппаратную функцию «Watchdog» для определения неполадок и выполнения необходимых действий по их устранению, если программное обеспечение перестает отвечать на запросы.

Автоматическое согласование

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

Коммутатор PowerConnect 6024/6024F улучшает автоматическое согласование тем, что обеспечивает объявление порта. С помощью объявления порта системный администратор может настраивать объявляемую портом скорость.

Для получения сведений об автоматическом согласовании см. раздел [«Определение конфигурации порта»](#) или [«Определение конфигурации LAG»](#).

Поддержка управления потоком (IEEE 802.3X)

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

Для получения сведений о настройке управления потоком для портов или объединенных групп каналов (LAG) см. раздел [«Определение конфигурации порта»](#) или [«Определение конфигурации LAG»](#).

Защита от блокировки очереди

Защита от блокировки очереди (HOL) предотвращает задержку трафика и потерю пакетов в том случае, когда трафик направляется на одни и те же наборы выходных портов. HOL блокирует пакеты очереди, и пакеты в начале очереди пересылаются до пакетов, находящихся в конце очереди.

Поддержка обратного давления

При дуплексном соединении приемник может предотвращать переполнение буфера путем захвата канала связи, делая его недоступным для дополнительного трафика.

Для получения сведений о настройке обратного давления для портов или объединенных групп каналов (LAG) см. раздел [«Определение конфигурации порта»](#) или [«Определение конфигурации LAG»](#).

Функции, поддерживающие MAC-адреса

Поддержка MAC-адресов

Коммутатор поддерживает до 16000 MAC-адресов и резервирует определенные MAC-адреса для использования системой.

Самораспознаваемые MAC-адреса

Коммутатор позволяет автоматически распознавать MAC-адреса во входящих пакетах.

Автоматическое время хранения MAC-адресов

MAC-адреса, от которых за определенный период времени не поступает трафика, устаревают. Это позволяет предотвратить переполнение таблицы связей.

Для получения сведений о сроке хранения MAC-адресов см. раздел [«Просмотр динамических адресов»](#).

Статические записи MAC

Определяемые пользователем записи MAC-адресов сохраняются в таблице связей вместе с самораспознаваемыми адресами.

Дополнительную информацию о настройке статических MAC-адресов см. в разделе [«Определение статических адресов»](#).

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

Пакеты, полученные от неизвестного источника, отправляются на обработку процессору и добавляются в аппаратную таблицу. В дальнейшем пакеты, полученные или направленные по этим адресам, будут передаваться более эффективно.

Поддержка передачи на несколько MAC-адресов

Служба многоадресной передачи представляет собой службу широковещательной передачи, которая позволяет устанавливать соединения «один ко многим» и «многие ко многим». В многоадресных службах Layer 2 принимается один кадр, адресованный указанному адресу многоадресной передачи, и создаются копии кадра, которые передаются на каждый соответствующий порт.

Для получения сведений о настройке поддержки многоадресных MAC-адресов см. раздел [«Поддержка пересылки многоадресного трафика»](#).

Функции Layer 2

Наблюдение по протоколу IGMP

Наблюдение на базе протокола IGMP проверяет содержимое кадров IGMP, когда они пересылаются коммутатором от станций на многоадресные маршрутизаторы. Наблюдение позволяет коммутатору определить станции, которым необходимы многоадресные сеансы и которым маршрутизаторы посылают многоадресные кадры.

Для получения сведений о настройке наблюдения по протоколу IGMP см. раздел [«Наблюдение по протоколу IGMP»](#).

Страница Port Mirroring

Зеркалирование портов контролирует и дублирует сетевой трафик путем пересылки копий входящих и исходящих пакетов с одного порта на другой (контролирующие).

Для получения сведений о зеркалировании портов см. раздел [«Определение сеансов с зеркалированием портов»](#).

Защита от «лавины» широковещательной передачи

Когда передаются кадры Layer 2, широковещательные и многоадресные кадры рассылаются «лавиной» на все порты соответствующей VLAN. «Лавина» занимает всю полосу пропускания и загружает все узлы, подключенные ко всем портам. Защита от «лавины» ограничивает число многоадресных и широковещательных кадров, принятых и переданных коммутатором.

Дополнительную информацию о настройке защиты от «лавины» см. в разделе [«Включение контроля «лавины»»](#).

Поддержка функций VLAN

Поддержка VLAN

VLAN представляют собой совокупности коммутируемых портов, входящих в состав одного домена широковещательной передачи. Принадлежность пакетов VLAN определяется либо на основе метки VLAN, либо на основе комбинации входящего порта и содержимого пакета. Пакеты с одинаковыми атрибутами, можно объединить в одну группу VLAN.

Для получения сведений о настройке групп VLAN см. раздел [«Настройка групп VLAN»](#).

VLAN, основанные на портах

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

Для получения сведений о настройке групп VLAN см. раздел [«Настройка групп VLAN»](#).

VLAN, основанные на протоколе IEEE802.1V

Правила классификации по группам VLAN определяются на уровне связи данных (Layer 2) протокола. Группы, основанные на протоколе VLAN, используются для отделения трафика Layer 2 для различения протоколов Layer 3.

Дополнительную информацию об определении VLAN, основанных на протоколе, см. в разделе [«Определение групп протоколов VLAN»](#).

Полное соответствие маркировке VLAN 802.1Q

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

Требованием этого стандарта является возможность отметки кадров с помощью необходимого значения метки класса обслуживания (CoS) (07).

Поддержка GVRP

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

Дополнительную информацию о настройке групп VLAN см. в разделе [«Настройка протокола GVRP»](#).

Private VLAN Edge

Порты PVE (Private VLAN Edge) выполняют функцию обеспечения безопасности уровня Layer 2, а именно безопасности между смежными портами внутри сети VLAN. Это расширяет обычную сеть VLAN. Трафик от защищенных портов отсылается на порты группового соединения и не может быть отправлен на другие порты VLAN.

Дополнительную информацию о настройке портов PVE см. в разделе [«Настройка портов»](#).

Функции протокола Spanning Tree

Протокол STP (Spanning Tree) на устройстве

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

Дополнительную информацию о настройке протокола STP см. в разделе [«Настройка протокола STP»](#).

Быстрая связь

Время реакции протокола STP может достигать 30-60 секунд. В это время определяются возможные циклы, а также выделяется необходимое время для распространения данных об изменениях состояния, а также на ответ соответствующих устройств. Для многих приложений это время считается слишком большим. Функция Fast Link позволяет избежать этой задержки и не требует нескольких маршрутов передачи данных для обеспечения устойчивости сети.

Для получения сведений о включении функции Fast Link для портов и групп LAG см. раздел [«Определение параметров STP для порта»](#) или [«Определение параметров STP для LAG»](#).

Поддержка протокола IEEE 802.1w Rapid Spanning Tree

Протокол Rapid Spanning Tree (RSTP) выявляет и использует топологию сети, обеспечивая лучшую сходимости для протокола STP без образования циклов пересылки.

Дополнительные сведения о настройке протокола RSTP см. в разделе [«Определение протокола RSTP»](#).

Протокол Multiple Spanning Tree

Протокол MSTP (Multiple Spanning Tree Protocol) отображает сети VLAN в экземплярах ST. Протокол MSTP обеспечивает другой сценарий выравнивания нагрузки. Пакеты, назначенные разным сетям VLAN, передаются через разные пути в областях MSTP (области MST). Области являются один или несколько мостов MSTP с одинаковыми настройками MSTP. При использовании этого стандарта администраторы могут назначать трафик VLAN для конкретных маршрутов.

Дополнительную информацию о MSTP см. в разделе [«Определение MST»](#).

Страница Link Aggregation (Объединение каналов)

Страница Link Aggregation (Объединение каналов)

Можно объединить до семи портов в одну группу LAG (Link Aggregated Group). Это обеспечивает защиту от сбоев вследствие физического разрыва соединения, а также соединения с большей полосой пропускания и улучшенные возможности разбиения полосы пропускания.

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

Дополнительную информацию о настройке групп LAG см. в разделе [«Определение настройки LAG»](#).

Объединение каналов и протокол LACP

В протоколе LACP осуществляется обмен данными по каналу связи между двумя точками и постоянно определяется возможность объединения различных каналов. При этом постоянно достигается максимально возможный уровень объединения каналов между заданной парой систем. Протокол LACP автоматически определяет, настраивает, связывает и контролирует связывание портов для объединяемых каналов внутри системы.

Дополнительную информацию о протоколе LACP см. в разделе [«Определение параметров протокола LACP»](#).

Функции маршрутизации

IP-маршрутизация

IP-маршрутизация переадресовывает близлежащему узлу любые пакеты, которые адресованы на MAC-адреса системы, а не на IP-адрес системы.

Дополнительную информацию о настройке IP-маршрутизации см. в разделе [«Настройка глобальной IP-маршрутизации»](#).

RIP версий 1 и 2

Routing Information Protocol - протокол данных маршрутизации (RIP) - это протокол дистанционно-векторной маршрутизации. В протоколе RIP маршруты выбираются на основе числа узлов до места назначения. RIP 2 повышает эффективность, удобство использования, а также улучшает методы проверки подлинности протокола RIP.

Дополнительную информацию о протоколе RIP см. в разделе [«Настройка RIP»](#).

OSPF версии 2

Протокол OSPF (Open Shortest Path First) - это протокол маршрутизации внутреннего шлюза. В сетях с большим числом соединенных маршрутизаторов протокол OSPF более эффективен, чем RIP, поскольку в протоколе OSPF используется меньшая полоса пропускания и сведение происходит быстрее.

Дополнительную информацию о настройке протокола OSPF см. в разделе [«Настройка параметров и фильтров OSPF»](#).

Протокол ARP (Address Resolution Protocol)

При IP-маршрутизации маршрутизаторы и коммутаторы Layer 3 используют различные протоколы маршрутизации для обнаружения топологии сети и определения таблиц маршрутизации. Протокол ARP автоматически определяет MAC-адреса устройств ближайшего узла систем, включая напрямую подключенные конечные системы. Пользователи могут это отменить, а вместо этого определить дополнительные записи таблицы ARP.

Дополнительную информацию о настройке ARP см. в разделе [«Определение параметров ARP»](#).

Сообщения протокола ICMP

Сообщения протокола ICMP (Internet Control Message Protocol) используются для передачи сообщений вне диапазона, относящихся к работе или неполадке сети.

IGMPv2

Протокол IGMP позволяет маршрутизатору отправлять запросы IGMP в виде широковещательных сообщений L2 по каждому интерфейсу. При отправке многоадресного пакета, содержащего MAC-адрес многоадресной рассылки, все узлы на этом интерфейсе маршрутизатора получают копию этого пакета. Узлы отслеживают все отчеты протокола IGMP. Если заинтересованные группы многоадресной рассылки уже были запрошены любой из станций на том же интерфейсе, то остальные станции не посылают дублирующиеся запросы.

Дополнительную информацию о настройке протокола IGMP см. в разделе [«Определение параметров интерфейса IGMP»](#).

Поддержка сопоставления самого длинного префикса

Сопоставления самого длинного префикса используются в основном для определения наилучшего маршрута для пакета через соседние узлы исключительно на основе адреса назначения, содержащегося в заголовке пакета. Поскольку IP-адреса обычно назначаются в соответствии с используемой топологией сети, получаемый в результате самый длинный префикс обычно соответствует кратчайшему маршруту до места назначения.

DVMRP

Протокол дистанционно-векторной многоадресной маршрутизации DVMRP (Distance Vector Multicast Routing Protocol) предлагает кратчайшие маршруты для сетей с источниками многоадресной рассылки с узлами, которые передают многоадресный IP-трафик.

Дополнительную информацию о настройке протокола DVMRP см. в разделе [«Настройка интерфейсов DVMRP»](#).

VRRP

Протокол VRRP (Virtual Router Redundancy Protocol) позволяет исключить отдельные точки сбоя в маршруте. Протокол VRRP использует электронный протокол, который динамически назначает обязанности виртуального маршрутизатора одному из маршрутизаторов VRRP в локальной сети.

Процесс выбора обеспечивает динамическое восстановление в случае отказа и передачу обязанностей, когда главное устройство недоступно. Конечные узлы в качестве маршрутизатора по умолчанию первого узла могут использовать любой из IP-адресов виртуального маршрутизатора.

Дополнительную информацию о настройке протокола VRRP см. в разделе [«Настройка VRRP»](#).

Функции Layer 3

TCP

Соединения протокола TCP (Transport Control Protocol) определяются между 2 портами во время обмена данными при исходной синхронизации. Порты TCP определяются по IP-адресу и 16-разрядному номеру порта. Октетные потоки делятся на пакеты TCP, каждый из которых содержит номер последовательности.

ретрансляции UDP

Ретрансляция UDP позволяет устройству пересылать определенные широковещательные пакеты UDP от одного интерфейса другому. IP-пакеты широковещательной рассылки от одного интерфейса необязательно переадресуются на другой интерфейс. Однако некоторые приложения используют широковещательную рассылку UDP для определения доступности службы. Другие службы требуют маршрутизации широковещательных пакетов UDP для предоставления служб клиентам в другой подсети.

Клиенты BootP и DHCP

Протокол DHCP позволяет получать дополнительные параметры настройки от сетевого сервера во время запуска системы. Служба DHCP представляет

собой непрерывный процесс. DHCP является расширением BootP.

Дополнительную информацию о DHCP см. в разделе [«Определение параметров IP-интерфейса DHCP»](#).

Ретрансляция BootP

BootP позволяет устройству запрашивать и получать данные конфигурации у серверов. Если соответствующий сервер BootP не напрямую подключен к домену широковещательной рассылки клиента, то служба ретрансляции BootP позволяет клиенту установить связь с сервером.

параметров ретрансляции DHCP

DHCP позволяет устройству запрашивать и получать данные конфигурации у серверов. Если соответствующий сервер DHCP не напрямую подключен к домену широковещательной рассылки клиента, то служба ретрансляции DHCP позволяет клиенту установить связь с сервером.

Дополнительную информацию о настройке параметров ретрансляции DHCP см. в разделе [«Определение параметров ретрансляции DHCP»](#).

Функции качества обслуживания (Quality of Service)

Поддержка функции качества обслуживания (QoS)

Чтобы решить проблему непредсказуемого сетевого трафика и оптимизировать производительность, можно использовать функцию качества обслуживания (QoS) во всей сети, чтобы установить приоритеты трафика в соответствии с определенными критериями. Данный коммутатор поддерживает два режима QoS: основной и расширенный.

Поддержка класса обслуживания 802.1p

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

Основной режим качества обслуживания

В основном режиме QoS можно активизировать режим доверия (т.е. доверять VPT, DSCP, TCP/UDP или никому). Кроме того, для интерфейса можно определить список управления однократным доступом.

Дополнительную информацию о включении основного режима QoS см. в разделе [«Настройка основного режима QoS»](#).

Расширенный режим качества обслуживания

Расширенный режим качества обслуживания определяет классификацию потока и назначает систему правил, относящихся к управлению полосой пропускания. Эти правила можно объединять в политику, которую можно применять для интерфейса.

Дополнительную информацию о включении расширенного режима QoS см. в разделе [«Настройка расширенного режима QoS»](#).

Функции управления устройствами

Сигналы и журналы прерываний SNMP

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

Дополнительную информацию о сигналах и прерываниях SNMP см. в разделе [«Определение параметров SNMP»](#).

Управление через веб-интерфейс

Системой можно управлять с помощью веб-интерфейса. Коммутатор содержит встроенный веб-сервер, обслуживающий HTML-страницы, которые можно использовать для контроля и настройки системы.

Загрузка файла конфигурации

Файл конфигурации коммутатора содержит данные конфигурации как всей системы, так и конфигурацию устройства определенного порта. Файл конфигурации можно отобразить с помощью команд консоли.

Дополнительную информацию о загрузке файлов конфигурации см. в разделе [«Загрузка файлов»](#).

Загрузка программного обеспечения

Загрузка программного обеспечения позволяет хранить резервные образы микропрограммы. Дополнительную информацию о загрузке программного обеспечения см. в разделе [«Загрузка программного обеспечения и перезагрузка»](#).

Протокол TFTP (Trivial File Transfer Protocol)

PowerConnect 6024/6024F поддерживает загрузку и передачу по протоколу TFTP образа загрузки, микропрограммы и конфигурации.

Удаленный мониторинг

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

Дополнительную информацию об удаленном мониторинге RMON см. в разделе [«Просмотр статистики удаленного мониторинга RMON»](#).

Протокол SNMP (Simple Network Management Protocol) версии 1, 2 и 3

Для управления доступом к системе определяется список записей сообщества, каждая из которых содержит строку сообщества и привилегии доступа. Существуют три уровня безопасности SNMP - только чтение, чтение и запись и супер. К самой таблице сообщества имеет доступ только супер-пользователь.

Интерфейс командной строки

Интерфейс командной строки консоли (CLI) максимально соответствуют общим принципам, принятым в промышленности. Консоль состоит из обязательных и необязательных элементов. В контекстной справке указан формат и диапазоны допустимых значений для текущих команд, а интерпретатор консоли предоставляет список команд и ключевых слов.

Syslog

Syslog - это протокол, который обеспечивает передачу уведомлений об ошибках указанным удаленным серверам, где их можно сохранить, изучить или выполнить соответствующие действия.

Дополнительную информацию о Syslog см. в разделе [«Управление журналами»](#).

SNTP

Протокол SNTP (Simple Network Time Protocol) гарантирует точность синхронизации времени такта сетевого коммутатора до миллисекунды. Синхронизация по времени выполняется сетевым сервером SNTP.

Дополнительную информацию о протоколе SNTP см. в разделе [«Настройка параметров SNTP»](#).

Трассировка

Трассировка позволяет выполнять обнаружение маршрутов IP, пакеты которых были пересланы во время процедуры пересылки. Программу CLI Traceroute можно запустить в режиме User EXEC или Privileged EXEC.

Поддержка порта для управления вне диапазона

Порт управления вне диапазона - это внешний порт Ethernet, по которому передается только трафик между системным администратором и управляющими приложениями. Порт управления вне диапазона предоставляет физически безопасный канал, а также обеспечивает отказоустойчивость.

Средства защиты

Списки управления доступом ACL

В списках ACL определены правила для пересылки и блокировки сетевого трафика. Можно определить списки ACL, чтобы повысить безопасность, определив правила классификации и назначив действия для каждого правила. Список ACL можно назначить для входного интерфейса (порта или VLAN).

Дополнительную информацию об определении списков ACL см. в разделах [«Определение списков ACL, основанных на IP-адресах»](#) и [«Определение списков ACL, основанных на MAC-адресах»](#).

Проверка подлинности на основе порта (802.1x)

Проверка подлинности на основе порта обеспечивает проверку подлинности пользователей системы на основе портов через внешний сервер. Только прошедшие проверку подлинности и одобренные пользователи системы могут передавать и принимать данные. Проверка подлинности портов выполняется с помощью сервера Remote Authentication Dial In User Service (RADIUS), использующего протокол EAP (Extensible Authentication Protocol).

Дополнительную информацию см. в разделе [«Настройка проверки подлинности на основе порта»](#).

Поддержка заблокированных портов

Заблокированные порты предоставляют доступ к порту только для пользователей с определенными MAC-адресами. Эти адреса определяются пользователем вручную или автоматически на этом порту. При получении кадра на заблокированном порту, если MAC-адрес источника кадра не связан с этим портом, срабатывает механизм защиты.

Дополнительную информацию о включении функции безопасности заблокированного порта см. в разделе [«Настройка безопасности портов»](#).

Безопасность управления паролями

Управление паролями повышает безопасность сети и улучшает контроль паролей. Паролям для доступа SSH, Telnet, HTTP, HTTPS и SNMP назначаются функции безопасности.

Дополнительную информацию об управлении паролями см. в разделе [«Управление паролями»](#).

TACACS+

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

Дополнительную информацию об определении параметров TACACS+ см. в разделах [«Настройка серверов TACACS+ вне диапазона»](#) и [«Настройка параметров TACACS+»](#).

Клиент RADIUS

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

Дополнительную информацию об определении параметров серверов RADIUS см. в разделе [«Настройка параметров RADIUS»](#).

Страница SSH

Secure Shell (SSH) - это протокол, обеспечивающий защиту и удаленное подключение к устройству. Это соединение предоставляет функциональные возможности, аналогичные входящему соединению telnet.

[Назад на страницу Содержание](#)

[Назад на страницу Содержание](#)

Системы Dell™ PowerConnect™ 6024/6024F



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



ВНИМАНИЕ. Указывает на опасность повреждения оборудования или потери данных и объясняет, как этого избежать.



ПРЕДУПРЕЖДЕНИЕ. Указывает на возможность материального ущерба, травмы или смерти.

Информация, включенная в состав данного документа, может быть изменена без уведомления.

© Dell Inc., 2005 **Все права защищены.**

Воспроизведение материалов данного руководства в любой форме без письменного разрешения корпорации Dell Inc. строго запрещено.

Товарные знаки, использованные в этом документе: *Dell, Dell OpenManage, логотип DELL, Inspiron, Dell Precision, Dimension, OptiPlex, PowerConnect, PowerApp, PowerVault, Axim, DellNet и Latitude* являются товарными знаками корпорации Dell Inc. *Microsoft и Windows* являются охраняемыми товарными знаками корпорации Майкрософт.

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

Январь 2005 года

[Назад на страницу Содержание](#)

[Назад на страницу Содержание](#)

Просмотр статистики

Системы Dell™ PowerConnect™ 6024/6024F

- [Просмотр таблиц](#)
- [Просмотр статистики удаленного мониторинга RMON](#)
- [Просмотр диаграмм](#)

В этом разделе приведена статистическая информация об интерфейсе, GVRP, Etherlike, RMON и использовании устройства.

 **ПРИМЕЧАНИЕ.** Команды консоли доступны не для всех страниц статистики.

Просмотр таблиц

Страница Table Views (Просмотр в виде таблиц) содержит ссылки для отображения статистики в графическом виде.

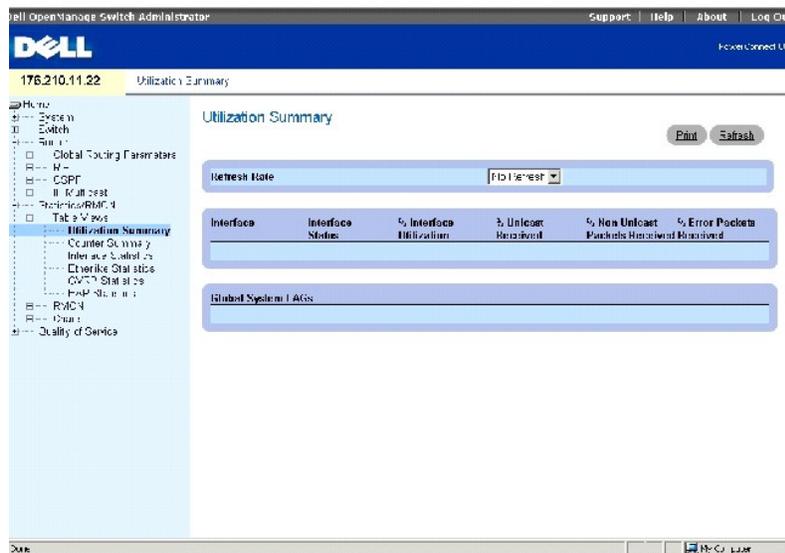
Чтобы открыть страницу, выберите Statistics/RMON (Статистика/RMON)→ Table Views (Просмотр в виде таблиц) на панели дерева.

Просмотр общих сведений по использованию

Страница [Utilization Summary](#) (Общие сведения по использованию) содержит статистику по использованию интерфейса.

Чтобы открыть страницу, выберите Statistics/RMON (Статистика/RMON)→ Table Views (Просмотр в виде таблиц)→ Utilization Summary (Общие сведения по использованию) на панели дерева.

Рис. 9-1. Страница Utilization Summary (Общие сведения по использованию)



Страница [Utilization Summary](#) (Общие сведения по использованию) содержит следующие поля.

Refresh Rate (Частота обновления) - период времени между обновлениями статистики интерфейса. Допустимые значения поля: No Refresh (Нет обновления), 15, 30 и 60 секунд.

Interface (Интерфейс) - номер интерфейса.

Interface Status (Состояние интерфейса) - состояние интерфейса.

% Interface Utilization (% использования интерфейса) - процент использования сетевого интерфейса на основе дуплексного режима интерфейса. Диапазон значений этого параметра составляет от 0 до 200 %. Максимальное значение 200% для дуплексного соединения показывает, что полоса пропускания входящих и исходящих соединений на 100% используется трафиком, проходящим через интерфейс. Максимальное значение для полудуплексного соединения составляет 100%.

% Unicast Received (% полученных одноадресных пакетов) - процент полученных на интерфейс одноадресных пакетов.

% Non Unicast Packets Received (% полученных многоадресных пакетов) - процент полученных на интерфейс многоадресных пакетов.

% Error Packets Received (% полученных пакетов с ошибками) - число пакетов с ошибками, полученных на интерфейс.

Просмотр сводки по счетчикам

Страница [Counter Summary](#) (Сводка по счетчикам) содержит статистику по использованию порта в числовых суммах, а не в процентах.

Чтобы открыть страницу, выберите [Statistics/RMON](#) (Статистика/RMON) → [Table Views](#) (Просмотр в виде таблиц) → [Counter Summary](#) (Сводка по счетчикам) на панели дерева.

Рис. 9-2. Страница Counter Summary (Сводка по счетчикам)

Interface	Interface Status	Received Unicast Packets	Transmit Unicast Packets	Received Non Unicast Packets	Transmit Non Unicast Packets	Received Errors	Transmit Errors
1	g1	Down	0	0	0	0	0
2	g2	Down	0	0	0	0	0
3	g3	Down	0	0	0	0	0
4	g4	Down	0	0	0	0	0
5	g5	Down	0	0	0	0	0
6	g6	Down	0	0	0	0	0
7	g7	Down	0	0	0	0	0
8	g8	Down	0	0	0	0	0
9	g9	Down	0	0	0	0	0
10	g10	Down	0	0	0	0	0
11	g11	Down	0	0	0	0	0
12	g12	Down	0	0	0	0	0
13	g13	Down	0	0	0	0	0
14	g14	Down	0	0	0	0	0
15	g15	Down	0	0	0	0	0
16	g16	Down	0	0	0	0	0
17	g17	Down	0	0	0	0	0
18	g18	Down	0	0	0	0	0
19	g19	Down	0	0	0	0	0
20	g20	Down	0	0	0	0	0
21	g21	Down	0	0	0	0	0
22	g22	Down	0	0	0	0	0
23	g23	Down	0	0	0	0	0
24	g24	Down	0	0	0	0	0
Global System LAGs							
25	LAG 1	Not Present	0	0	0	0	0
26	LAG 2	Not Present	0	0	0	0	0
27	LAG 3	Not Present	0	0	0	0	0
28	LAG 4	Not Present	0	0	0	0	0
29	LAG 5	Not Present	0	0	0	0	0
30	LAG 6	Not Present	0	0	0	0	0
31	LAG 7	Not Present	0	0	0	0	0

Refresh Rate (Частота обновления) - период времени между обновлениями статистики интерфейса. Допустимые значения поля: No Refresh (Нет обновления), 15, 30 и 60 секунд.

Interface (Интерфейс) - номер интерфейса.

Interface Status (Состояние интерфейса) - состояние интерфейса.

Received Unicast Packets (Получено одноадресных пакетов) - число полученных на интерфейс одноадресных пакетов.

Transmit Unicast Packets (Передано одноадресных пакетов) - число переданных одноадресных пакетов из интерфейса.

Received non-Unicast Packets (Получено многоадресных пакетов) - число полученных на интерфейс многоадресных пакетов.

Transmit Non Unicast Packets (Передано многоадресных пакетов) - число переданных многоадресных пакетов из интерфейса.

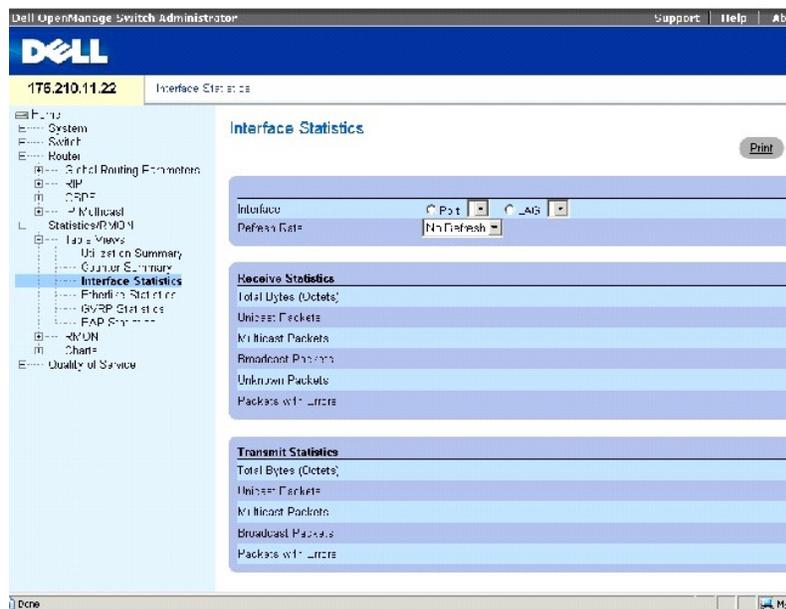
Received Errors (Получено ошибок) - число полученных ошибок на интерфейс.

Transmit Errors (Передано ошибок) - число переданных ошибок из интерфейса.

Просмотр статистики интерфейса

Страница **Interface Statistics** (Статистика интерфейса) содержит статистику по принятым и переданным пакетам. Поля для полученных и переданных пакетов идентичны. Чтобы открыть страницу, выберите **Statistics/RMON** (Статистика/RMON) → **Table Views** (Просмотр в виде таблиц) → **Interface Statistics** (Статистика интерфейса) на панели дерева.

Рис. 9-3. Страница Interface Statistics (Статистика интерфейса)



Interface (Интерфейс) - указывает, отображается статистика для порта или LAG.

Refresh Rate (Частота обновления) - период времени между обновлениями статистики интерфейса. Допустимые значения поля: No Refresh (Нет обновления), 15, 30 и 60 секунд.

Статистика приема

Total Bytes (Octets) [(Всего байт (октетов))] - число октетов, принятых на выбранный интерфейс.

Unicast Packets (Одноадресные пакеты) - число одноадресных пакетов, полученных на выбранный интерфейс.

Multicast Packets (Многоадресные пакеты) - число многоадресных пакетов, полученных на выбранный интерфейс.

Broadcast Packets (Пакеты широковещательной рассылки) - число пакетов широковещательной рассылки, полученных на выбранный интерфейс.

Unknown Packets (Неизвестные пакеты) - число неизвестных пакетов, полученных на выбранный интерфейс.

Packets with Errors (Пакеты с ошибками) - число ошибок, переданных с выбранного интерфейса.

Статистика передачи

Total Bytes (Octets) [(Всего байт (октетов))] - число октетов, принятых на выбранный интерфейс.

Unicast Packets (Одноадресные пакеты) - число одноадресных пакетов, переданных на выбранный интерфейс.

Multicast Packets (Многоадресные пакеты) - число многоадресных пакетов, переданных на выбранный интерфейс.

Broadcast Packets (Пакеты широковещательной рассылки) - число пакетов широковещательной рассылки, переданных на выбранный интерфейс.

Packets with Errors (Пакеты с ошибками) - число ошибок, переданных с выбранного интерфейса.

Отображение статистики интерфейса

1. Откройте страницу **Interface Statistics** (Статистика интерфейса).
2. Выберите интерфейс в поле **Interface** (Интерфейс).

Сброс счетчиков статистики интерфейса

1. Откройте страницу **Interface Statistics** (Статистика интерфейса).
2. Щелкните **Reset All Counters** (Сбросить все счетчики).

Просмотр статистики интерфейса с помощью команд консоли

Следующая таблица содержит команды CLI для просмотра статистики интерфейса.

Таблица 9-1. Команды консоли для статистики интерфейса

Команда консоли	Описание
<code>show interfaces counters [ethernet интерфейс port- channel номер_канала_порта]</code>	Отображает трафик, видимый физическим интерфейсом.

Далее приведен пример команд консоли.

```
Console> show interfaces counters
```

```
Port InOctets InUcastPkts InMcastPkts InBcastPkts
```

```
-----
```

```
g1 0 0 0 0
```

```
g2 0 0 0 0
```

```
g3 0 0 0 0
```

```
g4 0 0 0 0
```

```
g5 0 0 0 0
```

```
g6 0 0 0 0
```

```
g7 0 0 0 0
```

```
g8 0 0 0 0
```

```
g9 0 0 0 0
```

```
g10 0 0 0 0
```

```
g11 1 0 0 0 0
```

```
g12 10 685 2 9 0 32
```

```
g13 0 0 0 0
```

```
g14 0 0 0 0
```

g15 0 0 0 0

g16 0 0 0 0

g17 0 0 0 0

g18 0 0 0 0

g19 0 0 0 0

g20 0 0 0 0

g21 0 0 0 0

g22 0 0 0 0

g23 0 0 0 0

g24 0 0 0 0

Просмотр статистики Etherlike

Страница **Etherlike Statistics** (Статистика Etherlike) содержит статистику интерфейса. Чтобы открыть страницу, выберите **Statistics/RMON** (Статистика/RMON) → **Table Views** (Просмотр в виде таблиц) → **Etherlike Statistics** (Статистика интерфейса) на панели дерева.

Рис. 9-4. Страница Etherlike Statistics (Статистика Etherlike)

The screenshot shows the 'Etherlike Statistics' page in the Dell OpenManage Switch Administrator. The interface includes a navigation tree on the left with 'Etherlike Statistics' selected. The main content area features a table of statistics for a chosen interface (Port g1, LAG 1). The table lists the following metrics and their values:

Frame Check Sequence (FCS) Errors	0
Single Collision Frames	0
Multiple Collision Frames	0
Signal Quality Error (SQE) Test Errors	0
Deferred Transmissions	0
Late Collisions	0
Excessive Collisions	0
Internal MAC Transmit Errors	0
Carrier Sense Errors	0
Oversize Packets	0
Internal MAC Receive Errors	0
Received Pause Frames	0
Transmitted Pause Frames	0

Additional controls include a 'Refresh Rate' dropdown set to 'No Refresh' and a 'Reset All Counters' button at the bottom of the table.

Interface (Интерфейс) - указывает, отображается статистика для порта или LAG.

Refresh Rate (Частота обновления) - период времени между обновлениями статистики интерфейса. Допустимые значения поля: No Refresh (Нет обновления), 15, 30 и 60 секунд.

Frame Check Sequence (FCS) Errors (Ошибки последовательности проверки кадра) - число ошибок последовательности проверки кадра, полученных на выбранный интерфейс.

Single Collision Frames (Кадры с одиночной коллизией) - число одиночных коллизий в кадрах, полученных на выбранный интерфейс.

Multiple Collision Frames (Кадры с множественными коллизиями) - число множественных коллизий в кадрах, полученных на выбранный интерфейс.

Single Quality Error (SQE) Test Errors (Ошибки проверки SQE) - число ошибок проверки SQE, полученных на выбранный интерфейс.

Deferred Transmissions (Отвергнутые передачи) - число отсроченных передач на выбранный интерфейс.

Late Collisions (Последние коллизии) - число последних коллизий, полученных на выбранный интерфейс.

Excessive Collisions (Чрезмерные коллизии) - число чрезмерных коллизий, полученных на выбранный интерфейс.

Internal MAC Transmit Errors (Внутренние ошибки передачи MAC) - число внутренних ошибок управления доступом к среде передачи (Internal MAC Transmit), полученных на выбранный интерфейс.

Carrier Sense Errors (Ошибки контроля несущей) - число ошибок контроля несущей, полученных на выбранный интерфейс.

Oversize Packets (Превышение размера пакетов) - число ошибок слишком длинных пакетов, полученных на выбранный интерфейс.

Internal MAC Receive Errors (Внутренние ошибки приема MAC) - число внутренних ошибок MAC-сигнала, полученных на выбранный интерфейс.

Receive Pause Frames (Принятые кадры паузы) - число ошибок паузы полученных на выбранный интерфейс.

Transmitted Paused Frames (Переданные кадры паузы) - число ошибок паузы, переданных на выбранный интерфейс.

Отображение статистики Etherlike для интерфейса

1. Откройте страницу **Etherlike Statistics** (Статистика Etherlike).
2. Выберите интерфейс в поле **Interface** (Интерфейс).
3. Щелкните **Query** (Запрос), чтобы отобразить статистику Etherlike интерфейса.

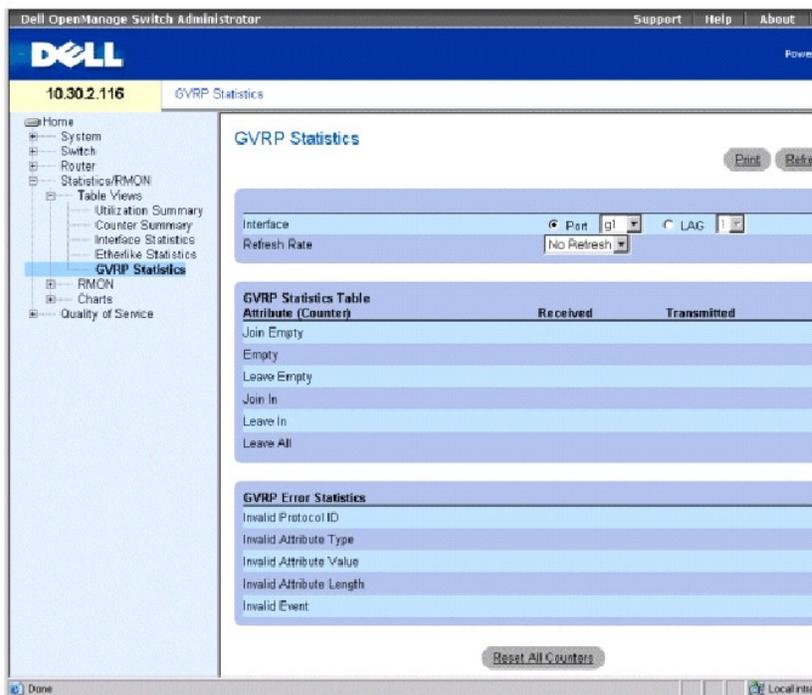
Сброс статистики Etherlike

1. Откройте страницу **Etherlike Statistics** (Статистика Etherlike).
2. Щелкните **Reset All Counters** (Сбросить все счетчики).

Просмотр статистики протокола GVRP

На странице **GVRP Statistics** (Статистика GVRP) показана статистика для протокола GVRP. Чтобы открыть эту таблицу, щелкните **Statistics/RMON** (Статистика/RMON) → **Table Views** (Просмотр в виде таблиц) → **GVRP Statistics** (Статистика интерфейса).

Рис. 9-5. Страница GVRP Statistics (Статистика GVRP)



Interface (Интерфейс) - указывает, отображается статистика для порта или LAG.

Refresh Rate (Частота обновления) - период времени между обновлениями статистики интерфейса. Допустимые значения поля: No Refresh (Нет обновления), 15, 30 и 60 секунд.

Join Empty(Объединить пустые) - статистика Join Empty протокола GVRP для устройства.

Empty (Пустые) - статистика Empty протокола GVRP для устройства.

Leave Empty (Оставлять пустые) - статистика Leave Empty протокола GVRP для устройства.

Join In (Присоединять) - статистика Join In протокола GVRP для устройства.

Leave In (Оставлять) - статистика Leave In протокола GVRP для устройства.

Leave All (Оставлять все) - статистика Leave all протокола GVRP для устройства.

Invalid Protocol ID (Недопустимый идентификатор протокола) - статистика Invalid Protocol ID протокола GVRP для устройства.

Invalid Attribute Type (Недопустимый тип атрибута) - статистика Invalid Attribute Type протокола GVRP для устройства.

Invalid Attribute Value (Недопустимое значение атрибута) - статистика Invalid Attribute Value протокола GVRP для устройства.

Invalid Attribute Length (Недопустимая длина атрибута) - статистика Invalid Attribute Length протокола GVRP для устройства.

Invalid Event - (Недопустимое событие) - статистика Invalid Event протокола GVRP для устройства.

Отображение статистики GVRP для порта:

1. Откройте страницу **GVRP Statistics** (Статистика GVRP).
2. Выберите интерфейс в поле **Interface** (Интерфейс).

Сброс статистики GVRP

1. Откройте страницу **GVRP Statistics** (Статистика GVRP).
2. Щелкните **Reset All Counters** (Сбросить все счетчики).

Просмотр статистики протокола GVRP с помощью команд консоли

В следующей таблице приведены команды консоли для просмотра статистики GVRP.

Таблица 9-2. Команды консоли для просмотра статистики GVRP

Команда консоли	Описание
	Отображает статистику протокола GVRP.

show gvrp statistics [ethernet интерфейс port-channel номер_канала_порта]	
	Отображает статистику ошибок протокола GVRP.
show gvrp error- statistics [ethernet интерфейс port-channel номер_канала_порта]	

Далее приведен пример команд консоли.

```
Console# show gvrp statistics
```

```
GVRP statistics:
```

```
-----
```

```
Legend:
```

```
rJE : Join Empty Received rJIn : Join In Received
```

```
rEmp : Empty Receivedr LIn : 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
```

```
-----
```

```
g1 0 0 0 0 0 0 0 0 0 0 0 0
```

```
g2 0 0 0 0 0 0 0 0 0 0 0 0
```

```
g3 0 0 0 0 0 0 0 0 0 0 0 0
```

```
g4 0 0 0 0 0 0 0 0 0 0 0 0
```

```
g5 0 0 0 0 0 0 0 0 0 0 0 0
```

```
g6 0 0 0 0 0 0 0 0 0 0 0 0
```

g7 0 0 0 0 0 0 0 0 0 0 0 0

g8 0 0 0 0 0 0 0 0 0 0 0 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

g1 0 0 0 0 0 0

g2 0 0 0 0 0 0

g3 0 0 0 0 0 0

g4 0 0 0 0 0 0

g5 0 0 0 0 0 0

g6 0 0 0 0 0 0

g7 0 0 0 0 0 0

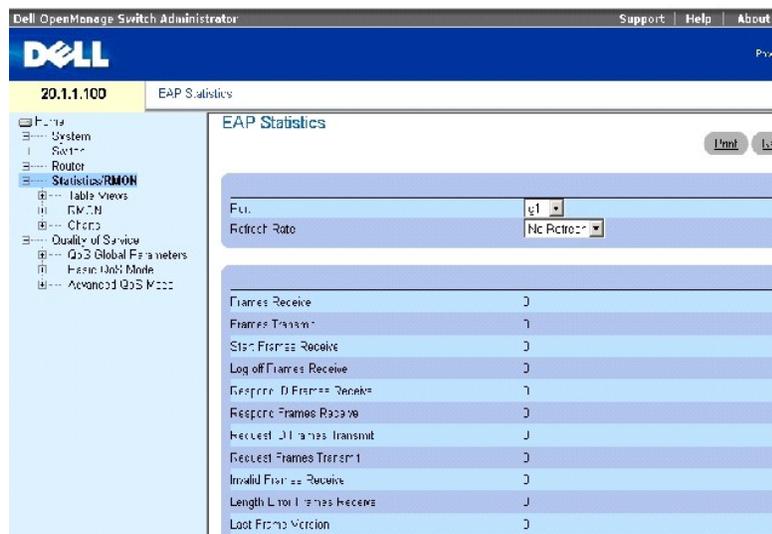
g8 0 0 0 0 0 0

Просмотр статистики EAP

Страница [EAP Statistics](#) (Статистика EAP) содержит сведения о пакетах EAP, полученных на определенный порт. Дополнительную информацию о EAP см. в разделе «[Проверка подлинности на основе порта \(802.1x\)](#)».

Чтобы открыть страницу [EAP Statistics](#) (Статистика EAP), щелкните Statistics/RMON (Статистика/RMON) → Table Views (Просмотр в виде таблиц) → EAP Statistics (Статистика интерфейса) на панели дерева.

Рис. 9-6. Страница EAP Statistics (Статистика EAP)



Страница [EAP Statistics](#) (Статистика EAP) содержит следующие поля.

Port (Порт) - опрашиваемый для статистики порт.

Refresh Rate (Частота обновления) - период времени между обновлениями статистики интерфейса.

Frames Receive (Получено кадров) - число верных кадров по протоколу EAPOL, полученных на порте.

Frames Transmit (Передано кадров) - число кадров по протоколу EAPOL, переданных через порт.

Start Frames Receive (Получено начальных кадров) - число кадров Start по протоколу EAPOL, полученных на порте.

Log off Frames Receive (Получено кадров разрегистрации) - число кадров Log off по протоколу EAPOL, полученных на порте.

Respond ID Frames Receive (Получено кадров с идентификаторами ответа) - число кадров Respond ID по протоколу EAP, полученных на порте.

Respond Frames Receive (Получено кадров ответа) - число верных кадров Respond по протоколу EAP, полученных на порте.

Request ID Frames Transmit (Передано кадров с идентификатором запроса) - число кадров Requested ID по протоколу EAP, переданных через порт.

Request Frames Transmit (Передано кадров запроса) - число кадров Request по протоколу EAP, переданных через порт.

Invalid Frames Receive (Получено неверный кадров) - число нераспознанных кадров по протоколу EAPOL, полученных на этом порте.

Length Error Frames Receive (Получено кадров с ошибкой длины) - число кадров по протоколу EAPOL с неверной длиной тела пакета, полученных на этом порте.

Last Frame Version (Версия последнего кадра) - номер версии протокола, указанный для последнего принятого кадра по протоколу EAPOL.

Last Frame Source (Источник последнего кадра) - MAC-адрес источника, указанный для последнего принятого кадра по протоколу EAPOL.

Отображение статистики EAP для порта

1. Откройте страницу [EAP Statistics](#) (Статистика EAP).
2. Выберите интерфейс в поле **Interface** (Интерфейс).

Отобразится статистика EAP интерфейса.

Просмотр статистики протокола EAP с помощью команд консоли

В следующей таблице приведены команды консоли для просмотра статистики интерфейса EAP.

Таблица 9-3. Команды консоли для просмотра статистики EAP

Команда консоли	Описание
show dot1x statistics ethernet <i>интерфейс</i>	Отображает статистику 802.1X для указанного интерфейса.

Далее приведен пример команд консоли.

```
console# show dot1x statistics ethernet g11

EapolFramesRx: 11

EapolFramesTx: 12

EapolStartFramesRx: 1

EapolLogoffFramesRx: 1

EapolRespIdFramesRx: 3

EapolRespFramesRx: 6

EapolReqIdFramesTx: 3
```

```
EapolReqFramesTx: 6  
  
InvalidEapolFramesRx: 0  
  
EapLengthErrorFramesRx: 0  
  
LastEapolFrameVersion: 1  
  
LastEapolFrameSource: 0008.3b79.8787
```

Просмотр статистики удаленного мониторинга RMON

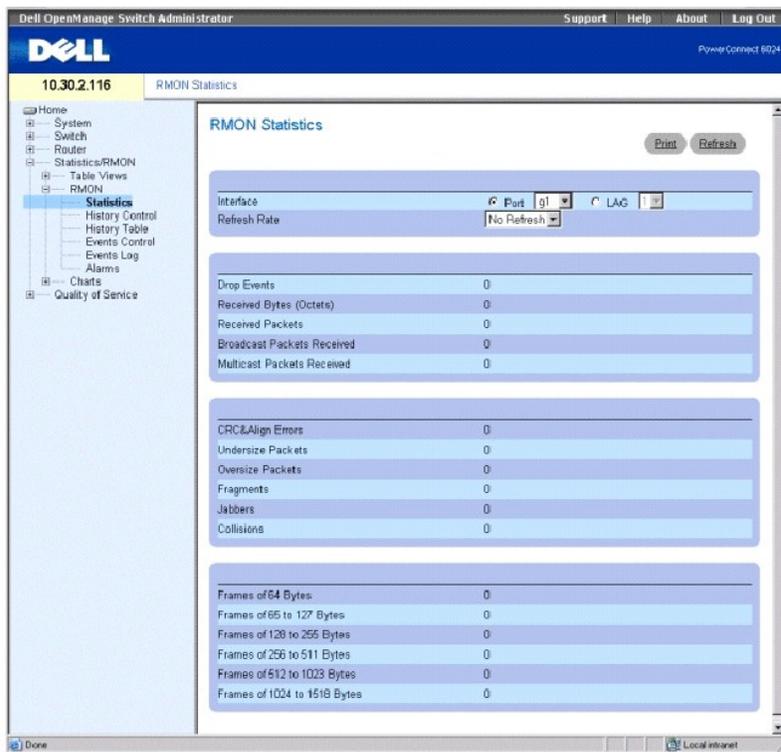
С помощью удаленного мониторинга (RMON) администраторы сети могут осуществлять удаленный доступ к информации. Чтобы открыть страницу RMON, щелкните **Statistics/RMON** (Статистика/RMON) → **RMON** на панели дерева.

Просмотр группы статистики RMON

Страница **RMON Statistics Group** (Группа статистики RMON) используется для отображения информации по использованию устройства и возникающих на нем ошибок.

Чтобы открыть страницу, выберите **Statistics/RMON** (Статистика/RMON) → **RMON** → **Statistics** (Статистика) на панели дерева.

Рис. 9-7. Страница RMON Statistics Group (Группа статистики RMON)



Interface (Интерфейс) - указывает порт или LAG, для которых отображается статистика.

Refresh Rate (Частота обновления) - период времени между обновлениями статистики интерфейса. Допустимые значения поля: No Refresh (Нет обновления), 15, 30 и 60 секунд.

Drop Events (Пропущенные события) - число событий, утерянных на интерфейсе с момента последнего сброса счетчиков.

Received Bytes (Octets) [(Получено байт (октетов))] - число октетов, полученных на интерфейс с момента последнего обновления устройства. Это число включает поврежденные пакеты и октеты FCS, но не включает биты фреймов.

Received Packets (Получено пакетов) - число пакетов, включая поврежденные пакеты, многоадресные и широковещательные пакеты, полученных с момента последнего обновления устройства.

Broadcast Packets Received (Получено широковещательных пакетов) - число хороших широковещательных пакетов, полученных на интерфейс с момента последнего обновления устройства. В это число не входят многоадресные пакеты.

Multicast Packets Received (Получено многоадресных пакетов) - число хороших многоадресных пакетов, полученных на интерфейс с момента последнего обновления устройства.

CRC & Align Errors (Ошибки контрольной суммы и выравнивания) - число ошибок контрольной суммы (CRC) и выравнивания, произошедших на интерфейсе с момента последнего обновления устройства.

Undersize Packets (Пакеты с размером меньше допустимого) - число пакетов с размером, меньше минимально допустимого (менее 64 октетов), полученных на интерфейс с момента последнего обновления устройства.

Oversize Packets (Превышение размера пакетов) - число пакетов с размером, больше максимально допустимого (более 1518 октетов), полученных на интерфейс с момента последнего обновления устройства.

Fragments (Фрагменты) - число фрагментов (пакеты размером менее 64 октетов, исключая биты кадров, но включая октеты FCS), полученных на интерфейс с момента последней очистки счетчиков.

Jabbers (Сбойные пакеты) - число пакетов, полученных во время сеанса выборки, с длиной больше 1518 октетов и содержащих контрольную последовательность кадра.

Collisions (Коллизии) - число коллизий, полученных на интерфейс с момента последнего обновления устройства.

Frames of xx Bytes - Number of xx (Кадры из xx байт) - число xx-байтовых кадров, полученных на интерфейс с момента последнего обновления устройства.

Просмотр статистики интерфейса

1. Откройте страницу **RMON Statistics Group** (Группа статистики RMON).
2. Выберите тип и номер интерфейса в поле **Interface** (Интерфейс).

Просмотр статистики удаленного мониторинга с помощью команд консоли

В следующей таблице приведены команды консоли для просмотра статистики удаленного мониторинга.

Таблица 9-4. Команды консоли для просмотра статистики RMON

Команда консоли	Описание
<code>show rmon statistics {ethernet интерфейс port-channel номер_канала_порта}</code>	Отображает статистику удаленного мониторинга по Ethernet.

Далее приведен пример команд консоли.

```
Console# show rmon statistics ethernet g1
```

```
Port g1
```

```
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

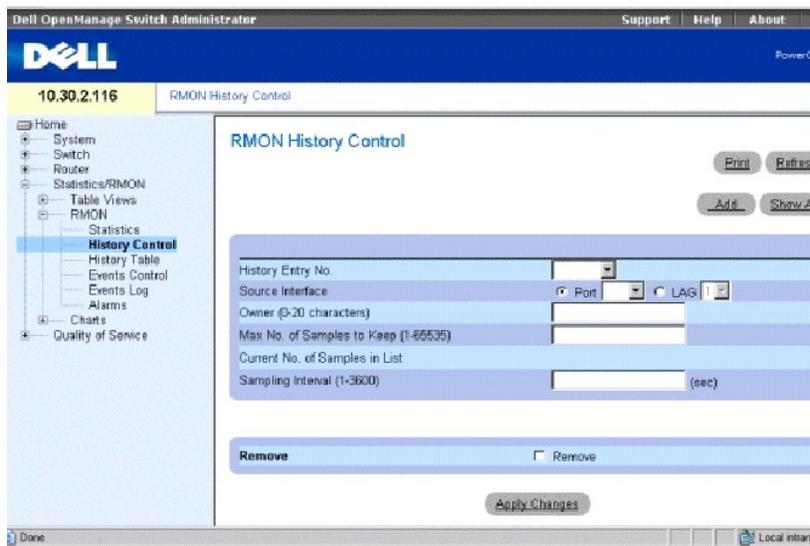
128 to 255 Octets: 0 256 to 511 Octets: 0

512 to 1023 Octets: 491 1024 to 1518 Octets: 389

Просмотр статистики управления журналом удаленного мониторинга

Страница **RMON History Control** (Управление журналом удаленного мониторинга) содержит информацию по выборкам данных удаленного мониторинга, полученных с портов. Например, в выборки могут входить определения интерфейса или интервалы опроса. Чтобы открыть страницу, выберите **Statistics/RMON** (Статистика/RMON) → **RMON** → **RMON History Control** (Управление журналом удаленного мониторинга) на панели дерева.

Рис. 9-8. Страница RMON History Control (Управление журналом удаленного мониторинга)



History Entry No. (Номер записи журнала) - номер записи в таблице управления журналом удаленного мониторинга.

Source Interface (Интерфейс-источник) - порт или LAG, из которых были получены выборки журнала.

Owner (Владелец) - станция удаленного мониторинга или пользователя, запросившего информацию по RMON.

Max No. of Samples to Keep (Максимальное число выборок для хранения) (1-65535) - число сохраняемых выборок. Значение по умолчанию: 50.

Current No. of Samples in List (Текущее число выборок) - текущее количество полученных выборок.

Sampling Interval (Интервал дискретизации) (1-3600) - время в секундах, за которое происходит выборка с портов. Возможные значения: 1-3600 сек. Значение по умолчанию: 1800 секунд (30 минут).

Remove (Удалить) - когда этот флажок установлен, запись удаляется из **History Control Table** (таблицы управления журналом).

Добавление записи управления журналом

1. Откройте страницу **RMON History Control** (Управление журналом удаленного мониторинга).
2. Нажмите кнопку **Add** (Добавить), чтобы отобразить страницу **Add History Entry** (Добавление записи журнала).
3. Введите значения в полях диалогового окна и нажмите кнопку **Apply Changes** (Применить изменения).

Запись будет добавлена в **History Control Table** (таблицу управления журналом).

Изменение записи в RMON History Control Table (Таблице управления журналом удаленного мониторинга)

1. Откройте страницу **RMON History Control** (Управление журналом удаленного мониторинга).
2. Выберите запись в поле **History Entry No.** (Номер таблицы журнала).
3. Измените поля, как необходимо, и нажмите кнопку **Apply Changes** (Применить изменения).

Запись таблицы изменяется, а устройство обновляется.

Удаление записи таблицы управления журналом

1. Откройте страницу **RMON History Control** (Управление журналом удаленного мониторинга).
2. Выберите запись в поле **History Entry No.** (Номер таблицы журнала).
3. Установите флажок **Remove** (Удалить), а затем нажмите кнопку **Apply Changes** (Применить изменения).

Запись таблицы будет удалена, а устройство обновлено.

Просмотр управления журналом удаленного мониторинга с помощью команд консоли

В следующей таблице приведены команды консоли для просмотра статистики GVRP.

Таблица 9-5. Команды консоли журнала удаленного мониторинга

Команда консоли	Описание
<code>rmon collection history индекс [owner имя владельца buckets номер_блока] [interval секунды]</code>	Включает и настраивает удаленный мониторинг на интерфейсе.
<code>show rmon collection history [ethernet интерфейс port-channel номер_канала_порта]</code>	Отображает статистику журнал совокупности удаленного мониторинга.

Далее приведен пример команд консоли.

```
Console (config)# interface ethernet g8
```

```
Console (config-if)# rmon collection history 1 interval 2400
```

```
Console(config-if)# exit
```

```
Console(config)# exit
```

```
Console# disable
```

```
Console> show rmon collection history
```

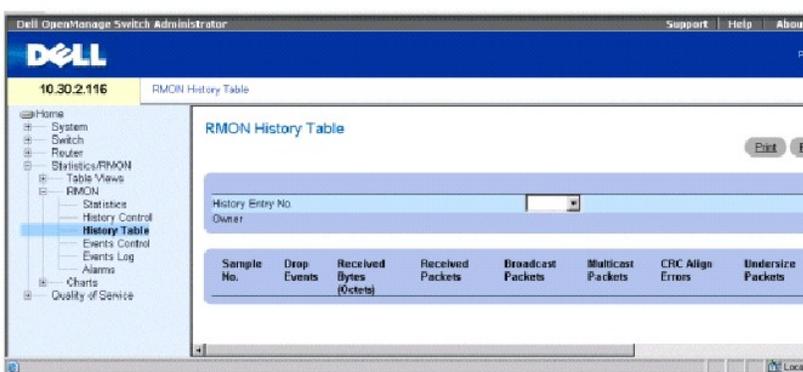
```
Index Interface Interval Requested Samples Granted Samples Owner
```

```
-----  
1 1 10 0 50 50 CLI
```

Просмотр журнала удаленного мониторинга

Страница RMON History Table (Журнал удаленного мониторинга) содержит статистические сетевые выборки для конкретного интерфейса. Каждая запись таблицы представляет собой все значения счетчиков, скомпилированные в течение однократной выборки. Чтобы открыть страницу RMON History Table, выберите Statistics/RMON→ (Статистика/RMON) RMON→ History Table (Таблица журнала) на панели дерева.

Рис. 9-9. RMON History Table (Таблица журнала удаленного мониторинга)



ПРИМЕЧАНИЕ. В таблице RMON History (Журнал удаленного мониторинга) показаны не все поля.

History Entry No. (Номер записи журнала) - содержит список номеров записей в таблице RMON History Control Table (Таблице управления журналом удаленного мониторинга).

Owner (Владелец) - указывает имя владельца группы статистики удаленного мониторинга, если доступна.

Sample No. (Номер выборки) - указывает определенную выборку, которую отражает информация в таблице.

Drop Events (Потерянные события) - число пакетов, потерянных из-за нехватки сетевых ресурсов в течение интервала выборки. Так как указать точное количество потерянных пакетов невозможно, то указывается, сколько раз были обнаружены потерянные пакеты.

Received Bytes (Octets) (Полученные байты (Октеты)) - число октетов данных, включая поврежденные пакеты, полученные по сети.

Received Packets (Полученные пакеты) - число пакетов, полученных во время интервала выборки.

Broadcast Packets (Широковещательные пакеты) - число корректных широковещательных пакетов, полученных во время интервала выборки.

Multicast Packets (Многоадресные пакеты) - число корректных многоадресных пакетов, полученных во время интервала выборки.

CRC Align Errors (Ошибки выравнивания CRC) - число пакетов, полученных во время сеанса выборки с длиной в 64-1518 октетов. Однако пакеты имеют неверную последовательность проверки кадра (FCS) с целым числом октетов или неверную FCS с нецелым числом.

Undersize Packets (Пакеты с размером меньше допустимого) - число пакетов, полученных во время сеанса выборки, с длиной меньше 64 октетов.

Oversize Packets (Пакеты с размером больше допустимого) - число пакетов, полученных во время сеанса выборки, с длиной больше 1518 октетов.

Fragments (Фрагменты) - число пакетов, полученных во время сеанса выборки, с длиной меньше 64 октетов и содержащих контрольную последовательность кадра.

Jabbers (Сбойные пакеты) - число пакетов, полученных во время сеанса выборки, с длиной больше 1518 октетов и содержащих контрольную последовательность кадра.

Collisions(Коллизии) - оценка общего количества коллизий пакетов, имевших место во время сеанса выборки. Коллизии обнаруживаются, когда порты повторителя засекают одновременную передачу с двух или более станций.

Utilization (Использование) - оценка степени использования главного физического уровня сети на интерфейсе во время сеанса выборки. Это значение отображается сотыми долями процента.

Просмотр статистики для определенной записи журнала

1. Откройте страницу **RMON History Table** (Журнал удаленного мониторинга).
2. Выберите запись в поле **History Entry No.** (Номер таблицы журнала).

Статистика записей будет отображена в таблице RMON History (Журнал удаленного мониторинга).

Просмотр управления журналом удаленного мониторинга с помощью команд консоли

В следующей таблице приведены команды консоли для просмотра журнала удаленного мониторинга.

Таблица 9-6. Команды консоли для управления журналом удаленного мониторинга

Команда консоли	Описание
show rmon history индекс {throughput errors other} [period сек]	Отображает журнал статистики удаленного мониторинга Ethernet.

Далее приведен пример команд консоли для отображения статистики удаленного мониторинга Ethernet для пропускной способности по индексу 1:

```
Console# show rmon history 1 throughput
```

```
Sample Set: 5 Owner: cli
```

Interface: 24 interval: 10

Requested samples: 50 Granted samples: 50

Maximum table size: 270

Time Octets Packets Broadcast Multicast %

09-Mar-2003 18:29:32 0 0 0 0 0

09-Mar-2003 18:29:42 0 0 0 0 0

09-Mar-2003 18:29:52 0 0 0 0 0

09-Mar-2003 18:30:02 0 0 0 0 0

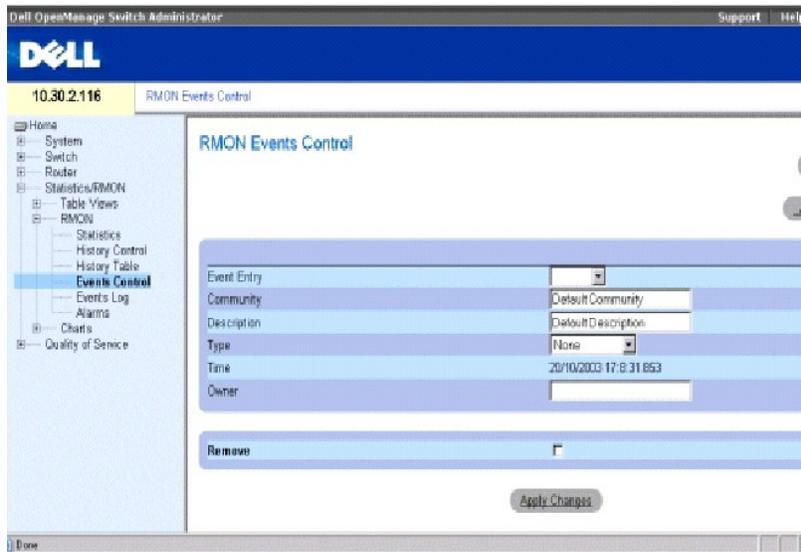
09-Mar-2003 18:30:12 0 0 0 0 0

09-Mar-2003 18:30:22 0 0 0 0 0

Определение событий удаленного мониторинга устройства

Используйте страницу R MON Events Control (Управление событиями удаленного мониторинга) для определения событий удаленного мониторинга. Чтобы открыть страницу, выберите Statistics/RMON (Статистика/RMON) → RMON → Events Control (Управление событиями) на панели дерева.

Рис. 9-10. Страница RMON Events Control (Управление событиями удаленного мониторинга)



Event Entry (Запись события) - указывает событие.

Community (Сообщество) - сообщество SNMP, к которому принадлежит событие.

Description (Описание) - описание события, определяемое пользователем.

Type (Тип) - тип события. Возможные значения:

Log (Журнал) - тип события - запись в журнале.

Trap (Прерывание) - тип события - прерывание.

Log and Trap (Журнал и прерывание) - тип события - запись в журнале и прерывание.

None (Нет) - событие отсутствует.

Time (Время) - время, когда произошло событие.

Owner (Владелец) - устройство или пользователь, который определил событие.

Remove (Удалить) - когда установлен этот флажок, событие удаляется из таблицы событий Events Table.

Добавление события удаленного мониторинга

1. Откройте страницу **RMON Events Control** (Управление событиями удаленного мониторинга).
2. Нажмите кнопку **Add** (Добавить), чтобы отобразить страницу **Add an Event Entry** (Добавление записи журнала).
3. Введите данные в диалоговом окне и нажмите кнопку **Apply Changes** (Применить изменения).

Событие будет добавлено в RMON Event Table (Таблицу событий удаленного мониторинга), а устройство обновлено.

Изменение события удаленного мониторинга

1. Откройте страницу RMON Events Control (Управление событиями удаленного мониторинга).
2. Выберите запись в поле Event Entry (Запись события).
3. Измените значения в полях на странице и нажмите кнопку Apply Changes (Применить изменения).

Запись таблицы RMON Events Table (Таблица событий удаленного мониторинга) будет изменена, а устройство обновлено.

Удаление записей о событиях удаленного мониторинга

1. Откройте страницу RMON Events Control (Управление событиями удаленного мониторинга).
2. Нажмите кнопку Show All (Показать все), чтобы открыть таблицу RMON Events Table (Таблицу событий удаленного мониторинга).
3. Установите флажок Remove (Удалить) для событий, которые необходимо удалить, а затем нажмите кнопку Apply Changes (Применить изменения).

Запись таблицы будет удалена, а устройство обновлено.



ПРИМЕЧАНИЕ. Можно удалить запись одного события со страницы RMON Events Control (Управление событиями удаленного мониторинга) с помощью флажка Remove (Удалить) на этой странице.

Определение событий устройств с помощью команд консоли

В следующей таблице приведены команды консоли для определения событий устройств.

Таблица 9-7. Команды консоли для определения событий устройств

Команда консоли	Описание
<code>rmon event тип_индекса [community текст] [description текст] [owner имя]</code>	Настраивает события удаленного мониторинга.
<code>show rmon events</code>	Отображает таблицу событий удаленного мониторинга.

Далее приведен пример команд консоли.

```
Console (config)# rmon event 10 log
```

```
Console(config)# exit
```

```
Console# disable
```

```
Console> show rmon events
```

```
Index Description Type Community Owner Last time sent
```

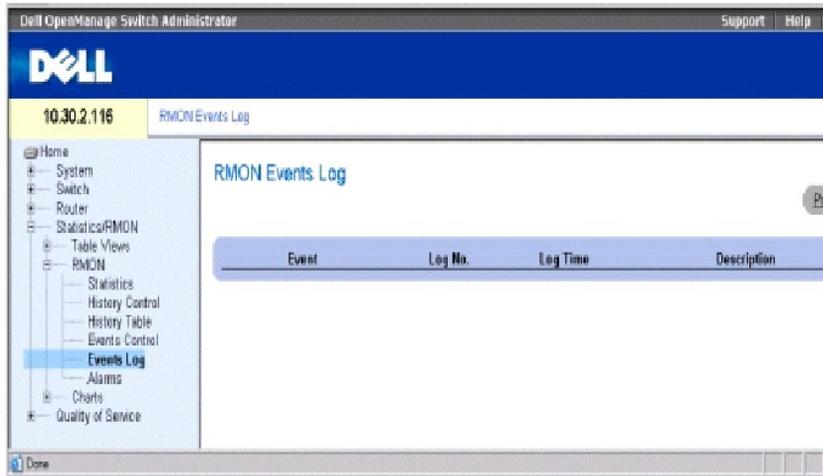
1 Errors Log CLI Jan 18 2002 23:58:17

2 High Broadcast Log-Trap router Manager Jan 18 2002 23:59:48

Просмотр журнала событий удаленного мониторинга

На странице **RMON Events Log** (Журнал событий удаленного мониторинга) представлен список событий удаленного мониторинга. Чтобы открыть страницу, выберите **Statistics/RMON** (Статистика/RMON) → **RMON** → **Events Log** (События) на панели дерева.

Рис. 9-11. Страница RMON Events Log (Журнал событий удаленного мониторинга)



Event (Событие) - номер записи в журнале событий удаленного мониторинга.

Log No. (№ журнала) - номер журнала.

Log Time (Время записи) - время внесения записи в журнал.

Description (Описание) - описывает запись в журнале.

Определение событий устройств с помощью команд консоли

В следующей таблице приведены команды консоли для определения событий устройств.

Таблица 9-8. Команды консоли для определения событий устройств

Команда консоли	Описание
<code>show rmon log [событие]</code>	Отображает таблицу журнала событий удаленного мониторинга.

Далее приведен пример команд консоли.

```
Console> show rmon log
```

```
Maximum table size: 500
```

```
Event Description Time
```

```
-----
```

```
1 Errors Jan 18 2002 23:48:19
```

```
1 Errors Jan 18 2002 23:58:17
```

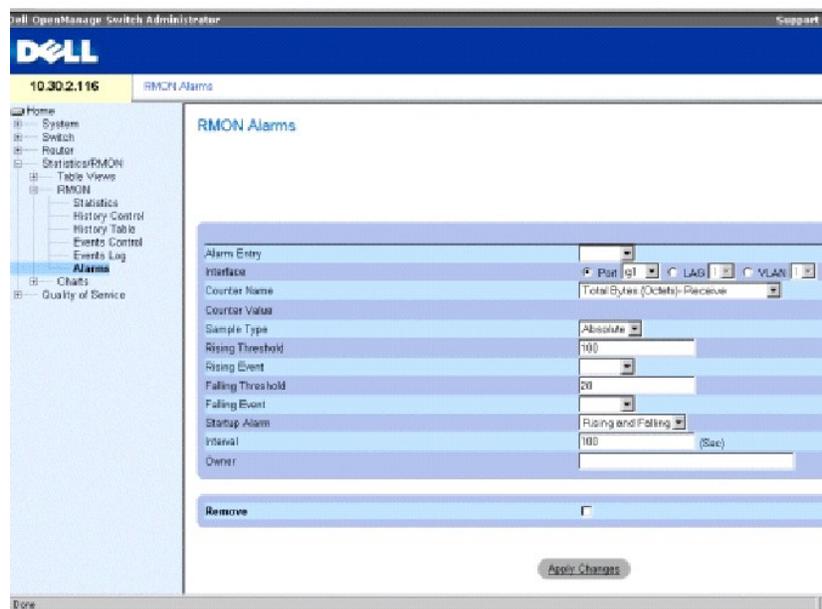
```
2 High Broadcast Jan 18 2002 23:59:48
```

Определение сигналов устройств удаленного мониторинга

Для настройки сетевых сигналов используйте страницу **RMON Alarms** (Сигналы удаленного мониторинга). Сетевая тревога происходит при обнаружении проблемы или события в сети. При повышении или понижении пороговых величин генерируются события. Для получения дополнительной информации о событиях см. раздел «[Просмотр журнала событий удаленного мониторинга](#)».

Чтобы открыть страницу, выберите **Statistics/RMON** (Статистика/RMON) → **RMON** → **Alarms** (Сигналы) на панели дерева.

Рис. 9-12. Страница RMON Alarms (Сигналы удаленного мониторинга)



Alarm Entry (Запись сигнала) - показывает определенный сигнал.

Interface (Интерфейс) - указывает порт, для которого отображается статистика RMON.

Counter Name (Имя счетчика) - показывает выбранную переменную MIB.

Counter Value (Значение счетчика) - значение выбранной переменной MIB.

Sample Type (Тип выборки) - определяет метод выборки для выбранной переменной и сравнивает значение с пороговыми величинами. Возможные значения:

Delta (Разность) - вычитается последнее значение выборки из текущего значения. Разница значений сравнивается с пороговой величиной.

Absolute (Абсолютное значение) - сравнивает значения с пороговыми величинами в конце интервала выборки.

Rising Threshold (Превышение порога) - значение счетчика превышения, активизирующее сигнал превышения верхней пороговой величины. Верхнее пороговое значение отображается в верхней части столбчатых диаграмм. Каждая контролируемая переменная обозначена цветом.

Rising /Falling Event (Событие увеличения/уменьшения) - механизм, который используется для выдачи сигналов LOG, TRAP или комбинация обоих. Если выбран LOG, то механизма сохранения нет ни на устройстве, ни в системе управления. Однако если не происходит перезагрузки устройства, то сигнал тревоги остается в таблице LOG устройства. Если выбран параметр TRAP, генерируется прерывание SNMP и сообщается через общий механизм прерывания. Можно сохранить TRAP с помощью этого же механизма.

Falling Threshold (Ниже порога) - значение счетчика понижений, активизирующее тревогу нарушения нижней пороговой величины. Нижнее пороговое значение графически отображается в верхней части столбчатых диаграмм. Каждая контролируемая переменная обозначена цветом.

Startup Alarm (Запуск сигнала) - переключатель, активизирующий генерацию сигнала. Превышение определяется переход пороговой величины от нижнего значения порога к верхнему.

Interval (sec) (Интервал (сек) - время интервала между сигналами.

Owner (Владелец) - устройство или пользователь, который определил сигнал.

Remove (Удалить) - когда этот флажок установлен, сигнал удаленного мониторинга отключается.

Добавление записи в таблицу сигналов

1. Откройте страницу **RMON Alarms** (Сигналы удаленного мониторинга).
2. Нажмите кнопку **Add** (Добавить), чтобы отобразить страницу **Add an Alarm Entry** (Добавление записи журнала).

Рис. 9-13. Страница Add an Alarm Entry (Добавление записи журнала)

The screenshot shows a web browser window titled "Add an Alarm Entry - Microsoft Internet Explorer". The page content is a form titled "Add an Alarm Entry". The form fields are as follows:

- Alarm Entry: 1
- Interface: Port g1 (selected from a dropdown menu)
- Counter Name: Total Bytes (Octets)-Receive (selected from a dropdown menu)
- Sample Type: Absolute (selected from a dropdown menu)
- Rising Threshold: 100 (text input)
- Rising Event: (empty dropdown menu)
- Falling Threshold: 20 (text input)
- Falling Event: (empty dropdown menu)
- Startup Alarm: Rising and Falling (selected from a dropdown menu)
- Interval: 100 (text input)
- Owner: (empty text input)

Buttons: "Refresh" (top right) and "Apply Changes" (bottom center).

3. Выберите интерфейс.
4. Введите значения в полях диалогового окна и нажмите кнопку **Apply Changes** (Применить изменения).

Сигнал удаленного мониторинга будет добавлен, а устройство обновлено.

Изменение записи в таблице сигналов

1. Откройте страницу **RMON Alarms** (Сигналы удаленного мониторинга).
2. Выберите запись в раскрывающемся меню **Alarm Entry** (Запись сигнала).
3. Измените значения в полях диалогового окна и нажмите кнопку **Apply Changes** (Применить изменения).

Запись будет изменена, а устройство обновлено.

Отображение таблицы сигналов

1. Откройте страницу **RMON Alarms** (Сигналы удаленного мониторинга).
2. Нажмите кнопку **Show All** (Показать все), чтобы открыть таблицу **RMON Alarms Table** (Таблицу сигналов).

Удаление записи в таблице сигналов

1. Откройте страницу **RMON Alarms** (Сигналы удаленного мониторинга).
2. Выберите запись в раскрывающемся меню **Alarm Entry** (Запись сигнала).
3. Установите флажок **Remove** (Удалить) и нажмите кнопку **Apply Changes** (Применить изменения).

Запись будет удалена, а устройство обновлено.

Определение сигналов устройств с помощью команд консоли

В следующей таблице приведены команды консоли для определения сигналов устройств.

Таблица 9-9. Команды консоли для сигналов устройств

--	--

Команда консоли	Описание
<code>rmon alarm индекс MIB_Object_ID interval rthreshold fthreshold revent fevent [type тип] [startup направление] [owner имя владельца]</code>	Настраивает условия выдачи сигналов удаленного мониторинга.
<code>show rmon alarm-table</code>	Отображает сводную таблицу сигналов.
<code>show rmon alarm</code>	Отображает конфигурацию сигналов удаленного мониторинга.

Далее приведен пример команд консоли.

```
Console (config)# rmon alarm 1000 1.3.6.1.2.1.2.2.1.10.1 360000 1000000 1000000 10 20
```

```
Console# show rmon alarm-table
```

```
Index OID Owner
```

```
-----
```

```
1 1.3.6.1.2.1.2.2.1.10.1 CLI
```

```
2 1.3.6.1.2.1.2.2.1.10.1 Manager
```

```
3 1.3.6.1.2.1.2.2.1.10.9 CLI
```

Просмотр диаграмм

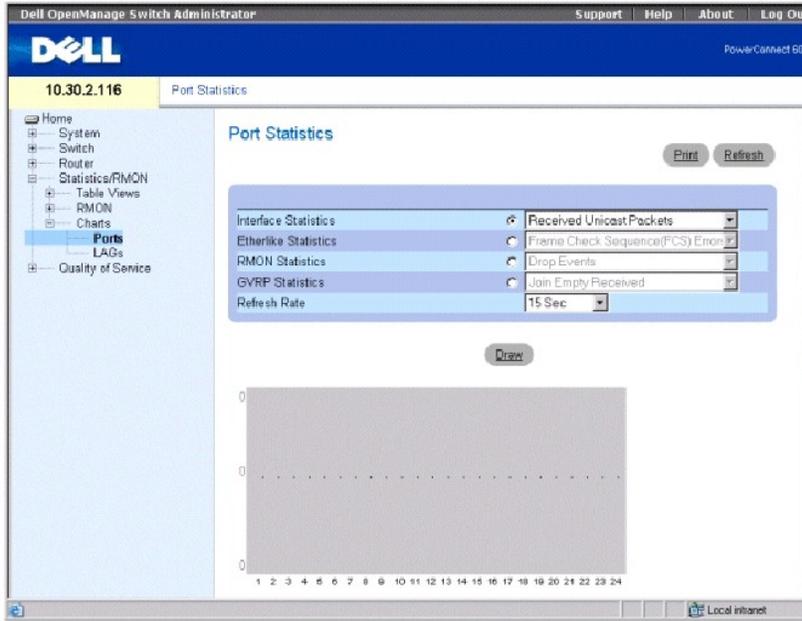
На странице [Chart \(Диаграммы\)](#) содержатся ссылки для отображения статистики в виде диаграммы. Чтобы открыть страницу, щелкните [Statistics/RMON \(Статистика RMON\)](#) → [Charts \(Диаграммы\)](#) на панели дерева.

Просмотр статистики портов

Для отображения статистики в виде диаграмм для элементов порта используйте страницу [Port Statistics \(Статистика портов\)](#).

Чтобы открыть страницу, выберите [Statistics/RMON \(Статистика/RMON\)](#) → [Charts \(Диаграммы\)](#) → [Ports \(Порты\)](#) на панели дерева.

Рис. 9-14. Страница Port Statistics (Статистика порта)



Interface Statistics (Статистика интерфейса) - выбор типа статистики интерфейса для отображения.

Etherlike Statistics (Статистика Etherlike) - выбор типа статистики Etherlike для отображения.

RMON Statistics (Статистика удаленного мониторинга) - выбор типа статистики удаленного мониторинга для отображения.

GVRP Statistics (Статистика GVRP) - выбор типа статистики GVRP для отображения.

Refresh Rate (Частота обновления) - период времени между обновлениями статистики интерфейса. Допустимые значения поля: No Refresh (Нет обновления), 15, 30 и 60 секунд.

Отображение статистики для порта

1. Откройте страницу **Port Statistics** (Статистика порта).
2. Выберите тип статистики для отображения.
3. Выберите необходимую частоту обновления в раскрывающемся меню **Refresh Rate** (Частота обновления).
4. Нажмите кнопку **Draw** (Нарисовать).

Отобразится график для выбранной статистики.

Просмотр статистики порта с помощью команд консоли

В следующей таблице приведены команды консоли для просмотра статистики портов.

Таблица 9-10. Команды консоли статистики портов

--	--

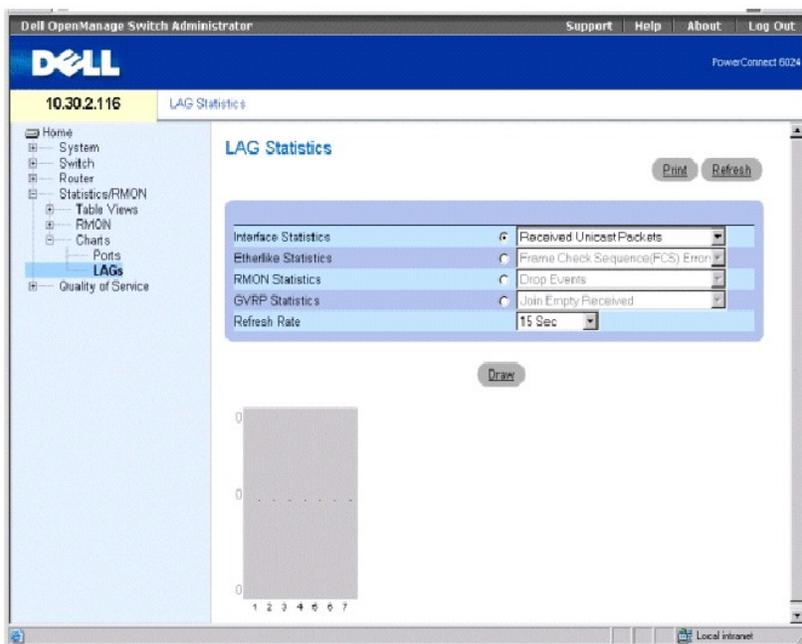
Команда консоли	Описание
show interfaces counters {ethernet интерфейс port- channel номер_канала_порта}	Отображает трафик, видимый физическим интерфейсом.
show rmon statistics {ethernet интерфейс port-channel номер_канала_порта}	Отображает статистику удаленного мониторинга по Ethernet.
show gvrp statistics {ethernet интерфейс port-channel номер_канала_порта}	Отображает статистику протокола GVRP.
show gvrp-error statistics {ethernet интерфейс port- channel номер_канала_порта}	Отображает статистику ошибок протокола GVRP.

Просмотр статистики группы LAG

Для отображения статистики в виде диаграмм для групп LAG используйте страницу **LAG Statistics** (Статистика LAG).

Чтобы открыть страницу, выберите **Statistics/RMON** (Статистика/RMON) → **Charts** (Диаграммы) → **LAGs** (Группы LAG) на панели дерева.

Рис. 9-15. Страница LAG Statistics (Статистика групп LAG)



Interface Statistics (Статистика интерфейса) - выбор типа статистики интерфейса для отображения.

Etherlike Statistics (Статистика Etherlike) - выбор типа статистики Etherlike для отображения.

RMON Statistics (Статистика удаленного мониторинга) - выбор типа статистики удаленного мониторинга для отображения.

GVRP Statistics (Статистика GVRP) - выбор типа статистики GVRP для отображения.

Refresh Rate (Частота обновления) - период времени между обновлениями статистики интерфейса. Допустимые значения поля: No Refresh (Нет обновления), 15, 30 и 60 секунд.

Отображение статистики LAG

1. Откройте страницу **LAG Statistics** (Статистика LAG).
2. Выберите тип статистики для отображения.
3. Выберите необходимую частоту обновления в раскрывающемся меню **Refresh Rate** (Частота обновления).
4. Нажмите кнопку **Draw** (Нарисовать).

Отобразится график для выбранной статистики.

Просмотр статистики LAG с помощью команд консоли

В следующей таблице приведены команды консоли для просмотра статистики LAG.

Таблица 9-11. Команды консоли для статистики LAG

Команда консоли	Описание
<code>show interfaces counters {ethernet интерфейс port- channel номер_канала_порта}</code>	Отображает трафик, видимый физическим интерфейсом.
<code>show rmon statistics {ethernet интерфейс port-channel номер_канала_порта}</code>	Отображает статистику удаленного мониторинга по Ethernet.
<code>show gvrp statistics {ethernet интерфейс port-channel номер_канала_порта}</code>	Отображает статистику протокола GVRP.
<code>show gvrp-error statistics {ethernet интерфейс port- channel номер_канала_порта}</code>	Отображает статистику ошибок протокола GVRP.

[Назад на страницу Содержание](#)