Руководство пользователя систем Dell™ PowerConnect™ 54xx

Примечания и предупреждения

ПРИМЕЧАНИЕ. ПРИМЕЧАНИЕ указывает важную информацию, которая необходима для содействия пользователю при работе с компьютером.

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

ОСТОРОЖНЫ. Сообщение БУДЬТЕ ОСТОРОЖНЫ указывает на возможность материального ущерба, травмы или летального исхода.

Декабрь 2008 Ред. A01

Назад на страницу Содержание

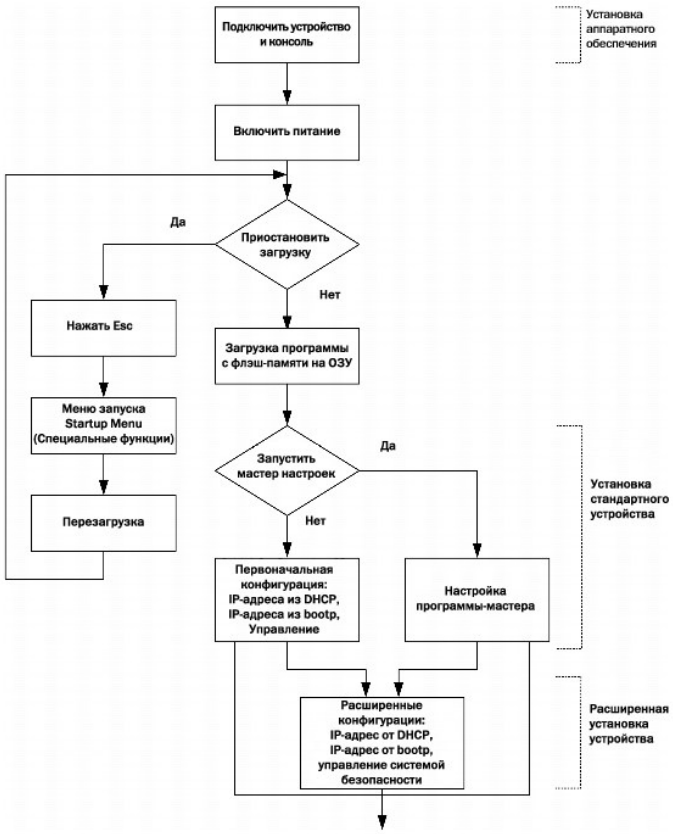
Запуск и настройка устройства

Руководство пользователя систем Dell™ PowerConnect™ 54xx

После выполнения всех внешних подключений подключите к устройству терминал для настройки устройства и других процедур. В качестве начальной настройки выполняется стандартная настройка устройства.

ПРИМЕЧАНИЕ. Перед выполнением дальнейших действий прочтите примечания к выпуску для этого продукта. Примечания к выпуску можно загрузить с веб-сайта **www.support.dell.com**.

Рис. 4-1. Процесс установки и настройки



Настройка терминала

Для настройки устройства необходимо запустить на терминале программу эмуляции терминала.

Настройте программу эмуляции терминала следующим образом.

1. Выберите соответствующий последовательный порт (последовательный порт 1 или последовательный порт 2) для подключения к консоли.
2. Задайте скорость передачи данных 9600 бод.
3. Задайте следующий формат данных: 8-битные данные, 1 стоповый бит, без контроля четности.

4. Присвойте управлению потоком значение **none** (нет).
5. В разделе **Properties** (Параметры) выберите режим **VT100 for Emulation** (Эмуляции VT100).
6. Выберите значение **Terminal keys** (Клавиши терминала) для **Function** (Функциональные клавиши), **Arrow** (Клавиши со стрелками) и **Ctrl**. Убедитесь, что выбраны **Клавиши терминала**, а не **Клавиши Windows**.

ПРЕДУПРЕЖДЕНИЕ. При использовании терминала HyperTerminal с операционной системой Microsoft® Windows 2000 убедитесь, что установлен пакет обновления 2 для Windows® 2000 или более поздней версии. Если пакет обновления установлен, клавиши со стрелками правильно работают в программе эмуляции HyperTerminal VT100. Информацию о пакетах обновления для Windows 2000 можно найти на сайте www.microsoft.com.

Загрузка устройства

ПРИМЕЧАНИЕ. Основные сведения по загрузке.

- Устройство поставляется с конфигурационными настройками по умолчанию.
- Имя пользователя и пароль по умолчанию в конфигурации устройства не заданы.

Для загрузки устройства выполните следующие действия.

1. Убедитесь, что серийный порт устройства подсоединен к терминалу ASCII или к разъему последовательного интерфейса настольного компьютера, на котором установлено программное обеспечение эмуляции терминала.
2. Найдите розетку питания переменного тока.
3. Обесточьте розетку питания переменного тока.
4. Подключите устройство к розетке переменного тока. См. раздел Подключение устройства к источнику питания.
5. Подайте напряжение на розетку переменного тока.

При включении питания с подключенным локальным терминалом устройство 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.

1. Убедитесь, что кабель ASCII подсоединен к терминалу и параметры программного обеспечения эмуляции настроены правильно.
2. Подсоедините источник питания к устройству.
3. Включите питание устройства.
4. При загрузке устройства в ходе выполнения теста определяется объем доступной памяти устройства, а затем продолжается загрузка. Далее приведен пример экрана теста POST:

```
------ Performing the Power-On Self Test (POST) ------

UART Channel Loopback Test.....................PASS

Testing the System SDRAM.......................PASS

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

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

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

BOOT Software Version 1.0.0.20 Built 22-Jan-xxxx 15:09:28

Processor: FireFox 88E6218 ARM946E-S, 64 MByte SDRAM.

I-Cache 8 KB. D-Cache 8 KB. Cache Enabled.

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

Preparing to decompress...
```

Процесс загрузки длится около 90 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.

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.

```
Decompressing SW from image-2

78c000

OK

Running from RAM...

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

*** Running SW Ver. x.x.x.x Date 12-Jul-xxxx Time 16:51:25 ***

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

HW version is 1

Base Mac address is: 00:15:77:12:34:56

Dram size is: 64M bytes

Dram first block size is: 47104K bytes

Dram first PTR is: 0x1200000

Flash size is: 16M

01-Jan-xxxx 01:01:07 %CDB-I-LOADCONFIG: Loading running configuration.

01-Jan-xxxx 01:01:07 %CDB-I-LOADCONFIG: Loading startup configuration.

Device configuration:

CPLD revision: 07

Slot 1 - PowerConnect 5448

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

-- Unit Standalone --

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

Run eeprom code for asic 0

Run eeprom code for asic 1

Tapi Version: v1.3.3.1

Core Version: v1.3.3.1

01-Jan-xxxx 01:01:59 %INIT-I-InitCompleted: Initialization task is completed

01-Jan-xxxx 01:02:00 %SNMP-I-CDBITEMSNUM: Number of running configuration items loaded: 0

01-Jan-xxxx 01:02:00 %SNMP-I-CDBITEMSNUM: Number of startup configuration items loaded: 0

01-Jan-xxxx 01:02:01 %Box-I-SFP-PRESENT-CHNG: unit_id 1 SFP 0 status is not present.

01-Jan-xxxx 01:02:01 %Box-I-SFP-PRESENT-CHNG: unit_id 1 SFP 1 status is not present.

01-Jan-xxxx 01:02:01 %Box-I-SFP-PRESENT-CHNG: unit_id 1 SFP 2 status is not present.

01-Jan-xxxx 01:02:01 %Box-I-SFP-PRESENT-CHNG: unit_id 1 SFP 3 status is not present.
```

После успешной загрузки коммутатора появится системное приглашение (console>), используемое для настройки устройства. Однако перед настройкой коммутатора необходимо убедиться, что на устройстве установлена последняя версия программного обеспечения. Если установлена не последняя версия, загрузите и установите последнюю версию. Подробную информацию о том, как загрузить последнюю версию, см. в разделе Загрузка программного обеспечения.

Начальная настройка

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

ПРИМЕЧАНИЕ. Конфигурация по умолчанию предполагает следующее.

- Устройство PowerConnect ранее не конфигурировалось и находится в том же состоянии, в котором оно было получено.
- Загрузка устройства PowerConnect прошла успешно.
- Установлено соединение консоли, а на экране терминала устройства VT100 отображается приглашение консоли.

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

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

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

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

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

Мастер настройки настраивает следующие поля.

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

Отобразится следующее:

```
Welcome to Dell Easy Setup Wizard

The Setup Wizard guides you through the initial switch configuration, and gets you up and running as quickly as possible. You can skip
the setup wizard, and enter CLI mode to manually configure the switch.
The system will prompt you with a default answer; by pressing enter, you accept the default.
You must respond to the next question to run the setup wizard within 60 seconds, otherwise the system will continue with normal operation
using the default system configuration.

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

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

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

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

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

Мастера настройки - шаг 1

Отобразится следующее:

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

Setup the initial SNMP version 2 account now.

Return later and setup additional SNMP v1/v3 accounts.

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

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

Введите [N], чтобы пропустить шаг 2.

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

```
To setup the SNMP management account you must specify the management system IP address and the "community string" or password that the
particular management system uses to access the switch. The wizard automatically assigns the highest access level [Privilege Level 15] to
this account.
You can use Dell Network Manager or CLI to change this setting, and to add additional management systems. For more information on adding
management systems, see the user documentation.
To add a management station:
Please enter the SNMP community string to be used: [Dell_Network_Manager]
Please enter the IP address of the Management System (A.B.C.D) or wildcard (0.0.0.0) to manage from any Management Station: [0.0.0.0]
```

Введите следующие сведения.

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

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

Нажмите клавишу **Enter**.

Мастер настройки - шаг 2

Отобразится следующее:

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

Введите следующие сведения.

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

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

Нажмите клавишу **Enter**.

Мастер настройки - шаг 3

Отобразится следующее:

```
Next, an IP address is setup.

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

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

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

Enter the IP address and IP subnet mask, for example 1.1.1.1 as the IP address and 255.255.255.0 as the IP subnet mask.

Нажмите клавишу **Enter**.

Мастер настройки - шаг 4

Отобразится следующее:

```
Finally, setup the default gateway.
Please enter the IP address of the gateway from which this network is reachable (e.g. 192.168.1.1).Default gateway (A.B.C.D):[0.0.0.0]
```

Введите шлюз по умолчанию.

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

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

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

SNMP Interface = Dell_Network_Manager@0.0.0.0
User Account setup = admin
```

```
Password = *
Management IP address = 1.1.1.1 255.255.255.0
Default Gateway = 1.1.1.2

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

Мастер настройки - шаг 5

Отобразится следующее:

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

Введите [N], чтобы не перезагружать **Мастер настройки**.

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

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

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

Мастер настройки - шаг 6

Отобразится приглашение команд консоли.

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 учетные записи) и включает в себя следующие темы.

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

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. При сбросе устройства в файле настройки сохраняется DHCP-команда, а IP-адрес не сохраняется. Чтобы получить IP-адрес от сервера DHCP, необходимо выполнить следующие действия:

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

- Назначение динамического IP-адреса:

```
console# configure

console(config)# interface ethernet g1

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

console(config-if)# exit

console(config)#
```

- Назначение динамического IP-адреса (на VLAN):

```
console# configure

console(config)# interface ethernet vlan 1

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

console(config-if)# exit
```

```
console(config)#
```

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

Console# **show ip interface**		
Gateway IP Address	Activity status	
----------	----------	
10.7.1.1	Active	
IP Address	Interface	Type
----------	----------	----------
10.7.1.192/24	VLAN 1	Static
10.7.2.192/24	VLAN 2	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 устройство получает новый файл настройки и выполняет загрузку на основе данных из этого файла. Затем коммутатор включает протокол DHCP в соответствии с инструкциями в новом файле настройки, а затем DHCP выдает указание на повторную загрузку того же файла.

Получение IP-адреса от сервера BOOTP

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

Чтобы получить IP-адрес от сервера BOOTP:

1. Выберите и подсоедините любой порт к серверу BOOTP или к подсети, в которой имеется такой сервер, чтобы получить IP-адрес.
2. В командной строке системы введите команду **delete startup configuration**, чтобы удалить запускаемую настройку из флэш-памяти.

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

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

Этот процесс показан в следующем примере:

```
console> консоль включить

console# delete startup-config

Startup file was deleted

console# reload

Изменения не были сохранены. Вы уверены, что хотите продолжить (да/нет) [нет]?

Эта команда приведет к полной перезагрузке системы и к завершению текущего сеанса. Хотите продолжить (да/нет) [нет]?

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

/* the switch 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.

- Терминал.
- Telnet.
- SSH.
- HTTP.
- HTTPS.

ПРИМЕЧАНИЕ. Пароли определяются пользователем.

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

Настройка первоначального пароля терминала

Для настройки первоначального пароля терминала введите следующие команды:

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

console(config)# aaa authentication enable default line

console(config)# line console

console(config-line)# login authentication default

console(config-line)# enable authentication default

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

- Во время первоначальной регистрации в устройстве через сеанс консоли в ответ на приглашение ввести пароль введите **george**.
- 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
```

- При первоначальной регистрации в устройстве через сеанс Telnet введите пароль **bob**.
- При установке режима устройства «включено» введите **bob**.

Настройка первоначального пароля SSH

Для настройки начального пароля SSH введите следующие команды:

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

console(config)# aaa authentication enable default line

console(config)# line ssh

console(config-line)# login authentication default

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

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

- При первоначальной регистрации в устройстве через сеанс SSH введите пароль jones.
- При установке режима устройства «включено» введите jones.

Настройка первоначального пароля HTTP

Для настройки первоначального пароля HTTP введите следующие команды:

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

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

Настройка первоначального пароля HTTPS

Для настройки первоначального пароля HTTPS введите следующие команды:

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

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

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

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

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

console(config)# ip https server
```

При 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.

Конфигурация баннеров входа в систему

Вы можете определить 3 типа баннеров входа в систему:

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

Для просмотра и настройки баннеров входа в систему:

```
console# banner motd Welcome

console# show banner motd

console# banner login Please log in

console# show banner login

console# banner exec Successfully logged in

console# show banner exec
```

Процедуры запуска

Процедуры меню Startup (Запуск)

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

Вход в меню Startup (Запуск) может быть осуществлен при загрузке устройства - необходимо войти в область ввода для пользователя сразу же после выполнения процедуры POST.

Для входа в меню Startup (Запуск):

1. Включите питание и дождитесь появления сообщения автозагрузки.

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

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

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

------ Performing the Power-On Self Test (POST) ------

UART Channel Loopback Test.....................PASS

Testing the System SDRAM.......................PASS

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

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

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

BOOT Software Version 1.0.0.20 Built 22-Jan-xxxx 15:09:28

Processor: FireFox 88E6218 ARM946E-S, 64 MByte SDRAM.

I-Cache 8 KB. D-Cache 8 KB. Cache Enabled.

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

Preparing to decompress...
```

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

```
[1] Download Software

[2] Erase Flash File

[3] Password Recovery Procedure

[4] Enter Diagnostic Mode

[5] Set Terminal Baud-Rate

[6] Back

Enter your choice or press 'ESC' to exit
```

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

ПРИМЕЧАНИЕ. При выборе параметра меню Startup (Запуск) необходимо принимать во внимание время ожидания: Если в течение 35 секунд (по умолчанию) не будет выбран ни один из пунктов меню, истечет время ожидания команды. Значение времени ожидания по умолчанию можно изменить с помощью команд консоли.

Загрузка программного обеспечения

Процедура загрузки программного обеспечения используется, 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 клавишу [1]. Появится следующее сообщение:

```
Downloading code using XMODEM
```

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

ПРИМЕЧАНИЕ. После загрузки программного обеспечения устройство перезагружается автоматически.

ПРИМЕЧАНИЕ. Количество времени, необходимое для загрузки, зависит от используемого инструмента.

Удаление файла флэш-памяти

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

Удаление настройки 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**. 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. Повторите начальную настойку устройства.

Восстановление пароля

Если определенный пользователем пароль утрачен, то можно вызвать процедуру восстановления пароля из меню Startup (Запуск). Эта процедура допускает однократный доступ к устройству без ввода пароля.

Восстановление пароля возможно только с локального терминала:

1. В меню Startup (Запуск) выберите **3** и нажмите клавишу <Enter>.

   Пароль будет удален.

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

Загрузка программного обеспечения через сервер TFTP

В этом разделе содержатся инструкции для загрузки программного обеспечения (системного и загрузочного образа) через сервер TFTP. Сервер TFTP должен быть настроен перед началом загрузки программного обеспечения.

Загрузка системного образа

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

При следующей загрузке устройство распаковывает и запускает текущий активный образ системы, если не указано иначе.

Для загрузки системного образа через сервер TFTP:

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

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

3. Чтобы проверить номер версии программного обеспечения, запущенного на устройстве, введите команду show version. Ниже приводится пример отображаемой информации:

   ```
   console# show version

   SW version 1.0.0.42 (date 22-Jul-xxxx time 13:42:41)

   Boot version 1.0.0.18 (date 01-Jun-xxxx time 15:12:20)

   HW version
   ```

4. Чтобы узнать, какой образ системы активен, введите команду show bootvar. Далее приведен пример отображаемой на экране информации:

```
console# sh bootvar

Images currently available on the Flash

Image-1 active (selected for next boot)

Image-2 not active

console#
```

5. Чтобы скопировать новый образ системы на устройство, введите команду 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.ros image

Accessing file `file1' on 176.215.31.3Ц

Loading file1 from 176.215.31.3:

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

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

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

6. Выберите образ для следующей загрузки, введя системную команду boot. После этой команды введите команду show bootvar, чтобы проверить, что копия, указанная в качестве параметра в команде boot system, выбрана для следующей загрузки.

Далее приведен пример отображаемой на экране информации:

```
console# boot system image-2

console# sh boot

Images currently available on the Flash

Image-1 active

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

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

7. Введите команду reload. Появится следующее сообщение:

```
console# reload

This command will reset the whole system and disconnect your current

session. Do you want to continue (y/n) [n]?
```

8. Введите Y. Устройство будет перезагружено.

Загрузка загрузочного образа

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

1. Убедитесь, что IP-адрес настроен для одного из портов устройства, и проверьте соединение с сервером TFTP.

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

3. Чтобы проверить номер версии программного обеспечения, запущенного на устройстве, введите команду show version. Ниже приводится пример отображаемой информации:

```
console# sh ver

SW version 1.0.0.42 (date 22-Jul-xxxx time 13:42:41)

Boot version 1.0.0.18 (date 01-Jun-xxxx time 15:12:20)

HW version 00.00.01 (date 01-May-xxxx time 12:12:20)
```

4. Чтобы скопировать загрузочный образ на устройство, введите команду copy tftp://{tftp address}/{file name} boot. Далее приведен пример отображаемой на экране информации:

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

   Erasing file..done.

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

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

5. Введите команду reload. Появится следующее сообщение:

   ```
   console# reload

   This command will reset the whole system and disconnect your current

   session. Do you want to continue (y/n) [n]?
   ```

6. Введите Y.

   Устройство будет перезагружено.

Назад на страницу Содержание

Назад на страницу Содержание

Глоссарий

Руководство пользователя систем Dell™ PowerConnect™ 54xx

Этот глоссарий содержит основные технические термины, представляющие интерес.

А Б В Г Д Е Ё Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я A B C D E F G H I J K L M N O P Q R

A

Автоматическое согласование

Допускает использование портов 10/100 Мбит/с или 10/100/1000 Мбит/с Ethernet для установки следующих функций:

- Дуплексный и полудуплексный режим
- Управление потоком
- Скорость

ACL

Access Control List - список управления доступом. Позволяет сетевым администраторам определять классификационные действия и правила для определенных входных портов.

ARP

Address Resolution Protocol - протокол разрешения адресов. Это протокол TCP/IP для преобразования IP-адресов в физические адреса.

ASIC

Application Specific Integrated Circuit - специализированная интегральная схема. Заказная микросхема, разработанная для определенного приложения.

Б

Бод

Число сигнальных элементов, передаваемых за одну секунду.

Большие кадры

Позволяют передавать данные меньшим числом пакетов. Большие кадры уменьшают размеры заголовков, снижают время обработки и вероятность разрывов.

B

BootP

Bootstrap Protocol - протокол загрузки. Позволяет рабочей станции обнаружить свой IP-адрес, IP-адрес сервера BootP в сети или файл конфигурации, загруженный в систему загрузки устройства.

BPDU

Bridge Protocol Data Unit - модуль данных мостового протокола. Предоставляет информацию о преобразовании данных в формате сообщения. BPDU передаются вместе с информацией устройства в составе конфигурации протокола Spanning Tree. Пакеты BPDU содержат информацию о портах, адресах, приоритетах и стоимости пересылки.

Входной порт

Порт, используемый для приема сетевого трафика.

Выравнивание нагрузки

Обеспечивает равномерное распределение данных и/или пакетов для обработки между доступными ресурсами сети. Например, в результате выравнивания нагрузки входящие пакеты равномерно распределяются между всеми серверами или направляются на следующий доступный сервер.

Выходные порты

Порт, используемый для передачи сетевого трафика.

Д

Дескриптор ресурса

Определяет ссылку на устройство, задаваемую пользователем.

Динамический режим распределения VLAN (DVA)

Обеспечивает автоматическое распределение пользователей по сетям VLANs при авторизации сервера RADIUS. После авторизации пользователя сервером RADIUS, пользователь автоматически подключается к сети VLAN, конфигурация которой произведена серверомRADIUS.

Домен

Совокупность компьютеров, программ и устройств в сети объединенная общими правилами и процедурами.

Дуплексный режим

Позволяет одновременно передавать и принимать данные. Существует два типа дуплексного режима:

- **Полный дуплексный режим**. обеспечивает бисинхронную передачу, например по телефону. Две стороны могут одновременно передавать информацию.
- **Полудуплексный режим**. обеспечивает асинхронную передачу, например по портативной радиостанции. Передачу информации может одновременно осуществлять только одна сторона.

E

Ethernet

Ethernet стандартизирован по IEEE 802.3. Ethernet – это наиболее распространенный стандарт, используемый для локальной сети. Поддерживает следующие скорости передачи данных: 10, 100 или 1000 Мбит/с.

EWS

Embedded Web Server - встроенный веб-сервер. Используется для управления устройством с помощью стандартного обозревателя. Встроенные веб-серверы используются в дополнение либо вместо CLI или NMS.

З

Запрос

Извлекает информацию из базы данных и предоставляет информацию для использования.

Зеркалирование портов

Контролирует и дублирует сетевой трафик путем пересылки копий входящих и исходящих пакетов с одного порта на другой (контролирующий).

И

ИС

Интегральная схема. Интегральные схемы – это небольшие электронные устройства, состоящие из полупроводникового материала.

К

Кадр

Пакеты, содержащие информацию заголовка и заключительной части, необходимую для физической среды.

Класс обслуживания

Класс обслуживания (CoS). Класс обслуживания является схемой приоритетов стандарта 802.1p. CoS обеспечивает способ маркировки пакетов, содержащих приоритетную информацию. Значение CoS от 0 до 7 добавляется к заголовку Layer II пакетов, где ноль означает самый низкий приоритет, а семь – самый высокий.

Перекрывающаяся передача двух или нескольких конфликтующих пакетов. Переданные данные использовать невозможно, и сеанс начинается заново.

Клиент DHCP

Интернет-узел, использующий протокол DHCP для получения параметров конфигурации, например сетевого адреса.

Комбинированные порты

Один логический порт, имеющий два физических подключения - подключение RJ-45 и подключение SFP.

Коммутатор

Фильтрует и пересылает пакеты из одного сегмента локальной сети в другой. Маршрутизаторы поддерживают любые типы пакетных протоколов.

Л

«Лавина» широковещательной передачи

Результат чрезмерного количества широковещательных сообщений, одновременно переданных по сети через один порт. Ответы на пересылаемые сообщения являются причиной чрезмерной нагрузки на сеть, перегружая ее ресурсы или вызывая задержки в сети.

Для получения более подробной информации по «лавинам» широковещательной передачи, см. в разделе Настройка выравнивания нагрузки.

ЛВС

Local Area Network - локальная (вычислительная) сеть. Сеть, развернутая в одном помещении, здании, на одной территории или в пределах другой географически ограниченной области.

М

Максимально возможная скорость доставки

Трафик выделен для очереди с самым низким приоритетом, доставка пакета не гарантируется.

Маршрутизатор

Устройство, устанавливающее соединение с отдельной сетью. Маршрутизаторы пересылают пакеты между двумя или несколькими сетями. Маршрутизаторы работают на уровне Layer 3.

MAC-адрес

Адрес Media Access Control. MAC-адрес – это аппаратный адрес, определяющий каждый узел в сети.

Маска

Фильтр, включающий или исключающий определенные значения, например части IP-адреса.

Например, если Блок 2 вставляется на первой минуте десятиминутного цикла, а Блок 1 вставляется на пятой минуте этого же цикла, они будут рассматриваться как блоки одного периода.

Маска ввода

Указывает, какие биты IP-адреса используются, а какие игнорируются. Маска ввода 255.255.255.255 указывает, что никакие биты не важны. Маска ввода 0.0.0.0 указывает, что все биты важны.

Маска подсети

Используется для замены всего IP-адреса или его части, которые используются в адресе подсети.

Многоадресная передача

Передает копии одного и того же пакета на несколько портов.

Мост

Устройство, соединяющее две сети. Мосты могут быть оснащены разным аппаратным обеспечением, но при этом не зависят от протоколов. Мосты функционируют на уровнях Layer 1 и Layer 2.

MD5

Message Digest 5 - профиль сообщения 5. Алгоритм, создающий 128-разрядную хеш-строку. MD5 является разновидностью алгоритма MD4, который обеспечивает большую безопасность по сравнению с MD4. MD5 проверяет целостность передаваемых данных, а также определяет источник передаваемых данных.

MDI

Media Dependent Interface - интерфейс, зависящий от среды. Кабель, используемый для оконечных станций.

MDIX

Media Dependent Interface with Crossover - интерфейс, зависящий от среды, с перекрещиванием. Кабель, используемый для концентраторов и коммутаторов.

MIB

Management Information Base - база управляющей информации. В базах MIB содержится информация, описывающая определенные аспекты сетевых компонентов.

Н

Назначение полосы пропускания

Часть полосы пропускания, назначенная для определенного приложения, пользователя и/или интерфейса.

Настройка для запуска

Сохраняет полную настройку устройства при отключении или перезагрузке устройства.

HOL

Head of Line - защита от блокировки очереди. Для пакетов устанавливается очередь. Пакеты, стоящие в начале очереди, пересылаются до пакетов, находящихся в конце очереди.

HTTP

Протокол HTTP (HyperText Transport Protocol). Используется для обмена документами формата HTML через Интернет между серверами и клиентами.

О

Обратное давление

Этот механизм используется в полудуплексном режиме и позволяет отключить получение сообщений на порты.

Объединительная платаp>

Основная шина, которая используется для передачи информации в устройстве.

Объединенные VLAN

Группа нескольких сетей VLAN, объединенных в одну сеть VLAN. Объединение VLAN позволяет маршрутизаторам отвечать на запросы ARP для узлов, расположенных в разных подсетях VLAN, принадлежащих одной общей сети VLAN. Маршрутизаторы отвечают, используя собственные MAC-адреса.

Одноадресная передача

Форма пересылки, при которой один пакет передается одному пользователю.

Оконечная система

Устройство конечного пользователя в сети.

OID

Object Identifier - идентификатор объекта. Используется в SNMP для идентификации управляемых объектов. В схеме сетевого управления «управляющее устройство/агент SNMP» каждый управляемый объект должен иметь идентифицирующий его OID.

П

Пакеты

Блоки информации, предназначенные для передачи в системах коммутирования пакетов.

Переключение

Переключение происходит, когда состояние интерфейсов постоянно меняется. Например, состояние порта STP постоянно изменяется с прослушивания на распознавание, а затем на пересылку. Это может привести к потере трафика.

Подсеть

Подсеть. Подсети – это части сети, использующие общий компонент адреса. В сетях TCP/IP устройства, использующие одинаковый префикс, являются частями одной и той же сети. Например, все устройства с префиксом 157.100.100.100 являются частями одной и той же сети.

Полоса пропускания

Полоса пропускания указывает объем данных, которые могут быть переданы за определенный период времени. Для цифровых устройств полоса пропускания указывается в битах в секунду (бит/с) или байтах в секунду.

Порт

Физические порты обеспечивает связь между компонентами, что позволяет микропроцессорам устанавливать связь с периферийным оборудованием.

Прерывание

Сообщение, отправленное по протоколу SNMP, означающее, что произошло системное событие.

Протокол

Набор правил, управляющий тем, как устройства обмениваются информацией по сети.

Протокол туннелирования ISATAP

см. *ISATAP.*

Протокол STP (Spanning Tree Protocol)

Исключает образование циклов сетевого трафика. Протокол STP (Spanning Tree Protocol) предоставляет древовидную топологию для любого расположения мостов. STP обеспечивает единственный путь между конечными станциями сети и исключает циклы.

Профили доступа

Позволяют сетевым администраторам определять профили и правила для доступа к устройству. Можно ограничить доступ к функциям управления группам пользователей, которые определены следующими критериями:

- входящими интерфейсами;
- исходными IP-адресами и/или маской исходной подсети.

Профили проверки подлинности

Набор правил, с помощью которых осуществляется вход и проверка подлинности пользователей и приложений.

P

Распознавание MAC-адреса

Распознавание MAC-адреса характеризует мост распознавания, в котором записывается MAC-адрес источника пакета. Пакеты, направляемые на этот адрес, пересылаются только на интерфейс моста, на котором находится этот адрес. Пакеты, направляемые на неизвестные адреса, пересылаются на интерфейсы всех мостов. Распознавание MAC-адреса минимизирует трафик в локальной сети, к которой выполнено подключение.

Режим доступа

Определяет метод, с помощью которого пользователь получает доступ к системе.

PDU

Protocol Data Unit - модуль данных протокола. Модуль данных, указанный в протоколе уровня и состоящий из управляющей информации протокола и пользовательских данных уровня.

PING

Packet Internet Groper - отправитель Интернет-пакетов. Проверяет доступность конкретного IP-адреса. Пакет отправляется на другой IP-адрес и ожидает ответа.

C

Сегментация

Делит локальную сеть на отдельные сегменты локальной сети для установки связи и маршрутизации. Сегментация позволяет преодолеть ограничения полосы пропускания в локальной сети.

Сервер

Центральный компьютер, предоставляющий службы другим компьютерам в сети. Службы могут включать хранение файлов и доступ к приложениям.

Скорость порта

Означает скорость порта. Существуют следующие скорости портов:

- Ethernet 10 Мбит/с
- Fast Ethernet 100 Мбит/с
- Gigabit Ethernet 1000 Мбит/с

Создание транков

Объединение каналов. Оптимизирует использование портов, связывая между собой группу портов и формируя один транк (объединенные группы).

Сообщества

Указывает группу пользователей, для которой сохраняются одинаковые права для доступа к системе.

CDB

Configuration Data Base - база данных конфигурации. Файл, содержащий информацию о конфигурации устройства.

CLI

Command Line Interface - интерфейс командной строки. Набор команд, указываемых в строке, которые используются для настройки системы. Дополнительную информацию по использованию консоли CLI см. в разделе **Использование режима командной строки**.

T

Telnet

Протокол Telnet (Terminal Emulation Protocol). Обеспечивает пользователям системы возможность входа в удаленные сети и использования имеющихся в них ресурсов.

TCP/IP

Протокол TCP (Transmission Control Protocol). Обеспечивает двум хостам возможность установки связи и обмена потоками данных. TCP гарантирует доставку пакета, а также передачу и прием пакетов в порядке их отправки.

TFTP

Протокол TFTP (Trivial File Transfer Protocol). Использует протокол UDP (User Data Protocol) без функций защиты для передачи файлов.

У

Узел

Конечная точка сетевого соединения или обычная точка пересечения нескольких сетевых линий. К узлам относятся:

- процессоры;
- контроллеры;
- рабочие станции.

Управление потоком

Позволяет низкоскоростным устройствам осуществлять связь с высокоскоростными устройствами. При этом высокоскоростные устройства делают паузы между отправкой пакетов.

Уровень 4

Устанавливает соединение и обеспечивает доставку всех данных в место их назначения. Пакеты, проверяемые на уровне Layer 4, анализируются, и решения о пересылке принимаются на основе того, как они используются.

Уровень MAC

Подуровень уровня *DTL (Data Link Control)*.

Ф

Файл образа

Системные образы сохраняются в двух секторах Flash, называемых образами (Image 1 и Image 2). Активный образ хранит активную копию, другой образ - вторую копию.

Файл рабочей настройки

Содержит все команды файла для запуска, а также все команды, введенные во время последнего сеанса. После отключения или перезагрузки устройства все команды, сохраненные в файле рабочей настройки, теряются.

Файл резервной настройки

Содержит резервную копию настройки устройства. Резервный файл настройки изменяется, когда в него копируется файл рабочей настройки или файл для запуска.

Фрагмент

Пакеты Ethernet размером менее 576 бит.

Х

Хост

Компьютер, являющийся источником информации или служб для других компьютеров.

Ц

ЦП

Центральный процессор. Часть компьютера, в которой обрабатывается информация. ЦП состоят из управляющего устройства и арифметико-логического устройства.

Ш

Широковещательный домен

Группы устройств, получающие широковещательные кадры, которые передаются любым устройством, входящим в назначенную группу. Маршрутизаторы связывают широковещательные домены, так как маршрутизаторы не пересылают широковещательных кадров.

Широковещательная передача

Метод передачи пакетов на все порты в сети.

D

DSCP

DiffServe Code Point - точка кодов DiffServe. DSCP обеспечивает способ маркировки IP-пакетов с помощью информации о приоритетах QoS.

F

FFT

Fast Forward Table - таблица быстрой пересылки. Предоставляет информацию о маршрутах пересылки. Если на устройство поступает пакет с известным маршрутом, то он пересылается по маршруту, указанному в FFT. Если маршрут неизвестен, ЦП пересылает пакет и обновляет FFT.

FIFO

First In First Out - метод «первым пришел - первым обслужен». Процедура установки очередности, когда первым пакетом в очереди является первый из поступивших пакетов.

G

GARP

Протокол GARP (General Attributes Registration Protocol). Регистрирует клиентские компьютеры в многоадресном домене.

Gigabit Ethernet

Gigabit Ethernet позволяет передавать данные со скоростью 1000 Мбит/с и совместим со стандартами Ethernet 10/100 Мбит/с.

GVRP

Протокол регистрации GARP VLAN (GVRP). Регистрирует клиентские компьютеры в группах VLAN.

I

IEEE

Institute of Electrical and Electronics Engineers - Институт инженеров по электротехнике и электронике. Ассоциация инженеров, занимающаяся разработкой сетей связи и стандартов информационных сетей.

IEEE 802.1p

Устанавливает приоритет для сетевого трафика на уровне канала передачи данных или подуровне MAC.

IEEE 802.1d

Мост стандарта IEEE 802.1d, используемый в протоколе STP, поддерживает MAC-преобразование, позволяющее исключить образование сетевых контуров.

IEEE 802.1Q

Определяет работу мостов VLAN, при которой возможно определение, работа и администрирование групп VLAN внутри инфраструктур локальных сетей с мостами.

IP

Internet Protocol - протокол Интернета. Определяет формат пакетов и способ назначения адресов для них. IP назначает пакетам адреса и пересылает пакеты на нужный порт.

IP, версия 6 (IPv6)

Версия систем обработки IP-адресов, позволяющая работать с более длинными адресами, чем традиционная IPv4. Адреса системы IPv6 имеют длину 128 бит, в то время как в версии IPv4 адреса имеют длину 32 бита; предоставляя больше свободного пространства для адресов.

IP-адрес

Адрес по протоколу Интернета. Уникальный адрес, назначаемый сетевому устройству, подключенному к двум или нескольким локальным или глобальным сетям.

IPX

Internetwork Packet Exchange - межсетевой пакетный обмен. Осуществляет передачу несвязанных данных.

ICMP

Протокол ICMP (Internet Control Message Protocol). Позволяет шлюзу или хосту назначения устанавливать связь с хостом, являющимся источником данных, например для передачи отчета об ошибке обработки.

ISATAP

Протокол автоматической туннельной внутриобъектной адресации .
ISATAP представляет собой автоматический механизм туннелирования, который использует сеть IPv4 в качестве слоя звена циркулярного доступа для IPv6. Протокол ISATAP предназначен дляпередачи пакетов IPv6 в пределах объекта в случаях, когда его собственная инфраструктура IPv6 еще не организована.

iSCSI

iSCSI - протокол связи, используемый для обмена данными между файловыми серверами и носителями. Файловые серверы называются *инициаторами*, а диски - *конечными устройствами*.

L

LAG

Link Aggregated Group - объединенная группа каналов. Объединяет порты или группы VLAN в единый виртуальный порт или единую группу VLAN.

Дополнительную информацию о группах LAG см. в разделе **Определение членства в группе LAG**.

Layer 2

Уровень канала передачи данных или уровень MAC. Содержит физический адрес клиентского компьютера или сервера. Обработка на уровне Layer 2 выполняется быстрее обработки на уровне Layer 3 из-за меньшего объема обрабатываемой информации.

LLDP-MED

Link Layer Discovery Protocol - Media Endpoint Discovery (Выявление конечной медиа-точки по протоколу обнаружения каналов передачи данных). Протокол LLDP позволяет сетевым администраторам выполнять поиск и устранение неисправностей и совершенствовать управление сетью путем выявления и сохранения топологии сети в средах, включающих оборудование самых разных поставщиков. Расширение протокола MED повышает гибкость сети, давая возможность различным системам IP использовать один сетевой протокол LLDP.

N

NA

Neighbor Advertisement - сообщение «соседнего» узла.

NMS

Network Management System - система сетевого управления. Интерфейс, обеспечивающий управление системой.

ND - Neighbor Discovery - обнаружение «соседнего» узла

Протокол обнаружения соседнего узла.

NS

Neighbor Solicitation - запрос обнаружения «соседнего» узла.

Q

QoS

Quality of Service - качество обслуживания. QoS позволяет сетевым администраторам решить, каким образом и какая часть сетевого трафика пересылается в зависимости от приоритетов, типов приложений, а также адресов источников и мест назначения.

R

RA

Сообщение сервера RADIUS.

RADIUS

Служба Remote Authentication Dial-In User Service. Способ проверки пользователей системы и отслеживания времени соединения.

RMON

Remote Monitoring - удаленный мониторинг. Предоставляет возможность сбора сетевой информации с одной рабочей станции.

RD

RADIUS Discovery - обнаружение сервера RADIUS.

RS

Router Solicitation - запрос маршрутизатора.

RSTP

Протокол RSTP (Rapid Spanning Tree Protocol). Выявляет и использует топологию сети, обеспечивая лучшую сходимость для протокола STP без образования циклов пересылки.

S

SoC

System on a Chip - система в микросхеме. Специализированная интегральная схема (ASIC), в которой содержится вся система. Например, телекоммуникационная SoC может содержать микропроцессор, процессор цифровых сигналов, оперативную (RAM) и постоянную (ROM) память.

SNMP

Протокол SNMP (Simple Network Management Protocol). Управляет локальными сетями. Программное обеспечение, использующее SNMP, осуществляет связь с сетевыми устройствами со встроенными агентами SNMP. Агенты SNMP собирают информацию о работе в сети и состоянии устройства и отправляют эту информацию назад на рабочую станцию.

SNTP

Протокол SNTP (Simple Network Time Protocol). Протокол SNTP гарантирует точность синхронизации времени такта сетевого коммутатора до миллисекунды.

SSH

Протокол SSH (Secure Shell). Обеспечивает вход в систему удаленного компьютера по сети, выполнение команд и передачу файлов с одного компьютера на другой.

U

UDP

Протокол UDP (User Data Protocol). Передает пакеты, но не гарантирует их доставку.

V

VLAN

Virtual Local Area Network - виртуальная локальная (вычислительная) сеть. Логические подгруппы локальной сети (ЛВС), созданные программным, а не аппаратным путем.

W

WAN

Wide Area Network - глобальная (вычислительная) сеть. Сеть, действующая в пределах большой географической зоны.

Назад на страницу Содержание

Назад на страницу Содержание

Описание аппаратного обеспечения

Руководство пользователя систем Dell™ PowerConnect™ 54xx

Конфигурации портов устройства

Описание портов передней панели систем серии PowerConnect 54xx

Системы серии PowerConnect 54xx оборудованы следующими портами.

- **24/48 портов для медного кабеля** - порты RJ-45, назначенные как порты 10/100/1000 BaseT Gigabit Ethernet
- **4 порта для оптоволоконного кабеля** - назначены как порты Gigabit
- **Порт терминала** - порт консоли RS-232

На следующем рисунке изображена передняя панель систем серии PowerConnect 54xx.

Рис 2-1. Передняя панель устройства PowerConnect 5424

На передней панели располагаются порты с 1 по 24/48. Это порты RJ-45 для медного кабеля, назначенные как 10/100/1000 Мбит/с и поддерживающие дуплексный и полудуплексный режимы. Также имеется четыре порта SFP для оптоволоконных кабелей, назначенные как комбинированные порты 21-24/45-48. Комбинированный порт представляет собой один логический порт, имеющий два физических подключения. Одновременно только одно физическое соединение может быть активно, поэтому активными могут быть медные порты или эквивалентные порты для оптоволоконных кабелей, но не оба вида портов одновременно. Порты верхнего ряда обозначены нечетными числами, а порты нижнего ряда четными числами.

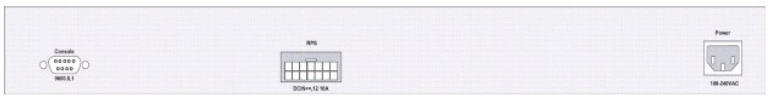
На передней панели установлены светодиодные индикаторы устройства и кнопка перезагрузки, которая используется для перезагрузки устройства в ручном режиме.

Устройство автоматически определяет, является ли подключенный к порту RJ-45 кабель кроссоверным или кабелем прямого подключения, и работает в обоих случаях.

Описание портов задней панели системы PowerConnect

На задней панели находятся разъемы питания, показанные на рис. 2-2.

Рис. 2-2. Задняя панель устройства



На задней панели устройства находятся два разъема питания и порт консоли RS-232. Для общего использования имеется разъем источника питания переменного тока, который можно подключить к источникам 110 В или 220 В.

Разъем источника питания постоянного тока используется для подключения резервного источника питания в случае сбоя в работе источника переменного тока.

Порты устройства

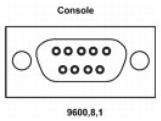
Порты SFP

Порт SFP - это компактный оптический модульный трансивер, поддерживающий горячую замену и обеспечивающий высокую скорость передачи данных. Он назначен как 1000Base-SX или LX.

Порт консоли RS-232

Один разъем DB-9 для последовательного соединения терминала, использующийся для отладки программ, загрузки программного обеспечения и т.д. Скорость передачи данных по умолчанию 9600 бод. Скорость передачи данных можно настроить в диапазоне от 2400 до 38400 бод.

Рис. 2-3. Порт консоли



Комбинированные порты

Комбинированный порт представляет собой один логический порт, имеющий два физических подключения.

- Разъем RJ-45 для подключения кабеля медной витой пары
- Разъем SFP для подключения различных оптоволоконных модулей

В комбинированном порту одновременно можно использовать только одно из двух физических соединений. Функции порта и доступные элементы управления портом определяются используемым физическим соединением.

Система автоматически определяет устройство, подключенное к комбинированному порту, и использует эту информацию для всех операций и интерфейсов управления.

Если имеются порты RJ-45 и SFP и разъем подключен к порту SFP, порт SFP активен, если только медный разъем порта Base-T с таким же номером не подключен и не установлено соединение.

Переключение с разъема RJ-45 на SFP (или наоборот) возможно без перезагрузки системы или сброса.

Фактические размеры

Устройство имеет следующие физические размеры.

- Высота - 44 мм (1,73 дюйма)
- Ширина - 440 мм (17,32 дюйма)
- Длина - 255 мм (10,03 дюйма)

Описания индикаторов

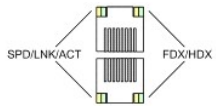
На передней панели находятся светодиоды (индикаторы), которые показывают состояние связи, питания, вентиляторов и системы диагностики.

Индикаторы портов

Индикаторы порта 10/100/1000 Base-T

У каждого порта 10/100/1000 Base-T имеется два индикатора. Параметры скорости/соединения/активности указываются на левом индикаторе, а дуплексный режим - на правом индикаторе.

Рис. 2-4. Индикаторы порта RJ-45 10/100/1000 BaseT



Описание показаний индикаторов порта RJ-45 приведено в следующей таблице.

Табл. 2-1. Показания индикатора порта 10/100/1000 Base-T с разъемом RJ-45 (с медными проводниками)

Индикатор	Цвет	Описание
Левый индикатор	Горит зеленым	Установлена связь с портом на скорости 1000 Мбит/с.
	Мигает зеленым	Через порт осуществляется прием или передача данных на скорости 1000 Мбит/с.
	Горит оранжевым	Установлена связь с портом на скорости 10 или 100 Мбит/с.
	Мигает оранжевым	Через порт осуществляется прием или передача данных на скорости 10 или 100 Мбит/с.
Правый светодиондый индикатор	Зеленый	Порт осуществляет передачу в полном дуплексном режиме.
	Не горит	Порт работает в полудуплексном режиме.

Индикаторы SFP

У каждого порта SFP имеется один индикатор, помеченный как LNK.

Рис. 2-5. Индикатор порта SFP

Описание показаний индикаторов порта SFP приведено в следующей таблице.

Табл. 2-2. Показания индикаторов порта SFP

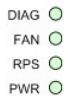
Индикатор	Цвет	Описание
SFP	Горит зеленым	Порт работает.
	Мигает зеленым	Через порт осуществляется прием или передача данных.
	Не горит	Порт не работает.

Когда порт SFP подключен, индикатор дуплексного режима соответствующего комбинированного порта для медного провода горит зеленым.

Системные индикаторы

Системные индикаторы, расположенные с левой стороны передней панели, предоставляют информацию об источниках питания, вентиляторах, температурных условиях и диагностическую информацию. На рис. 2-6 изображены системные индикаторы.

Рис. 2-6. Системные индикаторы



Описание показаний индикаторов приведено в следующей таблице.

Табл. 2-3. Показания системных индикаторов

Индикатор	Цвет	Описание
Диагностика (DIAG)	Мигает зеленым	В системе запущен диагностический тест.
	Горит зеленым	Система прошла диагностический тест.
	Горит красным	Система не прошла диагностический тест

Вентилятор (FAN)	Горит зеленым	Вентиляторы устройства работают нормально.
	Горит красным	Один или несколько вентиляторов не работают.
Резервный источник питания (RPS)	Горит зеленым	Резервный источник питания работает.
	Горит красным	Резервный источник питания не работает.
	Не горит	Резервный источник питания выключен.
Основной источник питания (PWR)	Горит зеленым	Источник питания работает нормально.
	Не горит	Источник питания выключен.
	Красный	Произошел сбой источника питания.
Температура (TEMP)	Не горит	Температура системы в норме.
	Горит красным	Температура системы слишком высока.

Компоненты оборудования

Источники питания

В устройстве имеется внутренний источник питания (источник переменного тока) и разъем для подсоединения устройства к внешнему источнику питания (источнику постоянного тока). Внешний источник питания обеспечивает резервное питание и называется резервным источником питания (RPS). Для включения устройства необходим только один источник питания. Работа с двумя источниками питания регулируется с помощью распределения нагрузки.

Распределение нагрузки - это разделение питания между двумя источниками. При выходе одного источника питания из строя второй источник автоматически продолжает снабжать устройство электроэнергией.

Индикатор источника питания отображает состояние источника питания. Более подробную информацию об индикаторах см. в разделе Описание индикаторов.

Источник питания переменного тока

Источник питания переменного тока преобразует стандартные 220/110 В переменного тока 50/60 Гц в 5 В постоянного тока при силе тока 5 А и в 12 В постоянного тока при силе тока 3 А. Источник питания автоматически определяет значение напряжения (110 или 220 В), поэтому производить настройку не требуется.

В источнике питания переменного тока используется стандартный разъем для 220/110 В переменного тока. Индикатор находится на передней панели и показывает, подсоединен ли источник питания переменного тока к устройству.

Источник питания постоянного тока

Внешний источник питания постоянного тока используется в качестве резервного. Питание на устройство может подаваться только с этого источника. В резервном источнике питания используется разъем типа RPS600. Производить настройку не требуется. Индикатор находится на передней панели и показывает, подсоединен ли источник питания постоянного тока к устройству.

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

Кнопка Reset (Сброс)

С помощью кнопки сброса, расположенной на передней панели, можно произвести сброс устройства вручную.

Система вентиляции

Для охлаждения устройства используется система вентиляторов. При возможном сбое в работе вентилятора его состояние можно проверить с помощью индикатора. Более подробную информацию об индикаторах см. в разделе Описание индикаторов.

Назад на страницу Содержание

Назад на страницу Содержание

Установка устройства PowerConnect

Руководство пользователя систем Dell™ PowerConnect™ 54xx

В этом разделе содержится информация о распаковке устройства, его размещении, установке и подключению кабелей.

Меры предосторожности при монтаже

ОСТОРОЖНЫ. Перед выполнением любой из следующих процедур прочтите и выполните инструкции по технике безопасности, указанные в System Information Guide (Информационном руководстве по системе), которое входит в комплект документации компании Dell.

ОСТОРОЖНЫ. Обратите внимание на следующие пункты до выполнения процедур, описанных в этом разделе.

- Убедись, что стойка или шкаф, в котором размещается устройство, надежно закреплены, чтобы предотвратить их шатание или опрокидывание.
- Убедитесь, что цепи источника питания надлежащим образом заземлены.
- Обращайте внимание на сервисную маркировку и соблюдайте содержащиеся в ней указания. Обслуживание любого устройства необходимо осуществлять только в соответствии с системной документацией. При открытии и снятии крышек, отмеченных треугольным значком с изображением молнии, возможно поражение электрическим током. Указанные компоненты должны обслуживаться только квалифицированными техническими специалистами.
- Убедитесь, что кабель питания, удлинитель и разъем не повреждены.
- Убедитесь, что устройство не подвергается воздействию влаги.
- Убедитесь, что устройство не размещается вблизи радиаторов отопления и других источников тепла.
- Убедитесь, что охлаждающие вентиляторы не заблокированы.
- Не вставляйте посторонние предметы в устройство, так как это может вызвать возгорание или поражение электрическим током.
- Используйте устройство только с оборудованием, для которого оно предназначено.
- Прежде чем снимать крышки или прикасаться к внутреннему оборудованию, дайте устройству остыть.
- Убедитесь, что устройство не перегружает силовые цепи, электропроводку и схемы защиты от перегрузки. Для определения вероятности перегрузки цепей питания необходимо суммировать силы электрического тока для всех устройств, смонтированных в одной цепи. Сравните это суммарное значение с заданным ограничением для цепи.
- Не монтируйте устройство в среде, в которой окружающая температура может превысить 45°C (113°F).
- Убедитесь, что есть свободный доступ воздуха к передней панели, боковым и задней стенкам устройства.

Требования к месту размещения

Устройство можно устанавливать в стандартную 19-дюймовую стойку или на столе. Перед установкой устройства убедитесь, что выбранное место для установки отвечает следующим требованиям:

- **Общее** - убедитесь, что подача питания производится правильно.
- **Питание** - устройство установлено на расстоянии 1,5 м (5 футов) от заземленной легко доступной розетки 220/110 В переменного тока, 50/60 Гц.
- **Расстояние** - имеется достаточное расстояние спереди для доступа оператора. Оставьте некоторое расстояние для силовых и сигнальных кабелей, а также для вентиляции.
- **Прокладка кабелей** - кабели следует прокладывать подальше от источников электрических помех, например, радиопередатчиков, усилителей, линий питания и осветительных приборов с флуоресцентными лампами.
- **Требования к окружающей среде** - во время работы температура окружающей среды должна быть в диапазоне от 0 до 45°C (от 32 до 113°F) при относительной влажности от 10% до 90 % без образования конденсата. Убедитесь, что вода или влага не проникают в корпус устройства.

Распаковка

Комплект поставки

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

- Устройство
- Кабель питания переменного тока
- Кроссоверный кабель RS-232
- Самоклеющиеся резиновые прокладки
- Крепежный набор для монтажа в стойке
- Компакт-диск с документацией

Распаковка устройства

Чтобы распаковать устройство:

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

ПРИМЕЧАНИЕ. Браслет для снятия электростатического разряда не входит в комплект, однако его рекомендуется надевать при выполнении следующей процедуры.

1. Установите контейнер на чистую ровную поверхность и обрежьте все крепежные ленты.
2. Откройте контейнер и снимите верхнюю его часть.
3. Аккуратно извлеките устройство из контейнера и установите его на устойчивую чистую поверхность.
4. Удалите весь упаковочный материал.
5. Осмотрите устройство на наличие повреждений. В случае обнаружения повреждений немедленно сообщите об этом.

Установка устройства

Общие сведения

Разъемы питания устройства находятся на задней панели. Подключение запасного блока питания постоянного тока (UPS) является необязательным, но рекомендуется. Разъем RPS постоянного тока находится на задней панели устройства.

Монтаж системы

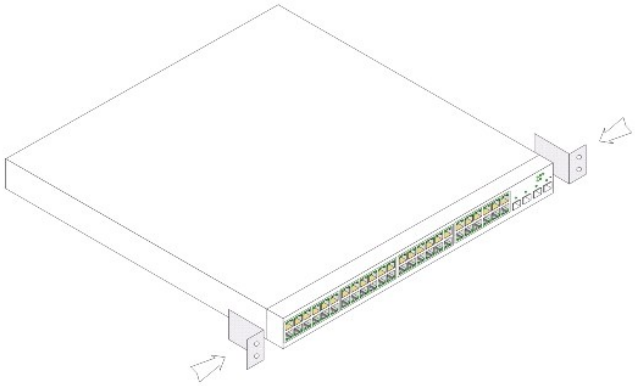
Монтаж устройства в стойке

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

ОСТОРОЖНЫ. При установке нескольких устройств в стойку устанавливайте устройства снизу вверх.

1. Установите прилагаемый кронштейн для установки в стойку с одной стороны устройства, чтобы крепежные отверстия на устройстве были совмещены с крепежными отверстиями на кронштейне. На рис. 3-1 показано, куда следует устанавливать кронштейны .

Рис. 3-1. Монтажные кронштейны соединительной стойки



2. Вставьте прилагаемые винты в отверстия и затяните с помощью отвертки.
3. Повторите то же самое для кронштейна установки в стойку с другой стороны устройства.
4. Вставьте устройство в 19-дюймовую стойку так, чтобы установочные отверстия на устройстве были совмещены с крепежными отверстиями в стойке.
5. Прикрепите устройство к стойке с помощью винтов (не входят в комплект). Сначала затяните нижнюю пару винтов, а затем верхнюю. Это гарантирует равномерное распределение веса устройства во время установки. Убедитесь, что вентиляционные отверстия не закрыты.

Установка устройства без стойки

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

1. Прикрепите резиновые ножки к устройству.
2. Установите устройство на ровную поверхность, оставив по 5,08 см (2 дюйма) с каждой стороны и 12,7 см (5 дюймов) сзади.
3. Убедитесь, что обеспечивается достаточная вентиляция устройства.

Подключение к устройству

Для настройки устройство необходимо подключить к терминалу.

Подключение устройства к терминалу

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

Для использования порта консоли требуется следующее:

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

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

1. Подсоедините кроссоверный кабель RS-232 к терминалу, на котором запущено программное обеспечение эмуляции терминала VT100.
2. Настройте программу эмуляции терминала следующим образом.
   a. Выберите соответствующий последовательный порт (последовательный порт 1 или последовательный порт 2) для подключения к консоли.
   b. Задайте скорость передачи данных 9600 бод.
   c. Задайте следующий формат данных: 8-битные данные, 1 стоповый бит, без контроля четности.

d. Установите для параметра управления потоком значение *none* (нет).

e. В разделе **Properties** (Параметры) выберите режим **VT100 for Emulation** (Эмуляции VT100).

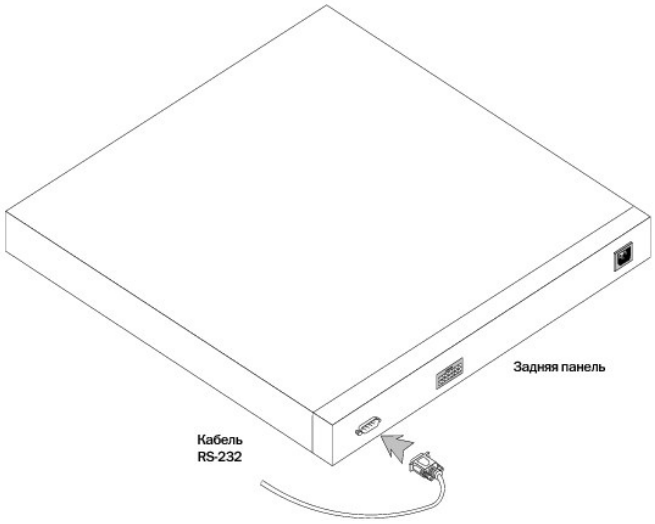
f. Выберите значение **Terminal keys** (Клавиши терминала) для **Function** (Функциональные клавиши), **Arrow** (Клавиши со стрелками) **и Ctrl**. Убедитесь, что выбраны **Terminal keys** (Клавиши терминала), *а не* **Windows keys** (Клавиши Windows).

△ **ПРЕДУПРЕЖДЕНИЕ. При использовании HyperTerminal с системой Microsoft® Windows 2000 убедитесь, что установлен пакет обновления 2 для Windows® 2000 или более поздней версии. При наличии пакета обновления 2 для Windows 2000 клавиши со стрелками правильно работают в программе эмуляции HyperTerminal VT100. Информацию о пакетах обновления для Windows 2000 можно найти на сайте www.microsoft.com.**

3. Подключите гнездовой разъем кроссоверного кабеля RS-232 напрямую в порт консоли устройства и затяните невыпадающие винты.

Порт консоли устройства расположен на задней панели.

Рис. 3-2. Подключение к порту консоли систем серии PowerConnect 54xx

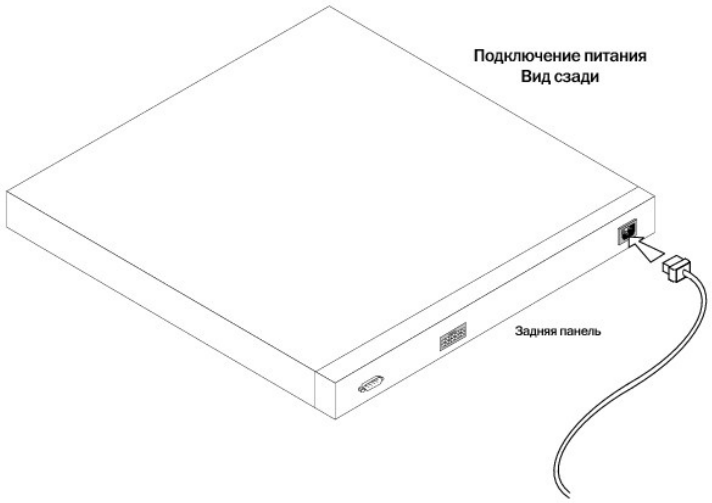


Подключение устройства к источнику питания

1. Используя стандартный кабель питания длиной 1,5 м (5 футов) с заземляющим контактом, подсоедините кабель питания к разъему электропитания на задней панели.

2. Подсоедините кабель питания к заземленной электророзетке.

Рис. 3-3. Подключение устройства к разъему питания



По состоянию индикаторов на передней панели проверьте, правильно ли подключено и работает устройство.

Подключение портов, кабели и расположение контактов

В этом разделе описаны физические интерфейсы и содержится информация о подключениях к портам. Сведения о типах подключений, портах и кабелях содержатся в разделе «Порты и разъемы и кабели». Поддерживаются диагностика медных и оптических трансиверов.

Разъемы RJ-45 для портов 10/100/1000BaseT

Порты 10/100/1000BaseT предназначены для подключения медных кабелей витой пары.

Чтобы установить соединение с портов для витой пары, пара Tx на одном кабеле должна быть подключена к паре Rx на другом конце кабеля и наоборот. При подключении кабелей таким образом, что Tx на одном конце подключена к Tx на другом конце, а Rx подключена к Rx, соединение не будет установлено.

При выборе кабелей для подключения портов устройства к соответствующим сетевым портам, кабели прямого подключения необходимо использовать для подключения устройства к станции, а кроссоверные кабели для подключения одно передающего устройство (коммутатор или концентратор) к другому. Кабели прямого подключения и кроссоверные кабели должны быть категории 5.

После подключения порта загорается его индикатор LINK.

Таблица 3-1. Ports, Connectors and Cables

Разъем	Порт/интерфейс	Кабель
RJ-45	Порт 10/100/1000BaseT	Кат.5

Номера и назначения штырьков разъема RJ-45 для портов 10/100/1000BaseT приводится в следующей таблице.

Таблица 3-2. Номера и назначения штырьков разъема RJ-45 для порта 10/100/1000BaseT Ethernet

№ штырька	Функция
1	TxRx 1+
2	TxRx 1-
3	TxRx 2+
4	TxRx 2-
5	TxRx 3+
6	TxRx 3-
7	TxRx 4+
8	TxRx 4-

Настройки порта по умолчанию

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

Автоматическое согласование

Автоматическое согласование позволяет автоматическое определение скорости, дуплексный режим, а также управление потоком при коммутировании портов 10/100/1000BaseT. Функция автоматического согласования по умолчанию включена на каждом порту.

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

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

Если станция на противоположной стороне канала попытается выполнить автосогласование с портом 10/100/1000BaseT устройства, для которого настроен полнодуплексный режим, то в результате автосогласования вызывающая станция будет переведена в полудуплексный режим.

MDI/MDIX

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

Если включен интерфейс MDI/MDIX (Media Dependent Interface with Crossover), возможно автоматическое исправление ошибок при выборе кабелей, что устраняет необходимость распознания кабеля прямого подключения и кроссоверного кабеля. (Стандарт кабелей для конечных станций - MDI (MDIMedia-Dependent Interface), а стандарт кабелей для концентраторов и коммутаторов - MDIX.)

Управление потоком

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

Обратное давление

Устройство поддерживает обратное давление для портов, настроенных для полудуплексного режима. По умолчанию эта функция отключена. Ее можно включить для каждого порта. Механизм обратного давления временно запрещает передающей стороне передачу дополнительного трафика. Принимающая сторона может занять соединение, делая его недоступным для дополнительного трафика.

Настройки по умолчанию для коммутируемых портов

В следующей таблице содержится описание настроек по умолчанию для порта.

Таблица 3-3. Настройки порта по умолчанию

Функция	**Настройка по умолчанию**
Скорость и режим работы порта	10/100/1000BaseT (для медных кабелей): автоматическое согласование, полнодуплексный
Состояние пересылки пакетов для порта	Enabled
Маркировка портов	Без маркировки
Управление потоком	Выкл (отключено на входе)
Обратное давление	Выкл (отключено на входе)

Назад на страницу Содержание

Назад на страницу Содержание

Введение

Руководство пользователя систем Dell™ PowerConnect™ 54xx

ПРЕДУПРЕЖДЕНИЕ. Перед выполнением дальнейших действий прочтите примечания к выпуску для этого продукта. Примечания к выпуску можно загрузить с веб-сайта support.dell.com.

Это руководство пользователя содержит информацию необходимую для установки, настройки и управления устройством PowerConnect.

Системы серии PowerConnect 54xx

Существует две версии систем серии PowerConnect 54xx: системы серии 5424 оснащены 24 портами Gigabit Ethernet, системы серии 5448 оснащены 48 портами Gigabit Ethernet. Системы также имеют четыре оптоволоконных порта SFP, назначенные как комбинированные порты, являющиеся альтернативой последним четырем портам Ethernet. Комбинированные порты представляют собой один порт, имеющий два физических подключения. Когда одно подключено, другое отключено.

На следующих рисунках изображены передняя и задняя панели систем серии PowerConnect 54xx.

Рис. 1-1. Передняя панель устройства PowerConnect 5424

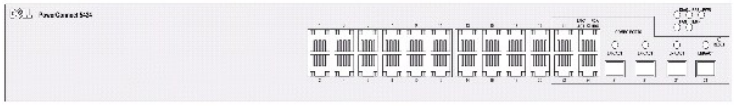


Рис. 1-2. Передняя панель устройства PowerConnect 5448

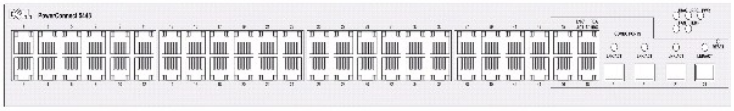
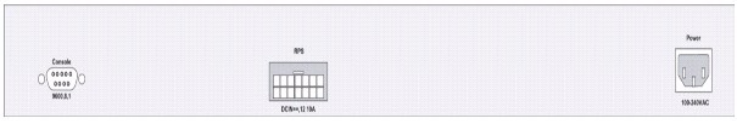


Рис. 1-3. Задняя панель устройств PowerConnect 5424 и 5428



Функции

В этом разделе описаны функции устройства, настраиваемые пользователем. Для получения списка всех обновленных функций устройства см. примечания к последнему выпуску программного обеспечения.

Общие функции

Поддержка IP версии 6 (IPv6)

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

Защита от блокировки очереди

Защита от блокировки очереди (HOL) приводит к задержке трафика и потере пакетов в том случае, когда трафик направляется на одни и те же наборы выходных портов. HOL блокирует пакеты очереди, и пакеты в начале очереди пересылаются до пакетов, находящихся в конце очереди.

Виртуальное тестирование кабеля (VCT)

VCT определяет 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. Это уменьшает объем служебной информации, время обработки и перерывы.

Дополнительную информацию о поддержке больших кадров см. в разделе Определение общих сведений об устройстве.

Поддержка MDI/MDIX

Устройство автоматически обнаруживает, какой кабель подключен - перекрестный кабель или кабель прямого подключения.

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

Дополнительную информацию о настройке MDI/MDIX для портов или объединенных групп каналов (LAG) см. в разделах Определение параметров порта или Настройка выравнивания нагрузки.

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.

Дополнительную информацию о настройке управления потоком для портов или групп LAG см. в разделах Определение параметров порта или Настройка выравнивания нагрузки.

Поддержка обратного давления

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

Дополнительную информацию о настройке обратного давления для портов или групп LAG см. в разделах Определение параметров порта или Настройка выравнивания нагрузки.

Оптимизация iSCSI

iSCSI - протокол связи, используемый для обмена данными между файловыми серверами и носителями. Файловые серверы называются *инициаторами*, а диски - *конечными устройствами*. Можно оптимизировать поток iSCSI, установив параметры приоритета кадров с помощью функции Quality of Service (Качество обслуживания) на устройстве. Устройство может также перехватывать кадры iSCSI и предоставлять информацию о связи iSCSI (называемой сеансами).

Для получения дополнительной информации см. раздел Оптимизация iSCSI.

Голосовая сеть VLAN

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

Дополнительную информацию см. в разделе Настройка голосовых сетей VLAN.

Гостевая сеть VLAN

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

Функции, поддерживающие MAC-адреса

Поддержка возможности MAC-адресов

Устройство поддерживает до восьми тысяч MAC-адресов. Устройство резервирует определенные MAC-адреса для использования системой.

Самораспознаваемые MAC-адреса

Устройство позволяет автоматически распознавать MAC-адреса во входящих пакетах. MAC-адреса сохраняются в таблице связей.

Автоматическое время хранения MAC-адресов

MAC-адреса, от которых за определенный период времени не поступает трафика, устаревают. Это позволяет предотвратить переполнение таблицы связей.

Дополнительную информацию о сроке хранения MAC-адресов см. в разделе Настройка адресных таблиц.

Статические записи MAC

Определяемые пользователем статические записи MAC-адресов, которые сохраняются в **таблице связей**.

Дополнительную информацию см. в разделе Настройка адресных таблиц.

Коммутация, основанная на MAC-адресах, с поддержкой VLAN

Пакеты, полученные от неизвестного источника, отправляются на обработку процессору, где адреса источника добавляются в аппаратную таблицу, В дальнейшем пакеты, полученные или направленные по этим адресам, будут передаваться более эффективно с использованием аппаратной таблицы.

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. Поддерживается наблюдение по протоколу IGMP, включая опрашивающее устройство IGMP, которое имитирует работу маршрутизатора многоадресной передачи, обеспечивая отслеживание многоадресного домена Layer 2 даже при отсутствии маршрутизатора многоадресной передачи. Если включены статические группы многоадресной передачи, вы можете установить порт назначения зарегистрированных групп и определить поведение многоадресных кадров.

Дополнительную информацию см. в разделе Поддержка пересылки многоадресного трафика.

Функции Layer 2

Наблюдение по протоколу IGMP

Наблюдение на базе протокола IGMP (Internet Group Membership Protocol) проверяет содержимое кадров IGMP, когда они пересылаются устройством от станций на многоадресные маршрутизаторы. Кадр позволяет устройству определить рабочие станции, настроенные для многоадресных сеансов, а также, какие маршрутизаторы посылают многоадресные кадры.

Дополнительную информацию см. в разделе Наблюдение по протоколу IGMP.

Страница Port Mirroring

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

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

Защита от «лавины» широковещательной передачи

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

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

Дополнительную информацию см. в разделе Включение контроля «лавины».

Поддержка функций VLAN

Поддержка VLAN

VLAN представляют собой совокупности коммутируемых портов, входящих в состав одного домена широковещательной передачи. Принадлежность пакетов VLAN определяется либо на основе метки VLAN, либо на основе комбинации входящего порта и содержимого пакета. Пакеты с одинаковыми атрибутами, можно объединить в одну группу VLAN.

Дополнительную информацию см. в разделе Настройка протокола Multiple Spanning Tree.

VLAN, основанные на портах

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

Дополнительную информацию см. в разделе Определение параметров портов VLAN.

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 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. Одним из важных требований для этого стандарта является возможность отметки кадров с помощью необходимого значения метки класса обслуживания (CoS) (0-7).

QinQ

Маркировка пакетов QinQ позволяет сетевым администраторам добавлять дополнительные метки на предварительно помеченные пакеты. Клиентские сети VLAN настраиваются при использовании QinQ. Добавление дополнительных меток на пакеты помогает расширить пространство VLAN. Дополнительная метка является для каждого клиента идентификатором VLAN (VLAN ID), что обеспечивает частный характер сетевого трафика и его изолированность. Идентификатор VLAN ID назначается для порта клиента в сети поставщика услуг. Затем для назначенного порта предоставляются дополнительные услуги для пакетов с двойными метками. Это позволяет администраторам расширять обслуживание пользователей VLAN.

Поддержка GVRP

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

Дополнительную информацию см. в разделе Настройка протокола GVRP.

Функции протокола Spanning Tree

Протокол STP (Spanning Tree Protocol)

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

Дополнительную информацию см. в разделе Настройка протокола STP.

Быстрая связь

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

Дополнительную информацию о включении функции Fast Link для портов и групп LAG см. в разделах Определение параметров STP для порта или Определение параметров STP для LAG.

Поддержка протокола IEEE 802.1w Rapid Spanning Tree

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

Дополнительную информацию см. в разделе Настройка протокола RSTP.

STP Root Guard

Функция Root Guard ограничивает работу интерфейса в качестве корневого порта для коммутатора.

Multiple Spanning Tree (MSTP)

Протокол MTSP сопоставляет сети VLAN в экземплярах STP. Данный протокол обеспечивает другой сценарий выравнивания нагрузки. Пакеты, назначенные разным VLAN, передаются через разные пути в областях MST. Областями являются один или несколько мостов Multiple Spanning Tree, по которым передаются кадры.

Страница Link Aggregation (Объединение каналов)

Дополнительную информацию см. в разделе Объединение портов.

Страница Link Aggregation (Объединение каналов)

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

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

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

Дополнительную информацию см. в разделе Определение принадлежности к группе 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 см. в разделе Определение параметров протокола LACP.

Функции Layer 3

Протокол ARP (Address Resolution Protocol)

ARP - это протокол TCP/IP для преобразования IP-адресов в физические адреса. 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 см. в разделе Отображение хоста домена.

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.

Клиенты BootP и DHCP

Протокол DHCP (Dynamic Host Configuration Protocol) 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.

Функции качества обслуживания (Quality of Service)

Поддержка класса обслуживания 802.1p

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

Дополнительную информацию см. в разделе Настройка качества обслуживания.

Функции управления устройствами

Сигналы и журналы прерываний SNMP

События журнала системы с кодами серьезности и отметками времени. События передаются как прерывания SNMP (Simple Network Management Protocol) списку получателей прерываний.

Дополнительную информацию о сигналах и прерываниях SNMP см. в разделе Настройка LLDP и LLDP-MED.

Протокол SNMP версии 1 и 2

Протокол SNMP (Simple Network Management Protocol) поверх протокола UDP/IP. Для управления доступом к системе определяется список записей сообщества, каждая из которых содержит строку сообщества и привилегии доступа. Существуют 3 уровня безопасности SNMP только чтение, чтение и запись и супер. К таблице сообщества имеет доступ только суперпользователь.

SNMP версии 3

Доступ к коммутатору SNMPv3 обеспечивает дополнительные функции безопасности, которые касаются целостности сообщений, проверки подлинности и шифрования, а также контроля доступа пользователя к определенным областям MIB-дерева. Структура безопасности SNMPv3 состоит из моделей безопасности, и каждая модель имеет свои уровни безопасности.

Управление через веб-интерфейс

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

Загрузка и выгрузка файла настройки

Настройка устройства PowerConnect сохраняется в файле настройки. Файл настройки содержит данные настройки как всей системы, так и настройку определенного порта устройства. Система может отображать файлы настройки в форме набора команд CLI, которые хранятся и обрабатываются как текстовые файлы.

Дополнительную информацию см. в разделе Управление файлами.

Протокол TFTP (Trivial File Transfer Protocol)

Устройство поддерживает загрузку и передачу по протоколу TFTP образа загрузки, программного обеспечения и файлов настройки.

Удаленный мониторинг

Удаленный мониторинг (RMON) - это расширение протокола SNMP, предоставляющее широкие возможности контроля сетевого трафика с поддержкой 64-битных счетчиков (в отличие от протокола SNMP, в котором возможен контроль и управление сетевым устройством). RMON - это стандартная база

MIB, в которой определены текущая и предыдущая статистика уровня MAC и объекты управления, предоставляющая данные в реальном времени для захвата по всей сети.

Дополнительную информацию см. в разделе Просмотр статистики удаленного мониторинга RMON.

Интерфейс командной строки

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

Syslog

Syslog - это протокол, который обеспечивает передачу уведомлений об ошибках удаленным серверам, где их можно сохранить, изучить или выполнить соответствующие действия. Реализованы многочисленные механизмы для отправки уведомления о значимых событиях в режиме реального времени и сохранения записи об этих событиях для последующего использования.

Дополнительную информацию о Syslog см. в разделе Управление журналами.

SNTP

Протокол SNTP (Simple Network Time Protocol) гарантирует точность синхронизации времени такта сетевого устройства до миллисекунды. Синхронизация по времени выполняется сетевым сервером SNTP. Источники времени устанавливаются по уровням. Уровни определяют расстояние от генератора тактовых импульсов. Чем выше уровень (где нуль - это самый высокий уровень), тем более точный генератор.

Дополнительную информацию 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 в режимах Privileged.

802.1ab (LLDP-MED)

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

Функция LLDP Media Endpoint Discovery (LLDP-MED) повышает гибкость сети, обеспечивая сосуществование различных систем IP в единой сети LLDP. Он предоставляет подробную информацию о топологии сети, о службе экстренных вызовов с использованием информации о расположении IP-телефона и информацию о поиске и устранении неисправностей.

Средства защиты

SSL

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

Проверка подлинности на основе порта (802.1x)

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

Дополнительную информацию см. в разделе Настройка проверки подлинности на основе порта.

Поддержка заблокированных портов

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

Дополнительную информацию см. в разделе Настройка безопасности портов.

Клиент RADIUS

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

Дополнительную информацию см. в разделе Настройка общих параметров RADIUS.

Страница SSH

Secure Shell (SSH) - это протокол, обеспечивающий защиту и удаленное подключение к устройству. В настоящее время имеется SSH версии 1. Функция сервера SSH позволяет клиенту SSH установить с устройством безопасное кодируемое соединение. Это соединение предоставляет функциональные возможности, аналогичные входящему соединению telnet. SSH использует шифрование с открытым ключом RSA для соединений с устройствами и проверки подлинности.

TACACS+

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

Дополнительную информацию см. в разделе Определение параметров TACACS+.

Списки управления доступом ACL

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

Дополнительную информацию см. в разделе Обзор списка ACL.

Наблюдение по протоколу DHCP

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

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

Дополнительная документация по режиму консоли

Справочное руководство по командной строке, которое находится на компакт-диске с документацией, содержит сведения о командах консоли, используемых для конфигурирования коммутаторов. Документ содержит важную информацию, включая описание CLI, синтаксис, значения по умолчанию, инструкции и примеры.

Назад на страницу Содержание

Назад на страницу Содержание

Настройка качества обслуживания

Руководство пользователя систем Dell™ PowerConnect™ 54xx

В этом разделе содержатся инструкции для определения и настройки параметров качества обслуживания (QoS). Чтобы открыть страницу, выберите **Quality of Service** (Качество обслуживания) на панели дерева.

Показатель Quality of Service (Качество обслуживания - QoS) позволяет обеспечить качество обслуживания и очередь приоритетов внутри сети. QoS улучшает поток сетевого трафика на основе политик, счетчиков кадров и контекста.

В качестве примеров области применения, в которой требуется QoS, можно привести некоторые типы трафика, например, голосовой, видео- и трафик данных реального времени, которым присваивается приоритетная очередность, в то время, как другим типам трафика присваивается очередность низшего приоритета. Это позволяет ускорить прохождение первоочередного трафика.

Показатель QoS характеризуется следующими элементами.

- **Classification** (Классификация). Определяет,какие поля соответствуют тем или иным значениям. Все пакеты, соответствующиепользовательским спецификациям, классифицируются вместе.
- **Action** (Действие). Определяет управлениетрафиком, в котором пакеты пересылаются по информации о пакете, а такжеопределяет значения полей пакетов, например приоритет VLAN (VPT) и DSCP(DiffServ Code Point).

Информация о классификации метки VPT

VLAN Priority Tags (Метки приоритета VLAN) используются для классификации пакетов путем их привязки к одной из очередей вывода. VLAN Priority Tag (Метка приоритета VLAN) для назначений очереди также определяются пользователем. В таблице ниже представлена подробная информация по меткам VPT для параметров очереди по умолчанию.

Значение CoS	Значения очереди пересылки
0	q3
1	q1
2	q2
3	q4
4	q5
5	q6
6	q7
7	q8

Для непомеченных при поступлении пакетов по умолчанию назначается метка VPT, которая устанавливается отдельно для каждого порта. Назначенная метка VPT используется для привязки пакета к очереди вывода и выступает в качестве выходной метки VPT.

Значения DSCP можно поставить в соответствие очереди приоритетов. В следующей таблице представлена привязка DSCP по умолчанию к значениям очереди пересылки.

Значение DSCP	Значения очереди пересылки
0-7	q1
8-15	q2
16-23	q3
24-31	q4
32-39	q5
40-47	q6
48-55	q7
56-63	q8

Привязка DSCP активизируется индивидуально для каждой системы.

Обслуживание CoS

После постановки пакетов в определенную очередь обслуживание CoS можно привязать к очереди (очередям). Настройка очередей вывода осуществляется с помощью схемы планирования одним из следующих способов.

- **Strict Priority** (Строгий приоритет). Гарантирует, что чувствительные ко времени приложения всегда передаются по скоростному пути. Strict Priority (Строгий приоритет) позволяет присвоить приоритеты для зависящего от целевого назначения и чувствительного ко времени трафика

через менее чувствительные ко времени приложения.
Например, при выборе способа Strict Priority (Строгий приоритет) передача голоса по IP осуществляется до пересылки трафика FTP или электронной почты (SMTP).
Очередь строгого приоритета очищается до пересылки трафика в оставшихся очередях.

- **Weighted Round Robin**. Гарантирует, что одно приложение не будет использовать все ресурсы устройства по пересылке. С помощью WRR осуществляется пересылка всех очередей в цикле. Приоритеты очереди определяются по длине очереди. Чем длиннее очередь, тем выше ее приоритет пересылки.
Например, если восемь очередей имеют веса 1, 2, 3, 4, 5, 6, 7 и 8, пакеты с высшим приоритетом пересылки будут назначены для очереди 8, а пакеты с низшим приоритетом пересылки - для очереди 1.
Устанавливая высший приоритет пересылки для очередей с длиной 8, WRR обрабатывает трафик высшего приоритета и гарантирует, что пересылка трафика низшего приоритета осуществляется надлежащим образом.

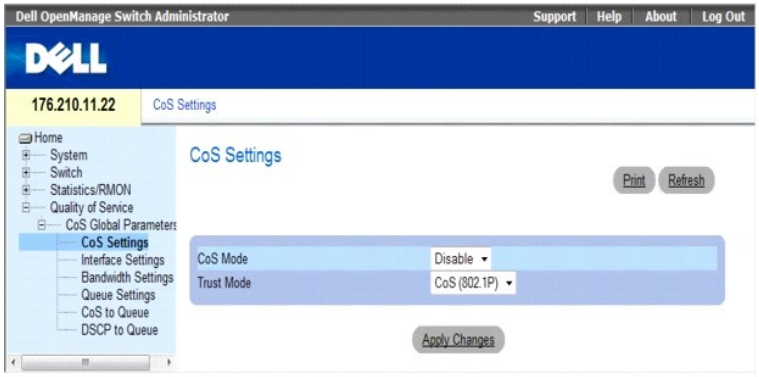
Схема планирования активируется для системы в целом. Для очередей со строгим приоритетом автоматически устанавливается очередь высшего приоритета. По умолчанию, всем величинам присваивается строгий приоритет. Значения весов очереди могут быть назначены в любом порядке с помощью WRR. Значения WRR можно назначить для всей системы. Трафик с максимально возможной скоростью доставки всегда поступает в очередь 1. Значения WRR должны назначаться так, чтобы очередь 1 оставалась наименее занятой для обслуживания такого трафика.

Определение общих параметров CoS

Общие параметры класса обслуживания устанавливаются на странице **CoS Settings** (Параметры CoS).

Чтобы открыть страницу **CoS Settings** (Параметры QoS), на панели дерева выберите **Quality of Service** (Качество обслуживания)→ **CoS Global Parameters** (Общие параметры CoS)→ **CoS Settings** (Параметры CoS).

Рис. 9-1. Параметры CoS



- **Cos Mode** (Режим CoS). Включает или отключает управление сетевым трафиком с помощью функции Quality of Service (Качество обслуживания).
- **Trust Mode** (Режим доверия). Определяет, какие поля будут использоваться для классификации пакетов, поступающих на устройство. Если ни одно правило не определено, трафик, содержащий предварительно определенные поля (CoS или DSCP), будет привязан к соответствующей таблице режимов доверия. Трафик, не содержащий предварительно определенных полей, привязывается к максимально возможной скорости доставки. Ниже указаны возможные значения поля Trust Mode (Режим доверия).
  - **CoS (802.1P)**. Назначение очереди вывода определяется меткой приоритета IEEE802.1p VLAN (VPT) или меткой VPT по умолчанию, назначенной для порта.
  - **DSCP**. Назначение очереди вывода определяется полем DSCP. Параметры интерфейса Trust (Доверие) заменяют общие параметры Trust (Доверие).

Включение функции Class of Service (Качество обслуживания)

1. Откройте страницу **CoS Settings** (Параметры Cos).
2. Выберите **Enable** (Включено) в поле **CoS Mode** (Режим CoS).
3. Нажмите кнопку Apply Changes (Применить изменения).

   На устройстве будет включена функция Class of Service (Качество обслуживания).

Включение режима Trust (Доверие)

1. Откройте страницу **CoS Settings** (Параметры Cos).
2. Выберите **Trust** (Доверие) в поле **Trust Mode** (Режим доверия).

3. Нажмите кнопку Apply Changes (Применить изменения).

   На устройстве будет включен режим Trust (Доверие).

Включение режима доверия с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для настройки полей, отображаемых на странице **CoS Settings** (Параметры CoS).

Команда консоли	Описание
qos trust [cos | dscp]	Настройка основного режима системы и переключение ее в состояние «доверия».
no cos trust	Возврат в состояние «без доверия».

Далее приведен пример команд консоли.

```
Console (config)# cos trust dscp
```

Определение параметров интерфейса QoS

На странице **Interface Settings** (Параметры интерфейса) имеются поля для каждого интерфейса, позволяющие определить, должен ли быть включен выбранный режим Trust (Доверие). Установка приоритета по умолчанию для входящих непомеченных пакетов также осуществляется на странице **Interface Settings**. Чтобы открыть страницу**Interface Settings**, на панели дерева выберите **Quality of Service** (Качество обслуживания)→ **CoS Global Parameters** (Общие параметры CoS)→ **Interface Settings** (Установки интерфейса).

Рис. 9-2. Страница Interface Settings (Параметры интерфейса)

- **Interface** (Интерфейс). Определенный порт или группа LAG для настройки:
- **Disable «Trust» Mode on Interface** (Отключить режим доверия для интерфейса). Отключает режимдоверия для выбранного интерфейса. Этот параметр заменяет режим Trust(Доверие), настроенный на устройстве.
- **Set Default CoS For Incoming Traffic To** (Задать CoS по умолчанию для входящего трафика). Определяет значениеметки CoS по умолчанию для входящих непомеченных пакетов. Метки CoS могут иметьзначения от 0 до 7. Значение по умолчанию - 0.

Назначение параметров QoS/CoS для интерфейса

1. Откройте страницу **Interface Settings** (Параметры интерфейса).
2. Выберите интерфейс в поле **Interface** (Интерфейс).
3. Определите поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

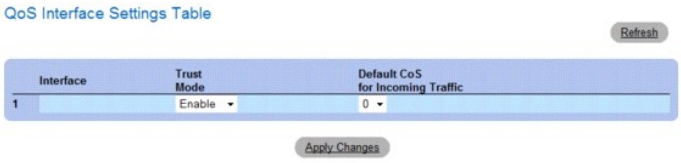
   Параметры CoS будут назначены для интерфейса.

Отображение таблицы параметров интерфейса QoS:

1. Откройте страницу **Interface Settings** (Параметры интерфейса).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется **страница с таблицей установок интерфейса QoS**.

Рис. 9-3. Таблица параметров интерфейса QoS



Назначение CoS для интерфейсов с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для настройки полей, отображаемых на странице **Interface Settings** (Параметры интерфейса).

Команда консоли	**Описание**
qos trust	Включение состояния доверия для каждого порта.
qos cos *cos_по_умолчанию*	Настройка значения по умолчанию для порта CoS.
no qos trust	Отключение состояния Trust (Доверие) для каждого порта.

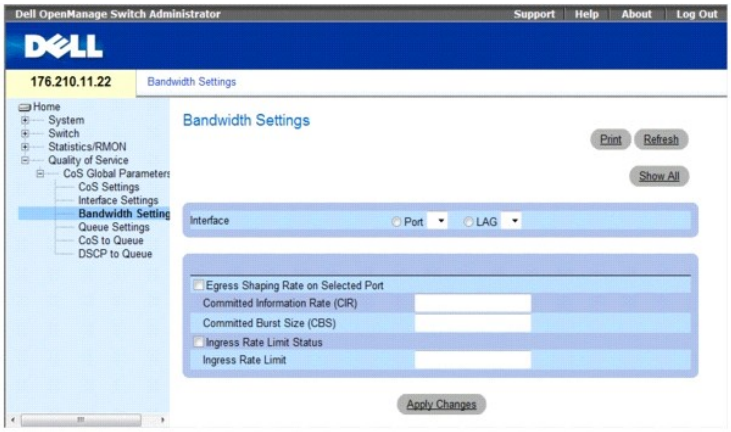
Далее приведен пример команд консоли.

```
Console (config)# interface ethernet g5

Console (config-if)# qos trust

Console (config-if)# qos cos 3
```

Определение параметров полосы пропускания

На странице **Bandwidth Settings** (Параметры полосы пропускания) находятся поля для определения параметров полосы пропускания для указанного выходящего интерфейса. Изменение графика очередей влияет на общие параметры очередей. Формирование очередей возможно на основе очередей и/или интерфейсов. Формирование определяется по наименьшей из указанных величин. Тип формирования очереди можно выбрать на странице Bandwidth Settings (Параметры полосы пропускания): на панели дерева выберите **Quality of Service** (Качество обслуживания)→ **CoS Global Parameters** (Общие параметры CoS)→ **Bandwidth Settings** (Параметры полосы пропускания).

Рис. 9-4. Параметры полосы пропускания



- **Interface** (Интерфейс). Указание порта или группы LAG, которые отображаются.

- **Egress Shaping Rate on Selected Port** (Скорость формирования выхода для выбранного порта). отображение состояния ограничения выходного трафика интерфейса.
  - **Checked** (Отмечено флажком). Ограничение выходного трафика включено.
  - **Not Checked** (Флажок снят). Ограничение выходного трафика выключено.
- **Committed Information Rate (CIR)** (Гарантированная скорость передачи данных (CIR)). Определениеограничения выходного трафика CIR для интерфейса.
- **Committed Burst Size** (Гарантированный объем данных (CBS)). определение ограничения выходного трафика CBS для интерфейса.
- **Ingress Rate Limit Status** (Состояние ограничения скорости на входе). Отображение состоянияограничения трафика на входе для интерфейса.
  - **Checked** (Отмечено флажком). Ограничение входного трафика включено.
  - **Not Checked** (Флажок снят). Ограничение трафика на входе выключено.
- **Ingress Rate Limit** (Ограничение скорости на входе). Определениеограничения трафика на входе для интерфейса.

Назначение параметров полосы пропускания для интерфейса:

1. Откройте страницу **Bandwidth Settings** (Параметры полосы пропускания).
2. Выберите интерфейс в поле **Interface** (Интерфейс).
3. Определите поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Параметры полосы пропускания будут назначены для интерфейса.

Отображение таблицы параметров полосы пропускания:

1. Откройте страницу **Bandwidth Settings** (Параметры полосы пропускания).
2. Нажмите кнопку **Show All** (Показать все).

   Отобразится таблица параметров полосы пропускания.

Рис. 9-5. Таблица параметров полосы пропускания

Присвоение параметров полосы пропускания с помощью команд консоли

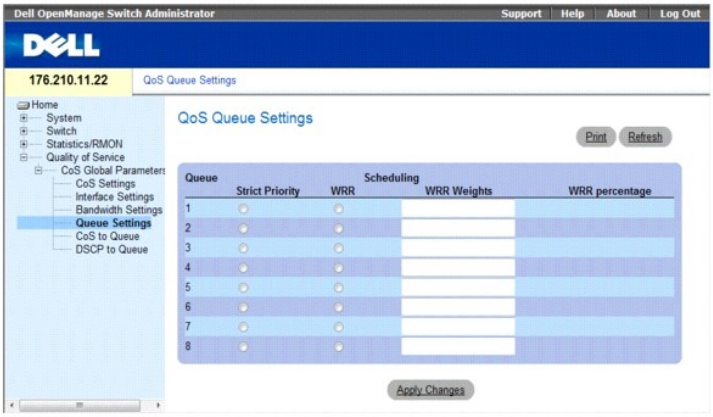
В следующей таблице приведены эквивалентные команды консоли для настройки полей, отображаемых на странице **Bandwidth Settings** (Параметры полосы пропускания).

Команда консоли	**Описание**
traffic-shape (форма трафика) *committed-rate (гарантированная_скорость)* [*committed-burst (гарантированный_объем)*] **no traffic-shape** (нет формы трафика)	Настройка формирователя для выходящего порта. Не используйте форму для отключения формирователя.
rate-limit (предел скорости) **no rate-limit** (предел скорости не установлен)	Ограничение скорости входящего трафика. Не используйте форму для отключения ограничения скорости.

Определение параметров очереди

На странице **QoS Queue Settings** (Параметры очереди QoS) находятся поля для настройки метода планирования, поддерживающего очереди. Чтобы открыть страницу **QoS Queue Settings** (Параметры очереди QoS) на панели дерева выберите **Quality of Service** (Качество обслуживания)→ **CoS Global Parameters** (Общие параметры CoS)→ **Queue Settings** (Параметры очереди).

Рис. 9-6. Параметры очереди QoS



- **Queues** (Очереди). номер очереди.
- **Strict Priority** (Строгий приоритет). Показывает, что планирование трафика основано строго на приоритете очереди. По умолчанию этот параметр включен.
- **WRR**. Показывает, что планирование трафика основано на весах Weighted Round Robin (WRR) для очередей выхода. Значения по умолчанию - 1 для очереди 1, 2 для очереди 2, 8 для очереди 3, 16 для очереди 4, 32 для очереди 5, 64 для очереди 6, 128 для очереди 7, 255 для очереди 8.
- **WRR Weights** (Вес WRR). Вес WRR, назначенный для каждой очереди.
- **WRR Percentage** (Значение WRR в процентах). Значение WRR для каждой очереди в процентах.

Определение параметров очереди

1. Откройте страницу **QoS Queue Settings** (Параметры очереди QoS).
2. Определите поля.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

   Параметры очереди будут определены, а устройство обновлено.

Назначение параметров очереди с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для настройки полей, отображаемых на странице **QoS Queue Settings** (Параметры очереди QoS).

Команда консоли	**Описание**
wrr-queue bandwidth *вес1 вес2. вес_n*	Назначает веса WRR для очередей выхода.
show qos interface [**ethernet** *номер_интерфейса*] [**queuing**]	Отображение данных QoS для интерфейса.

Далее приведен пример команд консоли.

```
Console (config)# wrr-queue bandwidth 10 20 30 40

Console(config)# exit

Console# exit

Console> show qos interface ethernet g1 queueing
```

```
Ethernet g1

wrr bandwidth weights and EF priority:
```

```
Console (config)# wrr-queue bandwidth 10 20 30 40

Console(config)# exit

Console# exit

Console> show qos interface ethernet g1 queueing

Ethernet g1

wrr bandwidth weights and EF priority:
```

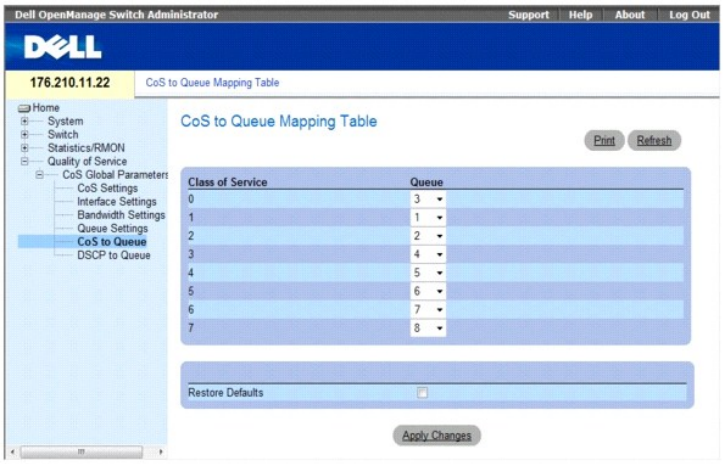
qid	weights	Ef	Priority
-----	--------	-----	----------
1	1	Disable	N/A
2	2	Disable	N/A
3	8	Disable	N/A
4	16	Disable	N/A
5	32	Disable	N/A
6	64	Disable	N/A
7	128	Disable	N/A
8	256	Disable	N/A

```
Cos queue map:

Cos qid

0 3

1 1

2 2

3 4

4 5

5 6

6 7

7 8
```

Привязка значений CoS к очередям

На странице **CoS to Queue Mapping Table** (Таблица привязки CoS к очереди) находятся поля для классификации параметров CoS для очередей трафика. Чтобы открыть страницу **CoS to Queue Mapping Table** (Таблица привязки CoS к очереди), на панели дерева выберите **Quality of Service** (Качество обслуживания)→ **CoS Global Parameters** (Общие параметры CoS)→ **CoS to Queue** (CoS к очереди).

Рис. 9-7. Таблица привязки CoS к очереди



- **Class of Service** (Класс обслуживания). Определяет значения метки приоритета CoS, где 0 - это низший класс, а 7 - высший.
- **Queue** (Очередь). Очередь пересылки трафика, к которой привязан приоритет CoS. Поддерживаются очереди приоритета трафика.
- **Restore Defaults** (Восстановить значения по умолчанию). Восстанавливаетзаводские файлы устройства для привязки значений CoS к очереди пересылки.

Привязка значения CoS к очереди

1. Откройте страницу **CoS to Queue Mapping Table** (Таблица привязки CoS к очереди).
2. Выберите запись CoS.
3. Определите номер очереди в поле **Queue** (Очередь).
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Значение CoS будет привязано к очереди, а устройство обновлено.

Привязка значений CoS к очередям с помощью команд консоли

В следующей таблице приведены команды консоли для настройки полей, отображаемых на странице **CoS to Queue Mapping Table** (Таблица привязки CoS к очереди).

Команда консоли	**Описание**
wrr-queue cos-map (карта очереди) *идентификатор_очереди cos1.cos8*	Связь значений CoS для выделения приоритетных очередей выхода.

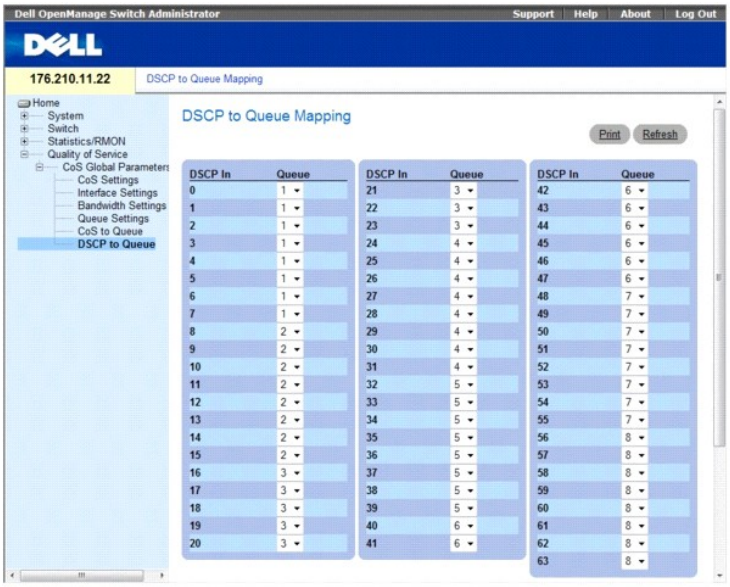
Далее приведен пример команд консоли.

```
Console (config)# wrr-queue cos-map 4 7
```

Привязка значений DSCP к очередям

На странице **DSCP to Queue** (DSCP к очереди) находятся поля для определения очереди выхода для определенных полей DSCP. Список параметров очереди по умолчанию DSCP представлен в разделе DSCP to Queue Mapping Table Default Values (Значения по умолчанию для таблицы привязки DSCP к очереди). Чтобы открыть страницу **DSCP to Queue** (DSCP к очереди), на панели дерева выберите **Quality of Service** (Качество обслуживания)→ **CoS Global Parameters** (Общие параметры CoS)→ **DSCP to Queue** (DSCP к очереди).

Рис. 9-8. DSCP к очереди



- **DSCP In** (DSCP входящего пакета). Значения в поле DSCP внутри входящего пакета.
- **Queue** (Очередь). Очередь, для которой назначены пакеты с определенным значением DSCP. Значения: от 1 до 8, где 1 - это наименьшее значение, а 8 - наибольшее.

Привязка значения DSCP и назначение очереди приоритета

1. Откройте страницу **DSCP to Queue** (DSCP к очереди).
2. Выберите значение в столбце **DSCP In** (DSCP входящего пакета).
3. Определите поля **Queue** (Очередь).
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   DSCP перезаписывается, а значение назначается для очереди пересылки.

Восстановление значений по умолчанию:

1. Откройте страницу **DSCP to Queue** (DSCP к очереди).
2. Установите флажок **Restore Defaults** (Восстановить значения по умолчанию).
3. Нажмите кнопку **Apply Changes** (Применить изменения).

   Значения по умолчанию будут восстановлены.

Привязка значений DSCP с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для настройки полей, отображаемых на странице **DSCP to Queue** (DSCP к очереди).

Команда консоли	**Описание**
qos map dscp-queue (карта очереди) *dscp-list toqueue-id (список идентификаторов очереди)*	Изменение привязки DSCP к очереди.

Далее приведен пример команд консоли.

```
Console (config)# qos map dscp-queue 33 40 41 to 1
```

Назад на страницу Содержание

Назад на страницу «Содержание»

Технические характеристики устройства

Руководство пользователя систем Dell™ PowerConnect™ 54xx

Данное приложение содержит необходимые сведения для запуска устройства.

Характеристики портов и кабелей

В этом разделе описаны характеристики портов.

Характеристики портов

В следующей таблице описаны типы портов устройства, а также описание типов портов.

Таблица 10-1. Характеристики портов

Устройство	**Характеристика**
PowerConnect 5400	▪ 24 порта GE или 48 портов GE ▪ 4 порта SFP ▪ Порт консоли RS-232
Типы портов	
RJ-45	▪ 10 Base-T ▪ 100 Base-T ▪ 1000 Base-T
SFP	Поддерживает стандартные миниатюрные разъемы Подключаемые гигабитные трансиверы
Параметры порта	
	▪ Автоматическое согласование скорости, дуплексный режим и управление потоком ▪ Обратное давление ▪ Защита от блокировки очереди ▪ Автоматический выбор MDI/MDIX ▪ Зеркалирование портов ▪ Защита от«лавины» широковещательной передачи

Условия работы

В этом разделе описаны условия эксплуатации, включая рабочую температуру и влажность.

Таблица 10-2. Условия работы

Параметр	**Характеристика**
Рабочая температура	от 0 до 45 C/от 32 до 113 F
Относительная влажность при работе	от 10% до 90% (без конденсации)

Физические характеристики устройства

В этом разделе описаны условия эксплуатации, включая рабочую температуру и влажность.

Таблица 10-3. Физические характеристики устройства

Параметр	Характеристика
Размер блока	• Ширина 19" • Высота 1U
Вентиляция	Два вентилятора на блок.

Характеристики памяти устройства

В этом разделе описаны характеристики памяти устройства.

Таблица 10-4. Характеристики памяти устройства

Тип памяти	Объем
DRAM ЦП	64 МБ
Флэш-память	16 МБ
Память с пакетным буфером	2 МБ

Характеристики функций

VLAN

- Поддержка VLAN на основе маркировки и портов в соответствии с IEEE 802.1Q
- Поддерживается до 4094 групп VLAN
- Зарезервированные группы VLAN для внутреннего использования системой
- Динамические группы VLAN с поддержкой GVRP
- Группы VLAN на основе протокола

Качество обслуживания

- Режим доверия Layer 2 (маркировка IEEE 802.1p)
- Режим доверия Layer 3 (DSCP)
- Настраиваемый режим WRR (Weighted Round Robin)
- Настраиваемое строгое планирование очередей

Многоадресная передача Layer 2

- Поддержка динамической многоадресной передачи - до 256 групп многоадресной передачи в режиме слежения IGMP или статической многоадресной передачи для незарегистрированных многоадресных групп

Безопасность устройства

- Защита доступа к коммутатору с помощью пароля
- Сигналы и блокировки на основе MAC-адреса порта
- Удаленная проверка подлинности RADIUS для доступа к коммутатору с целью управления
- TACACS+
- Фильтрация доступа для управления с помощью профилей доступа для управления
- Шифрование управления SSH/SSL

- Наблюдение по протоколу DHCP
- Проверка 802.1x с динамическим распределением VLAN
- Списки ACL, основанные на IP и MAC-адресах

Дополнительные функции коммутатора

- Объединенный канал с поддержкой до 8 объединяемых каналов на устройство и до 8 портов на объединенный канал (IEEE 802.3ad)
- Поддержка LACP
- Поддержка больших кадров до 10 КБ
- Защита от «лавины» широковещательной передачи
- Зеркалирование (отражение трафика) портов

Управление устройством

- Веб-интерфейс управления
- Доступ к консоли с помощью Telnet
- Поддержка SNMPv1 и SNMP v2
- Поддержка 4 групп RMON
- Передача микропрограммы и файлов настройки по протоколу TFTP
- Два образа микропрограммы на плате
- Поддержка передачи и загрузки нескольких файлов настройки
- Статистика для контроля ошибок и оптимизации производительности
- Поддержка управления IP-адресов BootP/DHCP
- Функции удаленной регистрации Syslog
- Поддержка SNTP
- Трассировка Layer 3
- Клиент Telnet
- Клиент DNS

Функции системы

- Хост IPv6
- LLDP-MED
- Голосовая сеть VLAN
- Оптимизация iSCSI

Назад на страницу «Содержание»

Назад на страницу «Содержание»

Настройка сведений об устройстве

Руководство пользователя систем Dell™ PowerConnect™ 54xx

В этом разделе приведены все системные операции и общие сведения по настройке безопасности сети, портов, адресных таблиц, протокола GARP, сети VLAN, протокола STP, объединения портов и многоадресной поддержки.

Настройка безопасности сети

Устройство позволяет выполнять настройку безопасности сети с помощью списков управления доступом и заблокированных портов. Чтобы открыть страницу **Network Security** (Безопасность сети), выберите **Switch** (Коммутатор)→ **Network Security** (Безопасность сети).

Обзор безопасности сети

В этом разделе описаны функции безопасности сети.

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). Проверка подлинности портов включает в себя:

- **Удостоверения**. Определяет порт, для которого выполняется проверка подлинности перед разрешением доступа к системе.
- **Просители**. Указывает хост, подключенный к проверенному порту, запрашивающему доступ к службам системы.
- **Сервер проверки подлинности**. Указывает внешний сервер, например сервер RADIUS, который выполняет проверку подлинности от имени администратора, а также указывает, может ли пользователь получить доступ к службам системы.

Проверка подлинности на основе портов формирует два состояния доступа:

- **Controlled Access** (Управляемый доступ). Разрешает связь между пользователем и системой, если пользователь прошел проверку.
- **Uncontrolled Access** (Неконтролируемый доступ). Разрешает неконтролируемый обмен данными независимо от состояния порта.

Устройство в настоящее время поддерживает проверку подлинности на основе порта с помощью серверов RADIUS.

Проверка подлинности на базе MAC

Проверка подлинности на базе MAC является альтернативой для 802.1x, которая обеспечивает доступ по сети к устройствам (таким как принтеры или IP-телефоны), которые не поддерживают формат запросов 802.1X. Проверка подлинности на базе MAC импользует MAC-адрес подключаемого устройства для предоставления или запрета доступа по сети.

Расширенная проверка подлинности на основе порта

Расширенная проверка подлинности на основе порта позволяет нескольким хостам подключаться к одному порту. Расширенная проверка подлинности на основе порта требует авторизации только одного хоста, чтобы доступ к системе имели все хосты. Если порт не авторизован, то доступ всех присоединенных к нему хостов к сети закрыт.

Расширенная проверка подлинности на основе порта позволяет использовать проверку подлинности по имени пользователя. Определенные группы VLAN в устройстве являются всегда доступными, даже если порты, подключенные к группе VLAN, не прошли авторизацию. Например, для передачи голоса по IP не требуется проверка подлинности, а для трафика передачи данных требуется. Можно определить группы VLAN, для которых не требуется проверка подлинности. Группы VLAN, не прошедшие проверку, доступны пользователям даже если порты, соединенные с VLAN определены как авторизованные.

Расширенная проверка подлинности на основе порта реализована в следующих режимах:

- **Режим одиночного хоста**. Включает только авторизованный хост и обеспечивает один сеанс доступа к порту.
- **Многохостовый режим**. Обеспечивает один сеанс доступа нескольких хостов к одному порту.Требуется авторизация только одного хоста, чтобы доступ к сети имели все хосты. В случае неудачной проверки подлинности хоста или появления сообщения выхода EAPOL доступ запрещается для всех подключенных клиентов.
- **Многосеансовый режим**. Обеспечивает многосеансовый доступ авторизованного хоста к порту.

- **Гостевая сеть VLAN**. Предоставляет ограниченный доступ к сети для неавторизованных портов. Если для порта запрещается доступ к сети через авторизацию на основе порта, а гостевая сеть VLAN включена, порт получает ограниченный доступ к сети. Например, администратор сети может использовать гостевые сети VLAN, чтобы запретить доступ к сети через проверку подлинности на основе порта, но разрешить доступ к Интернету для неавторизованных пользователей.

Настройка проверки подлинности на основе порта

Страница **Port Based Authentication** (Проверка подлинности на основе порта) содержит поля для настройки проверки подлинности на основе порта и для включения гостевых сетей VLAN. 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)

- **Port Based Authentication State** (Состояние проверки подлинности на основе порта). Позволяет выполнять проверку подлинности на основе порта для устройства. Ниже указаны 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. Ниже указаны возможные значения.
  - **None** (Нет). Не используется никакой метод проверки подлинности на основе порта.
  - **RADIUS**. Проверка подлинности на основе порта выполняется на сервере RADIUS.
  - **RADIUS, None** (RADIUS, Нет). Проверка подлинности на основе порта сначала выполняется на сервере RADIUS. Если проверка подлинности порта не выполняется, то не используется никакой метод проверки подлинности, и сеанс разрешается.
- **Guest VLAN** (Гостевая сеть VLAN). Определяет, включена ли гостевая сеть VLAN для устройства. Возможные значения поля таковы:
  - **Enable** (Включено). Включение гостевой сети VLAN для неавторизованных портов. Если включен параметр гостевой сети VLAN, неавторизованный порт автоматически присоединяется к сети VLAN, выбранной в поле со списком сетей VLAN.
  - **Disable** (Выключено). Отключена проверка подлинности на основе порта для устройства. Это значение по умолчанию.
- **VLAN List** (Список VLAN). Когда включен параметр гостевой сети, в этом поле указывается информация о том, к какой сети VLAN принадлежит гость.
- **Interface** (Интерфейс). Содержит список интерфейсов.
- **User Name** (Имя пользователя). Имя пользователя, настроенное на сервере RADIUS.
- **Admin Interface Control** (Управление интерфейсом). Определяет состояние авторизации порта. Ниже указаны возможные значения.
  - **Authorized** (Авторизирован). Устанавливает интерфейс в авторизированное состояние (трафик разрешен).
  - **Unauthorized** (Не авторизирован). Устанавливает интерфейс в неавторизированное состояние (трафик запрещен).
  - **Auto** (Автоматически). Состояние авторизации устанавливается методом авторизации.
- **Current Interface Control** (Текущее управление интерфейсом). Определяет текущее состояние авторизации настроенного порта.
- **Authentication Type** (Тип авторизации). Определяет тип авторизации порта. Ниже указаны возможные значения.

- **802.1x Only** (Только 802.1x). Устанавливает тип авторизации только на основе 802.1x.
- **MAC Only** (Только MAC). Устанавливает тип авторизации только на основе MAC.
- **802.1x & MAC**. Устанавливает типы авторизации 802.1x и MAC.

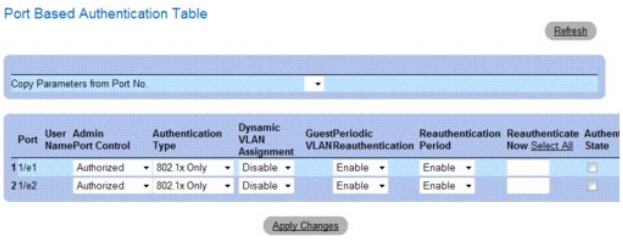
- **Dynamic VLAN Assignment** (Динамическое распределение VLAN). Показывает, включен ли режим динамического распределения VLAN для этого порта. Эта функция позволяет сетевым администраторам автоматически распределять пользователей сетям VLAN при авторизации на сервере RADIUS. После авторизации пользователя сервером RADIUS, он автоматически подключается к сети VLAN, конфигурация которой произведена сервером RADIUS.
  - При включении функции DVA необходимо отключить функции Port Lock и Port Monitor.
  - Динамическое распределение VLAN (DVA) может работать только при условии того, что выполнено конфигурирование сервера RADIUS, включена функция авторизации порта и установлен режим авторизации 802.1x для многосеансового доступа.
  - Если ответное сообщение сервера RADIUS не содержит названия сети VLAN пользователя, значит, пользователю отказано в доступе.
  - Авторизованные порты будут добавлены к VLAN пользователя как непомеченные.
  - Неавторизованные порты остаются членами VLAN и Гостевой VLAN. Конфигурация статической VLAN не была применена к этому порту.
  - В списке, (см. ниже), указаны сети VLAN, которые не подлежат обработке функцией DVA: Неавторизованная VLAN, Динамическая VLAN, созданная GVRP, Голосовая VLAN, VLAN, созданная по умолчанию и Гостевая VLAN.
  - Сетевые администраторы могут удалять VLAN пользователя, пока он зарегистрирован в системе. Пользователь авторизуется при следующей повторной авторизации, если VLAN этого пользователя будет создана заново или на сервере RADIUS будет сконфигурирована новая VLAN.
- **Guest VLAN** (Гостевая сеть). Определяет, включена ли гостевая сеть VLAN для интерфейса.
- **Periodic Reauthentication** (Периодическое повторение проверки подлинности). Для выбранного порта,если это возможно, выполняется периодическая проверка подлинности. Периодповторной проверки подлинности определяется полем **Reauthentication Period (300-4294967295)**.
- **Reauthentication Period (300-4294967295)** (Период повторения проверки подлинности). Определяет время, по истечению которого для выбранного порта будет выполнена повторная проверка подлинности. Значение этого поля указывается в секундах. Значение по умолчанию: 3600 секунд.
- **Reauthenticate Now** (Немедленная повторная проверка подлинности). Выполняет повторную проверку подлинности выбранного порта.
- **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 по умолчанию: 30 секунд.
- **Quiet Period (0-65535)** (Период молчания). Число секунд, в течение которых устройство остается в состоянии молчания после обмена данными в ходе неудачной проверки подлинности. Возможные значения поля: 0-65535. Значение по умолчанию: 60 секунд.
- **Supplicant Timeout (1-65535)** (Тайм-аут просителя). Время до повторной отправки запросов EAP пользователю. Значение этого поля указывается в секундах. Значение по умолчанию: 30 секунд.
- **Max EAP Requests (1-10)** (Максимальное число запросов EAP). Общее число отправляемых запросов EAP. Если ответ не получен по истечении указанного периода, процесс проверки подлинности начинается заново. Значение по умолчанию: 2 попытки.

Отображение таблицы проверки подлинности на основе порта

1. Откройте страницу **Port Based Authentication** (Проверка подлинности на основе порта).
2. Нажмите кнопку **Show All** (Показать все).

Откроется страница **Port Based Authentication Table** (Таблица проверки подлинности на основе порта).

Рис. 7-2. Таблица Port Based Authentication Table (Таблица проверки подлинности на основе порта)



Termination Cause (Причина завершения). Причина, по которой была завершена проверка подлинности на основе порта.

Copy To Checkbox (Флажок 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. Выберите интерфейс в таблице **Port Based Authentication Table** (Таблица проверки подлинности на основе порта).
5. Установите флажок **Copy to** (Копировать в), чтобы определить интерфейс, для которого будут скопированы параметры проверки подлинности на основе порта.
6. 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).

Команда консоли	**Описание**
aaa authentication dot1x default *метод1* [*метод2*.]	Указывает один или несколько методов проверки подлинности, авторизации и учета (AAA), используемые на интерфейсах IEEE 802.1X.
dot1x auth-not-req	Обеспечивает доступ к VLAN авторизованных устройств.
dot1x guest-vlan	Определяет Гостевую VLAN.
dot1x guest vlan enable	Обеспечивает интерфейсный доступ авторизованных пользователей к Гостевой VLAN.
dot1x mac-authentication	Выполняет проверку подлинности на основе MAC-адреса станции (проверка подлинности на основе MAC).
dot1x max-req *число*	Устанавливает максимальное число попыток отправки запросов EAP клиенту перед возобновлением процесса проверки подлинности.
dot1x re-authenticate [**ethernet** *интерфейс*]	Инициализирует вручную повторную проверку подлинности всех портов, поддерживающих 802.1X или указанного порта, поддерживающего 802.1X.
dot1x re- authentication	Включает периодические повторные проверки подлинности клиента.
dot1x timeout quiet-period *секунды*	Устанавливает число секунд, в течение которых устройство остается в состоянии молчания после обмена данными в ходе неудачной проверки подлинности.
dot1x timeout re-authperiod *секунды*	Устанавливает число секунд между попытками повторной проверки подлинности.
dot1x timeout server-timeout *секунды*	Устанавливает время повторной передачи пакетов на сервер проверки подлинности.
dot1x timeout supp-timeout *секунды*	Устанавливает время для повторной отправки кадра запроса EAP клиенту.
dot1x timeout tx- period *секунды*	Устанавливает число секунд, в течение которых устройство ожидает ответа на запрос EAP от клиента перед повторной отправкой запроса.
dot1x traps mac-authentication failure	Посылает сигнал прерывания при отрицательном результате проверки подлинности MAC-адреса (при проверке подлинности на основе MAC-адресов).
dot1x radius-attribues VLan	Обеспечивает подключение пользователя к сети VLAN, в зависимости от типа пользователя.
show dot1x [**ethernet** *интерфейс*]	Отображает состояние 802.1X для устройства или указанного интерфейса.
show dot1x advanced	Отображает расширенные функции 802.1X коммутатора указанного интерфейса.
show dot1x users [**username** *имя пользователя*]	Отображает пользователей 802.1X для устройства.

Далее приведен пример команд консоли.

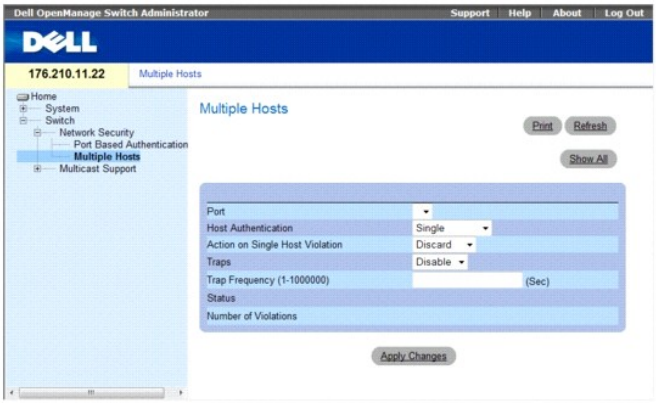
```
console> enable

Console# show dot1x
```

Interface	Admin Mode	Oper Mode	Reauth Control	Reauth Period	Username
---------	----------	----------	--------	------	--------
g1	Auto	Authorized	Ena	3600	Bob
g2	Auto	Authorized	Ena	3600	John
g3	Auto	Unauthorized	Ena	3600	Clark
g4	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)



- **Port** (Порт). Номер порта, для которого включен режим расширенной проверки подлинности на основе порта.
- **Host Authentication** (Проверка подлинности хоста). Определяет тип проверки подлинности хоста. Возможные значения полей:
  - **Single** (Режим одиночного хоста). Включает только авторизованный хост и обеспечивает один сеанс доступа к порту.
  - **Multiple Host** (Несколько хостов). Задействует один хост для авторизации нескольких хостов, для осуществления одного сеанса входа в систему. Этот параметр необходимо включить, чтобы отключить фильтр на входе или использовать защиту блокировки для выбранного порта.
  - **Multiple Session** (Несколько сеансов). Предоставляет многосеансовый доступ одного авторизованного хоста к системе. Это значение по умолчанию.
- **Action on Single Host Violation** (Действие при нарушении доступа одного хоста). Определяет действие, которое необходимо применять для пакетов, поступающих в режиме одного хоста от хоста, MAC-адрес которого отличается от MAC-адреса клиента (просителя). Поле **Action on Single Host Violation** (Действие при нарушении доступа одного хоста) можно определить только в том случае, если для поля **Multiple Hosts** (Несколько хостов) указано значение **Disable** (Отключить). Ниже указаны возможные значения:
  - **Forward** (Переслать). Пересылает пакет от неизвестного источника, но MAC-адреса не распознаются.
  - **Discard** (Отвергнуть). Отбрасывает пакеты от любого неизвестного источника. Это значение по умолчанию.
  - **Shutdown** (Завершить работу). Отбрасывает пакеты от любого неизвестного источника и блокирует порт. Порт будет заблокирован, пока не будет выполнена его активизация или перезагружено устройство.
- **Traps** (Системные прерывания). Включает или отключает отправку системных прерываний на хост в случае нарушения доступа.
- **Trap Frequency (1-1000000) (Sec)** (Частота системных прерываний (сек)). Определяет временной интервал между отправками системных прерываний на хост. Поле **Trap Frequency (1-1000000)** (Частота системных прерываний) можно определить только в том случае, если для поля **Multiple Hosts** (Несколько хостов) указано значение **Disable** (Отключить). Значение по умолчанию: 10 секунд.
- **Status** (Состояние). Состояние хоста. Ниже указаны возможные значения.
  - **Unauthorized** (Не проверяются). Клиенты (просители) имеют полный доступ к порту.
  - **Authorized** (Проверяются). Клиенты (просители) имеют ограниченный доступ к порту.
- **Number of Violations** (Число нарушений). Число пакетов, поступивших на интерфейс в режиме одного хоста от хоста, MAC-адрес которого отличается от MAC-адреса клиента (просителя).

Отображение таблицы Multiple Hosts Table (Таблица нескольких хостов)

1. Откройте страницу **Multiple Hosts** (Несколько хостов).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется таблица **Multiple Hosts Table** (Таблица нескольких хостов) opens.

Рис. 7-4. Страница Multiple Hosts Table (Таблица нескольких хостов)

Включение нескольких хостов с использованием команд консоли

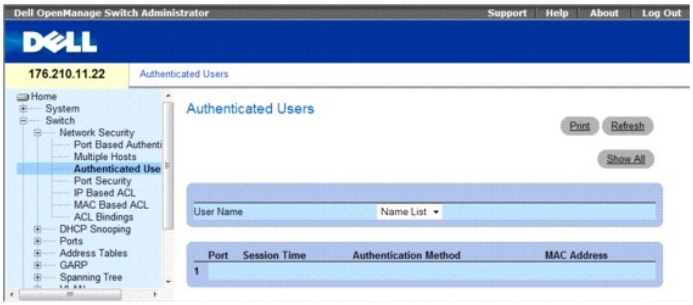
В следующей таблице приведены команды консоли для включения расширенной проверки подлинности на основе порта, соответствующие полям на странице **Multiple Hosts** (Несколько хостов).

Команда консоли	**Описание**
dot1x multiple-hosts	Разрешает наличие нескольких хостов (клиентов) на проверяемом порту 802.1X, для которых в команде настройки интерфейса dot1x port-control установлено значение auto.
dot1x single-host-violation {**forward** | **discard** | **discard-shutdow**n} [**trap** секунды]	Настраивает действие, которое необходимо выполнить, когда станция, MAC-адрес которой отличается от MAC-адреса клиента (просителя), осуществляет попытку доступа к интерфейсу.

Проверка подлинности пользователей

Страница **Authenticated Users** (Проверяемые пользователи) отображает список доступа пользователей к портам. Этот список определяется на странице **Add User Name** (Добавление имени пользователя). Чтобы открыть страницу **Authenticated Users** (Проверка подлинности пользователей), выберите **Switch** (Коммутатор)→ **Network Security** (Безопасность сети)→ **Authenticated Users** (Пользователи, подлинность которых прошла проверку).

Рис. 7-5. Страница Authenticated Users (Проверка подлинности пользователей)



- **User Name** (Имя пользователя). Список пользователей, авторизированных с использованием сервера RADIUS.
- **Port** (Порт). Номера портов, используемые для проверки подлинности - для каждого имени пользователя.
- **Session Time** (Время сеанса). Время с момента входа пользователя на устройство. Формат поля **дни:часы:минуты:секунды**, например 3 дня: 2 часа: 4 минуты: 39 секунд.
- **Authentication Method** (Метод проверки подлинности). Метод, использовавшийся при последней проверке подлинности. Ниже указаны возможные значения.
  - **Remote** (Удаленно). Проверка подлинности пользователя выполняется на удаленном сервере.
  - **None** (Нет). Проверка подлинности пользователя не выполнялась.
- **MAC Address** (MAC-адрес). MAC-адрес клиента (просителя).

Отображение таблицы проверки подлинности пользователей

1. Откройте страницу **Add User Name** (Добавление имени пользователя).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **Authenticated Users Table** (Таблица проверки подлинности пользователей).

Рис. 7-6. Страница Authenticated Users Table (Таблица проверки подлинности пользователей)

Проверка подлинности пользователей с помощью команд консоли

В следующей таблице приведены команды консоли для проверки подлинности пользователей, соответствующие полям на странице **Add User Name** (Добавление имени пользователя).

Команда консоли	**Описание**
show dot1x users [**username** *имя пользователя*]	Отображает пользователей 802.1X для устройства.

Далее приведен пример команд консоли.

```
console# show dot1x users

Username  Session Time  Last Auth  Auth Method  MAC Address        Interface
--------  ------------  ---------  -----------  -----------------  ---------
Bob       1d3h          58m        Remote       00:08:3b:79:87:87  g1
John      8h19m         2m         None         00:08:3b:89:31:27  g2
```

Настройка безопасности портов

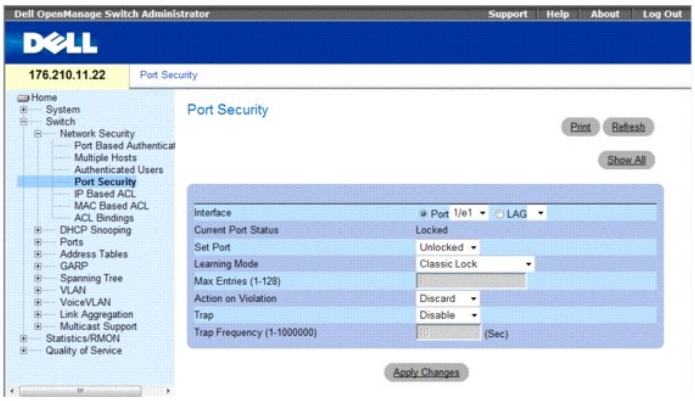
Безопасность сети можно повысить, если разрешить доступ к определенным портам только пользователям с определенными MAC-адресами. MAC-адреса определяются динамически в процессе подключения или настраиваются статически. Функция безопасности блокировки портов проверяет полученные пакеты и определяет, откуда 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
- 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 на странице **Port Parameters** (Параметры портов), см. раздел Определение параметров 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). Выбранный тип интерфейса, на котором включена блокировка порта.

- **Port** (Порт). Выбранный тип интерфейса - порт.
- **LAG**. Выбранный тип интерфейса - LAG.

- **Current Port Status** (Текущее состояние порта). Определяет текущее состояние порта.
- **Set Port** (Установить порт). Порт заблокирован или разблокирован. Ниже указаны возможные значения.
  - **Unlocked** (Разблокирован). Порт разблокирован. Это значение по умолчанию.
  - **Locked** (Заблокирован). Порт заблокирован.
- **Learning Mode** (Режим распознавания). Режим распознавания порта. Ниже указаны возможные значения.
  - **Classic Lock** (Классическая блокировка). Порт не распознает новые IP-адреса. Компьютер с другим адресом нельзя подключить к сети через порт.
  - **Limited Dynamic Lock** (Ограниченная динамическая блокировка). Порт распознает ограниченное число новых IP-портов, а затем будет заблокирован.
- **Max Entries (1-128)** (Максимальное число записей). Количество новых IP-адресов, которые распознает порт до моменте блокировки, если для параметра «Learning Mode» (Режим распознавания) установлено значение «Limited Dynamic Lock» (Ограниченная динамическая блокировка).
  - **Action on Violation** (Действие при нарушении). Действие, которое должно применяться к пакетам, поступающим на заблокированный порт. Ниже указаны возможные значения.
  - **Forward** (Переслать). Пересылает пакет от неизвестного источника, но MAC-адреса не распознаются.
  - **Discard (Отвергнуть)**. Отбрасывает пакеты от любого неизвестного источника. Это значение по умолчанию.
  - **Shutdown** (Завершить работу). Отбрасывает пакеты от любого неизвестного источника и блокирует порт. Порт будет заблокирован, пока не будет выполнена его активизация или перезагружено устройство.
- **Trap** (Системное прерывание). Включает системные прерывания, отправляемые при получении пакета на заблокированный порт.
- **Trap Frequency (1-1000000)** (Частота системных прерываний). Время в секундах, которое проходит между системными прерываниями. Это поле относится только к заблокированным портам. Значение по умолчанию: 10 секунд.

Определение заблокированного порта

1. Откройте страницу **Port Security** (Безопасность портов).
2. Выберите тип и номер интерфейса.
3. Определите поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Заблокированный порт будет добавлен в **Port Security Table** (Таблицу безопасности портов), а устройство обновлено.

Отображение таблицы заблокированных портов

1. Откройте страницу **Port Security** (Безопасность портов).
2. Нажмите кнопку **Show All (Показать все).**

   Откроется страница **Port Security Table (Таблица безопасности портов)**.

   Заблокированные порты также можно определить в **Locked Ports Table** (Таблице заблокированных портов) и на странице **Port Security** (Безопасность порта).

Рис. 7-8. Страница Port Security Table (Таблица безопасности портов)

Настройка безопасности заблокированных портов с помощью команд консоли

В следующей таблице приведены команды консоли для настройки функции безопасности заблокированных портов, как отображается на странице **Port Security** (Безопасность портов).

Команда консоли	**Описание**
Завершение работы	Отключает интерфейсы.
set interface active {**ethernet** *интерфейс* | **port-channel** *номер_канала_порта*}	Вновь активизирует интерфейс, отключенный по причинам безопасности порта.
port security [**forward** | **discard** | **discard-shutdown**] [**trap** *секунды*]	Блокирует функцию опознавания новых адресов для интерфейса.
show ports security {**ethernet** *интерфейс* | **port-channel** *номер_канала_порта*}	Выводит состояние блокировки для порта.

Далее приведен пример команд консоли.

Console # **show ports security**

Port	Status	Action	Trap	Frequency	Counter
-----	-------	-------	-------	---------	--------
g7	Unlocked	Discard	Enable	100	88
g8	Unlocked	Discard, Shutdown	Disable		
g3	Unlocked	-	-	-	-

Обзор списка ACL

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

Определение списков ACL, основанных на IP-адресах

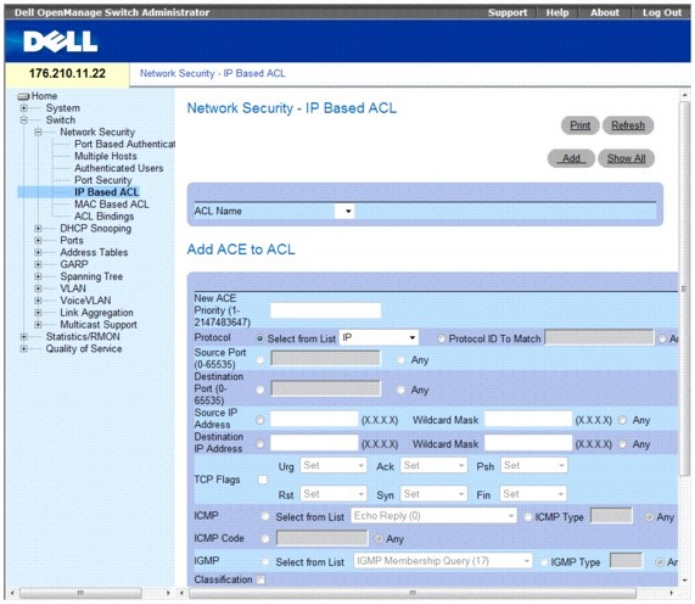
Списки управления доступом (ACL), состоящие из записей управления доступом (ACE), позволяют сетевым администраторам определять классификационные действия и правила для определенных входных портов. Пакеты, поступающие на входной порт с активным списком ACL, пропускаются или отбрасываются и входной порт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

Например, администратор сети определяет правило ACL, которое устанавливает, что порт с номером 20 может получить пакеты TCP, но если будет получен пакет UDP, этот пакет будет отброшен.

Списки ACL состоят из элементов управления доступом (ACE), которые создают фильтры, определяющие классификации трафиков. Каждая запись ACE является правилом; доступно 1024 правила. Правила предназначены не только для конфигурации пользователя, они также используются для протоколов iSCSI и PVE, поэтому не все 1024 правила доступны для записей ACE. Предполагается, что для пользователя доступно по крайней мере 600 правил.

Чтобы определить ACL на основе IP, выберите **Switch** (Коммутатор)→ **Network Security** (Безопасность сети)→ **IP Based ACL** (ACL на основе IP).

Рис. 7-9. Network Security - IP Based ACL (Безопасность сети - ACL, основанный на MAC-адресах)



- **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. Ниже указаны возможные значения.
  - **IP**. Протокол Интернета (IP). Определяет формат пакетов и способ назначения адресов для них. IP назначает пакетам адреса и пересылает пакеты на нужный порт.
  - **ICMP**. Протокол управляющих сообщений Интернета (Internet Control Message Protocol (ICMP)). Протокол ICMP позволяет шлюзу или хосту назначения устанавливать связь с хостом, являющимся источником данных, например, для передачи отчета об ошибке обработки.
  - **IGMP**. Протокол управления группами Интернета (Internet Group Management Protocol (IGMP)). Позволяет хостам уведомлять локальный коммутатор или маршрутизатор о том, что они могут получить передачи, назначенные для определенной многоадресной группы.
  - **TCP**. Протокол управления передачей (Transmission Control Protocol (TCP)). Обеспечивает двум хостам возможность установки связи и обмена потоками данных. TCP гарантирует доставку пакета, а также передачу и прием пакетов в порядке их отправки.
  - **EGP**. Протокол внешнего шлюза (Exterior Gateway Protocol (EGP)). Разрешает обмен данными маршрутизации между двумя соседними хостами шлюза в сети автономных систем.
  - **IGP**. Протокол внутреннего шлюза (Interior Gateway Protocol (IGP)). Позволяет выполнять обмен данными маршрутизации между шлюзами в автономной сети.
  - **UDP**. Протокол пользовательских датаграмм (User Datagram Protocol (UDP)). Протокол связи, который передает пакеты, но не гарантирует их доставку.
  - **HMP**. Протокол отображения хоста (Host Mapping Protocol (HMP)). Собирает сетевую информацию с различных сетевых хостов. HMP контролирует разброс хостов в Интернете, а также хосты в отдельной сети.
  - **RDP**. Протокол удаленного рабочего стола (Remote Desktop Protocol (RDP)). Позволяет клиенту устанавливать связь с сервером терминала в сети.
  - **IDPR**. Сопоставляет пакет с протоколом IDPR.
  - **IPV6**. Сопоставляет пакет с протоколом IPV6.
  - **IPV6 ROUTE**. Сопоставляет пакет с протоколом маршрутизации IPV6.
  - **IPV6 FRAG**. Сопоставляет пакет с протоколом IPV6 FRAG.
  - **IDRP**. Сопоставляет пакет с протоколом IDRP (Inter-Domain Routing Protocol).
  - **RVSP**. Сопоставляет пакет с протоколом RSVP (ReSerVation Protocol).
  - **AH**. Заголовок проверки подлинности (AH). Обеспечивает проверку подлинности хоста, являющегося источником данных, и целостность данных.
  - **EIGRP**. Расширенный протокол маршрутизации внутреннего шлюза (Enhanced Interior Gateway Routing Protocol (EIGRP)). Обеспечивает быструю сходимость, поддержку масок подсети различной длины, а также поддерживает протоколы нескольких уровней сети.
  - **OSPF**. Протокол Open Shortest Path First (OSPF). Это протокол состояния канала, иерархический протокол внутреннего шлюза (IGP) для сетевого протокола туннелирования канального уровня (L2TP), дополнение к протоколу PPP, который используется поставщиками услуг Интернета для работы виртуальных частных сетей (VPN).
  - **IPIP**. IP через IP (IPIP). Формирует пакеты IP для создания туннелей между двумя маршрутизаторами. В результате туннель IPIP отображается как один интерефейс, а не как несколько отдельных интерфейсов. IPIP обеспечивает выход в Интернет в интрасетях с туннельным доступом и является альтернативой маршрутизации от источника.
  - **PIM**. Сопоставляет пакет с протокольно независимой многоадресной рассылкой (PIM).
  - **L2TP**. Сопоставляет пакет с протоколом Интернета (L2IP).

- **ISIS**. Промежуточная система - промежуточная система (ISIS). Распределяет информацию маршрутизации IP через единую автономную систему в сетях IP
- **Protocol ID To Match** (Идентификатор протокола для сопоставления). Добавляет определенные пользователем протоколы, пакеты которых будут сопоставляться с записью ACE. У каждого протокола имеется определенный уникальный номер. Возможные значения поля: 0-255.
- **Any** (Любой). Сопоставляет протокол с любым другим протоколом.

- **Source Port** (Порт-источник). Исходный порт TCP/UDP. Выберите значение **Any** (Любой), чтобы включить все порты.
- **Destination Port** (Порт-приемник). Порт назначения TCP/UDP. Выберите значение **Any** (Любой), чтобы включить все порты.
- **Source IP Address** (IP-адрес источника). Сопоставляет IP-адрес исходного порта, на который адресованы пакеты, с записью ACE. Маски ввода указывают, какие биты используются, а какие игнорируются. Маска ввода 0.0.0.0 указывает, что все биты важны.
- **Destination IP Address** (IP-адрес назначения). Сопоставляет IP-адрес порта назначения, на который адресованы пакеты, с записью ACE. Маски ввода указывают, какие биты используются, а какие игнорируются. Маска ввода 0.0.0.0 указывает, что все биты важны.
- **TCP Flags** (Флаги). Устанавливает указанный флаг TCP, который может быть запущен. Для использования флагов TCP установите флажок **TCP Flag** (Флаг TCP), а затем выберите необходимые флаги.
- **ICMP**. Указывает тип сообщения ICMP для фильтрации пакетов ICMP. Можно выбрать из списка, ввести сообщение или выбрать значение **Any** (Любой) для всех типов сообщений ICMP. Это поле доступно, только, когда в поле **Protocol** (Протокол) выбран ICMP.
- **ICMP Code** (Код ICMP). Указывает код сообщения ICMP для фильтрации пакетов ICMP, которые могут фильтроваться по типу сообщения ICMP или по коду сообщения ICMP. Это поле доступно, только когда в поле **Protocol** (Протокол) выбран ICMP.
- **IGMP**. Пакеты IGMP могут фильтроваться по типу сообщения IGMP. Можно выбрать из списка, ввести сообщение или выбрать значение **Any** (Любой) для всех типов сообщений IGMP. Это поле доступно, только, когда в поле **Protocol** (Протокол) выбран IGMP.
- **Classification Mach DSCP** (Соответствие классификации DSCP). Сопоставляет значение пакета DSCP с записью ACL. При сравнении пакетов с записями ACL используется значение DSCP или значение приоритета пакета IP. Возможные значения поля: 0-63.
- **Match IP Precedence** (Соответствие приоритета IP). Обозначает сопоставление приоритета IP-пакетов со значением приоритета IP-пакетов. Приоритет IP-пакетов делает возможным маркировку кадров, превышающих пороговое значение CIR. В перегруженной сети кадры с высокой скоростью обработки данных не учитываются в отличие от кадров с низкой скоростью обработки данных.
- **Action** (Действие). Указывает операцию передачи для ACL. Ниже указаны возможные значения.
  - **Permit** (Разрешить). Пересылает пакеты, отвечающие критериям ACL.
  - **Deny** (Запретить). Отбрасывает пакеты, отвечающие критериям ACL.
  - **Shutdown** (Завершение работы). Отбрасывает пакет, отвечающий критериям ACL, и отключает порт, на который он был адресован.

Добавление записей ACE к спискам ACL, основанных на IP-адресах

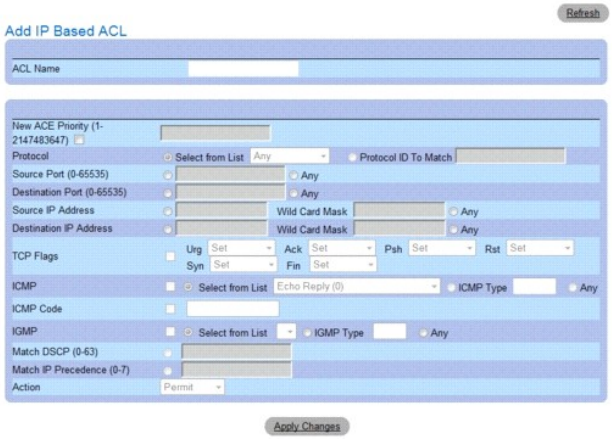
1. Откройте страницу **Network Security - IP Based ACL** (Безопасность сети - ACL на основе IP-адресов).
2. Выберите ACL.
3. Измените соответствующие поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Добавление списков ACL, основанных на IP-адресах

1. Откройте страницу **IP Based ACL** (ACL на основе IP-адресов):
2. Нажмите кнопку **Add** (Добавить).

   Откроется страница Network Security - IP Based ACL (Безопасность сети - ACL, основанный на IP-адресах).

   Рис. 7-10. Add IP Based ACL (Добавление ACL, основанного на MAC-адресах).



3. Определите соответствующие поля.

4. Нажмите кнопку **Apply Changes** (Применить изменения). Протокол, основанный на IP-адресах, будет определен, а устройство обновлено.

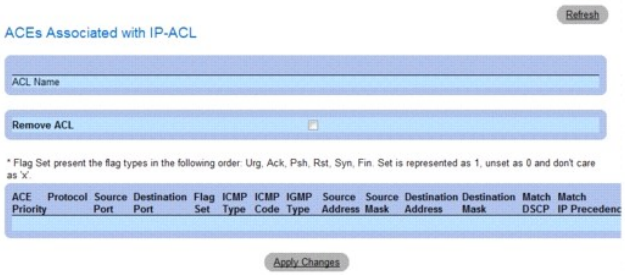
Отображение записей ACE, связанных со списками ACL на основе IP-адресов

1. Откройте страницу **Network Security - IP Based ACL** (Безопасность сети - ACL, основанный на IP-адресах).

2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **ACEs Associated with IP-ACL** (Записи ACE, связанные с ACL, основанным на IP-адресах) .

Рис. 7-11. Страница ACEs Associated with IP-ACL (Записи ACE, связанные с ACL, основанным на IP-адресах)



Удаление списка ACL, основанного на IP-адресах

1. Откройте страницу **Network Security - IP Based ACL** (Безопасность сети - ACL, основанный на IP-адресах).

2. Нажмите кнопку **Show All** (Показать все). Откроется страница **ACEs Associated with IP-ACL Table** (Таблица с записями ACE, связанными с ACL, основанным на IP-адресах).

3. Установите флажок **Remove ACL** (Удалить ACL).

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

Удаление записи ACE, основанной на IP-адресах

1. Откройте страницу **Network Security - IP Based ACL** (Безопасность сети - ACL, основанный на IP-адресах).

2. Нажмите кнопку **Show All** (Показать все). **Откроется страница ACEs Associated with IP-ACL Table** (Таблица с записями ACE, связанными с ACL, основанным на IP-адресах).

3. Установите флажок **Remove** (Удалить) рядом с записью ACE.

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

Настройка списков ACL, основанных на IP-адресах, с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для настройки списков ACL, основанных на **IP-адресах**.

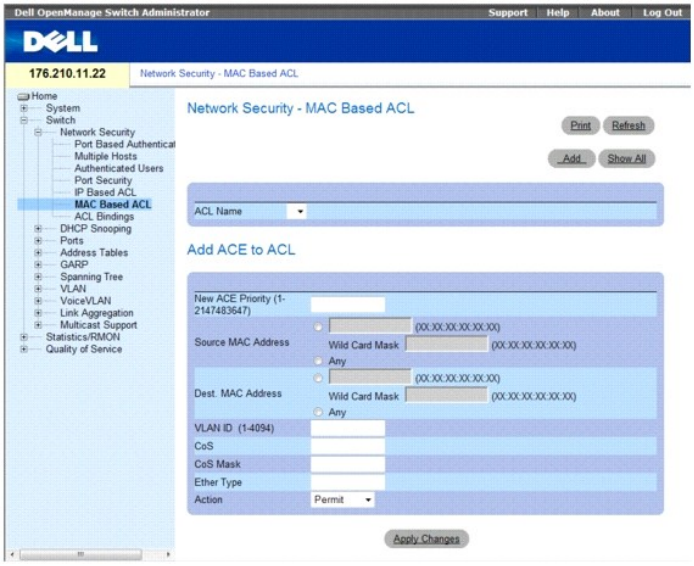
Команда консоли	Описание
ip access-list *имя-списка-доступа* **no ip access-list** *имя-списка-доступа*	Чтобы определить список доступа IPv4 и перейти в режим настройки списка доступа IPv4, используйте команду ipv4 access-list в режиме Global Configuration. Для удаления списка доступа используйте форму no этой команды.
permit {**any** | *протокол*} {**any** | {*источник маска_ввода_источника*}} {**any** | {*destination маска_ввода_назначения*}} [**dscp** *номер* | **ip-precedence** *номер*] [**fragments**] **permit-icmp** {**any** | {*источник маска_ввода_источника*}} {**any** | {*назначение маска_ввода_назначения*}} {**any** | *тип_icmp*} {**any** | *код_icmp*} [**dscp** *номер* | **ip-precedence** *номер*] **permit-igmp** {**any** | {*источник маска_ввода_источника*}} {**any** | {*назначение маска_ввода_назначения*}} {**any** | *тип_igmp*} [**dscp** *номер* | **ip-precedence** *номер*] **permit-tcp** {**any** | { *источник маска_ввода_источника*}} {**any** | *порт_источника*} {**any** | { *назначение маска_ввода_назначения*}} {**any** | *порт_назначения*} [**dscp** *номер* | **ip-precedence** *номер*] [**flags** *список_флагов*] **permit-udp** {**any** | { *источник маска_ввода_источника*}} {**any** | *порт_источника*} {**any** | {*назначение маска_ввода_назначения*}} {**any** | *порт_назначения*} [**dscp** *номер* | **ip-precedence** *номер*]	Чтобы задать условия для прохождения пакета в именованный список доступа на основе IP-адресов, используйте команду разрешения в режиме настройки списка доступа.
deny [**disable-port**] {**any** | *протокол*} {**any** | {*источник маска_ввода_источника*}} {**any** | {*назначение маска_ввода_назначения*}} [**dscp** *номер* | **ip-precedence** *номер*] [**fragments**] **deny-icmp** [**disable-port**] {**any** | {*источник маска_ввода_источника*}} {**any** | {*назначение маска_ввода_назначения*}} {**any** | *тип_icmp*} {**any** | *код_icmp*} [**dscp** *номер* | **ip-precedence** *номер*] **deny-igmp** [**disable-port**] {**any** | {*источник маска_ввода_источника*}} {**any** | {*назначение маска_ввода_назначения*}} {**any** | *тип_igmp*} [**dscp** *номер* | **ip-precedence** *номер*] **deny-tcp** [**disable-port**] {**any** | { *источник маска_ввода_источника*}} {**any** | *порт_источника*} {**any** | { *назначение маска_ввода_назначения*}} {**any** | *порт_назначения*} [**dscp** *номер* | **ip-precedence** *номер*] [**flags** *список_флагов*] **deny-udp** [**disable-port**] {**any** | { *источник маска_ввода_источника*}} {**any** | *источник_порта*} {**any** | {*назначение маска_ввода_назначения*}} {**any** | *порт_назначения*} [**dscp** *номер* | **ip-precedence** *номер*]	Чтобы задать условия для прохождения пакета в именованный список доступа на основе IP-адресов, используйте команду запрета в режиме настройки списка доступа.

Определение списков управления доступом, основанных на MAC-адресах

На странице **Network Security - MAC Based ACL** (Безопасность сети - ACL, основанный на MAC-адресах) можно определить списки ACL, основанные на MAC-адресах. Запись ACE может быть добавлена только в том случае, если список ACL не связан с интерфейсом.

Чтобы определить списки ACL, основанные на MAC-адресах, выберите **Switch** (Коммутатор)→ **Network Security** (Безопасность сети)→ **MAC Based ACL** (ACL, основанный на MAC-адресах).

Рис. 7-12. Страница Network Security - MAC Based ACL (Безопасность сети - ACL, основанный на MAC-адресах).



- **ACL Name** (Имя ACL). Отображает определенные пользователем списки ACL, основанные на MAC-адресах.
- **New ACE Priority** (Новый приоритет ACE). Приоритет ACE, определяющий, какая запись ACE соответствует пакету на основе схемы первого совпадения. Возможные значения: 1-2147483647.
- **Source Address** (Адрес источника). Сопоставляет исходный MAC-адрес, на который адресованы пакеты, с записью ACE. Маски ввода указывают, какие биты используются, а какие игнорируются. Маска ввода 0.0.0.0 указывает, что все биты важны.
- **Destination Address** (Адрес назначения). Сопоставляет MAC-адрес назначения, на который адресованы пакеты, с записью ACE. Маски ввода указывают, какие биты используются, а какие игнорируются. Маска ввода 0.0.0.0 указывает, что все биты важны.
- **VLAN ID** (Идентификатор сети VLAN). Сопоставляет идентификатор сети VLAN пакета с записью ACE. Возможные значения этого поля от 1 до 4095.
- **CoS**. Указывает значения CoS, по которым фильтруются пакеты.
- **Cos Mask** (Маска Cos). Указывает маску CoS, по которой фильтруются пакеты.
- **Ethertype**. Указывает пакет Ethertype, по которому фильтруются пакеты.
- **Action** (Действие). Указывает операцию передачи для ACL. Возможные значения этого поля:
  - **Permit** (Разрешить). Пересылает пакеты, отвечающие критериям ACL.
  - **Deny** (Запретить). Отбрасывает пакеты, отвечающие критериям ACL.
  - **Shutdown** (Завершение работы). Отбрасывает пакет, отвечающий критериям ACL, и отключает порт, на который он был адресован.

Добавление записей ACE к спискам ACL, основанных на IP-адресах

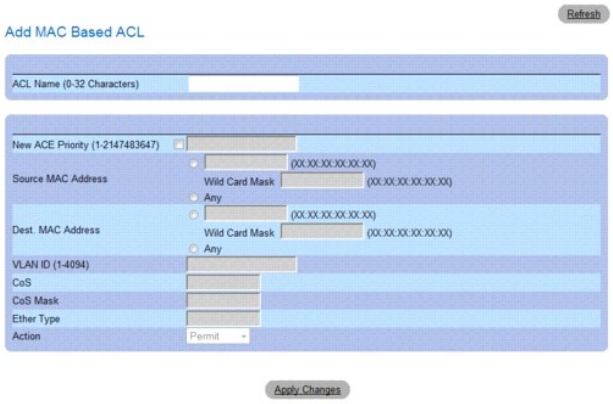
1. Откройте страницу **Network Security - MAC Based ACL** (Безопасность сети - ACL, основанный на MAC-адресах).
2. Выберите ACL.
3. Измените соответствующие поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Добавление списков ACL, основанных на MAC-адресах

1. Откройте страницу **MAC Based ACL** (ACL, основанный на MAC-адресах).
2. Нажмите кнопку **Add** (Добавить).

Откроется страница **Network Security - MAC Based ACL** (Безопасность сети - ACL, основанный на MAC-адресах) .

Рис. 7-13. Страница Add Mac Based ACL (Добавление ACL, основанного на MAC-адресах)

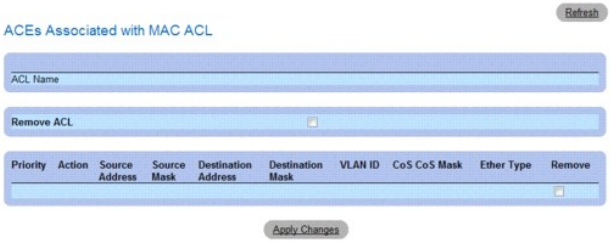


3. Определите соответствующие поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения). Протокол, основанный на MAC-адресах, будет определен, а устройство обновлено.

Отображение записей ACE, связанных со списками ACL на основе MAC-адресов

1. Откройте страницу **Network Security - MAC Based ACL** (Безопасность сети - ACL, основанный на MAC-адресах).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **ACEs Associated with MAC Based ACL** (Таблица с записями ACE, связанными с ACL, основанным на MAC-адресах) .



Удаление списка ACL, основанного на MAC-адресах

1. Откройте страницу **Network Security - MAC Based ACL** (Безопасность сети - ACL, основанный на MAC-адресах).
2. Нажмите кнопку **Show All** (Показать все). Откроется страница **ACEs Associated with MAC-ACL Table** (Таблица с записями ACE, связанными с ACL, основанным на MAC-адресах).
3. Установите флажок **Remove ACL** (Удалить ACL).
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Удаление записи ACE, основанной на MAC-адресах

1. Откройте страницу **Network Security - MAC Based ACL** (Безопасность сети - ACL, основанный на MAC-адресах).
2. Нажмите кнопку **Show All** (Показать все). Откроется страница **ACEs Associated with MAC-ACL Table** (Таблица с записями ACE, связанными с ACL, основанным на MAC-адресах).
3. Установите флажок **Remove** (Удалить) рядом с записью ACE.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Настройка списков ACL, основанных на MAC-адресах, с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для настройки списков ACL, основанных на MAC-адресах.

Команда консоли	Описание
mac access-list *имя-списка-доступа* **no mac access-list** *имя-списка-доступа*	Чтобы определить список доступа Layer 2 и перейти в режим настройки списка доступа MAC, используйте команду mac access-list в режиме Global Configuration. Для удаления списка доступа используйте форму no этой команды.
permit {**any** | {*источник маска_ввода_источника*} {**any** | { *назначение маска_ввода_назначения*}} [**vlan** *идентификатор-vlan*] [**cos** *cos маска_ввода_cos*] [**ethtype** *тип-eth*] [**inner-vlan** *идентификатор-vlan*]	Чтобы задать условия разрешения для списка доступа на основе MAC-адресов, используйте команду разрешения в режиме настройки списка доступа на основе MAC-адресов.
deny [**disable-port**] {**any** | {*источник маска_ввода_источника*} {**any** | { *назначение маска_ввода_назначения*}} [**vlan** *идентификатор-vlan*] [**cos** *cos маска_ввода_cos*] [**ethtype** *тип-eth*] [**inner-vlan** *идентификатор-vlan*]	Чтобы задать условия запрета для списка доступа на основе MAC-адресов, используйте команду запрета в режиме настройки списка доступа на основе MAC-адресов.

Определение привязки списка ACL

Когда выполняется связь списка ACL с интерфейсом, все правила, определенные в записях ACE, применяются для выбранного интерфейса. Каждый раз, когда список ACL назначается для порта или группы LAG, потоки с этого входящего интерфейса, которые не соответствуют списку ACL, сравниваются с правилом по умолчанию (опускание несоответствующих пакетов).

Для привязки списков ACL к интерфейсам выполните следующие действия.

1. Откройте страницу **Network Security - ACL Bindings** (Безопасность сети - Привязки ACL), выберите **Switch** (Коммутатор)→ **Network Security** (Безопасность сети)→ **ACL Binding**s (Привязки ACL).

   Рис. 7-14. Страница Network Security - ACL Binding (Безопасность сети - Привязки ACL)

2. В поле **Select an ACL** (Выбрать ACL) выберите значение IP Based (ACL на основе IP-адресов) или MAC Based (ACL на основе MAC-адресов).

3. В поле **Bind ACL to an Interface** (Привязать список ACL к интерфейсу) выберите порт или LAG.

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

   Список ACL будет привязан к интерфейсу.

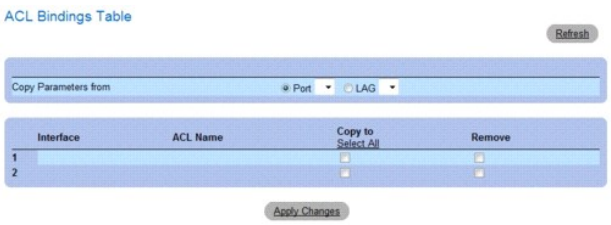
Отображение таблицы привязки ACL

1. Откройте страницу **Network Security - ACL Binding** (Безопасность сети - Привязки ACL).

2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **ACL Bindings Table** (Таблица привязки ACL).

   Рис. 7-15. Страница ACL Bindings Table (Таблица привязки ACL)



Копирование параметров ACL на другие интерфейсы

1. Откройте страницу **Network Security - ACL Binding** (Безопасность сети - Привязки ACL).
2. Нажмите кнопку **Show All** (Показать все). Откроется страница **ACL Bindings Table** (Таблица привязки ACL).
3. В поле **Copy Parameters from** (Копировать параметры из) выберите порт или группу LAG, откуда необходимо скопировать параметры ACL.
4. В таблице установите флажок **Copy to** (Копировать в) для каждой записи, для которой требуется скопировать параметры.
5. Нажмите кнопку **Apply Changes** (Применить изменения).

Удаление привязок ACL

1. Откройте страницу **Network Security - ACL Binding** (Безопасность сети - Привязки ACL).
2. Нажмите кнопку **Show All** (Показать все). Откроется страница **ACL Bindings Table** (Таблица привязки ACL).
3. В таблице установите флажок **Remove** (Удалить) для каждой привязки, которую требуется удалить.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Настройка привязок ACL с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для настройки привязки ACL.

Команда консоли	**Описание**
service-acl input *имя-acl* **no service-acl input**	Для управления доступом к интерфейсу используйте команду service-acl в режиме настройки интерфейса. Для удаления функции управления доступом используйте форму no этой команды.
show access-lists [имя]	Используйте команду show access-lists в режиме Privileged EXEC для отображения списков управления доступом (ACL), настроенных на коммутаторе.

Далее приведен пример нескольких команд консоли.

```
Switch# show access-lists

IP access list ACL1

permit 234 172.30.40.1 0.0.0.0 any

permit 234 172.30.8.8 0.0.0.0 any
```

Настройка наблюдения по протоколу DHCP

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

С помощью наблюдения по протоколу DHCP фильтруются ненадежные сообщения. Наблюдение по протоколу DHCP создает и поддерживает таблицу

наблюдения по протоколу DHCP, в которой содержится информация, полученная от ненадежных пакетов. Если пакет поступает с интерфейса, находящегося за пределами сети или отсутствующего в правилах сетевого брандмауэра, такие интерфейсы считаются ненадежными. На доверенные интерфейсы пакеты поступают только из сети или от сетевого брандмауэра.

В таблице наблюдения по протоколу DHCP отображаются MAC-адрес, IP-адрес, время использования и идентификатор VLAN для ненадежных интерфейсов, а также информация об интерфейсах.

Раздел протокола DHCP включает следующие темы.

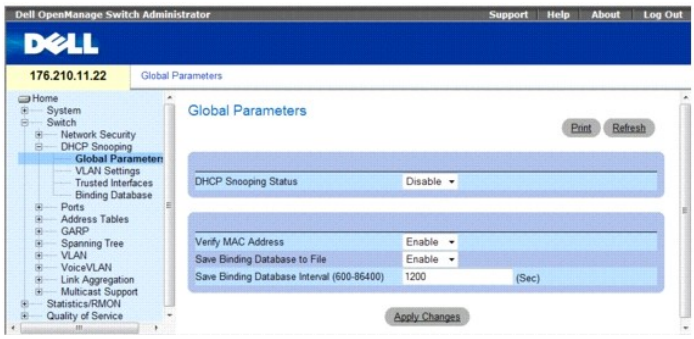
- Определение свойств для наблюдения по протоколу DHCP.
- Определение в сетях VLAN наблюдения по протоколу DHCP.
- Определение доверенных интерфейсов.
- Добавление интерфейсов в базу данных для наблюдения по протоколу DHCP.

Определение общих параметров для наблюдения по протоколу DHCP

На странице **DHCP Snooping Global Parameters** (Общие параметры для наблюдения по протоколу DHCP) содержатся параметры для включения и настройки наблюдения по протоколу DHCP на устройстве.

Чтобы определить общие параметры для наблюдения по протоколу DHCP, выберите **Switch** (Коммутатор)→ **DHCP Snooping** (Наблюдение по протоколу DHCP)→ **Global Parameters** (Общие параметры).

Рис. 7-16. Страница Global Parameters (Общие параметры)



- **DHCP Snooping Status** (Состояние наблюдения по протоколу DHCP). Обозначает, включено ли наблюдение по протоколу DHCP на устройстве. Ниже указаны возможные значения.
  - **Enable** (Включено). Включает наблюдение по протоколу DHCP на устройстве.
  - **Disable** (Выключено). Выключает наблюдение по протоколу DHCP на устройстве. Это значение по умолчанию.
- **Verify MAC Address** (Проверить MAC-адреса). Обозначает, выполнена ли проверка MAC-адресов. Ниже указаны возможные значения.
  - **Enable** (Включено). Выполняется проверка на соответствие исходного MAC-адреса ненадежного порта MAC-адресу клиента.
  - **Disable** (Выключено). Отключает проверку на соответствие исходного MAC-адреса ненадежного порта MAC-адресу клиента. Это значение по умолчанию.
- **Save Binding Database to File** (Сохранить базу данных привязки в файл). Указывает способ сохранения базы данных для наблюдения по протоколу DHCP, а именно сохранение в файл. Ниже указаны возможные значения:
  - **Enable** (Включено). Сохранение базы данных в файл. Это значение по умолчанию.
  - **Disable** (Выключено). Выключено сохранение базы данных в файл.
  - **Save Binding Database Internal** (Сохранить базу данных привязки внутри). Обозначает, как часто обновляется база данных для наблюдения по протоколу DHCP. Возможные значения поля: 600 - 86400 секунд. Значение по умолчанию: 1200 секунд.

Настройка общих параметров для наблюдения по протоколу DHCP с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для настройки общих параметров для наблюдения по протоколу DHCP.

Команда консоли	Описание
ip dhcp snooping **no ip dhcp snooping**	Команда настройки общих параметров ip dhcp snooping используется для глобального включения наблюдения по протоколу DHCP. Чтобы восстановить значение по умолчанию, используйте форму no этой команды.
ip dhcp snooping verify **no ip dhcp snooping verify**	Команда настройки общих параметров ip dhcp используется для того, чтобы настроить коммутатор, который будет проверять на ненадежном порте соответствие исходного MAC-адреса в пакете DHCP с адресом оборудования клиента. Чтобы настроить коммутатор на отмену проверки MAC-адресов, используйте форму no этой команды.

ip dhcp snooping database **no ip dhcp snooping database**	Команда настройки общих параметров ip dhcp snooping database используется для настройки файла привязки для наблюдения по протоколу DHCP. Чтобы удалить файл привязки, используйте форму no этой команды.
ip dhcp snooping database update-freq *секунды* **no ip dhcp snooping database update-freq**	Команда настройки общих параметров ip dhcp snooping database update-freq используется для настройки частоты обновления файла привязки для наблюдения по протоколу DHCP. Для возврата к значениям по умолчанию используйте форму no этой команды
show ip dhcp snooping [**ethernet** *интерфейс* | **port-channel** *номер_порта_канала*]	В режиме EXEC с помощью команды show ip dhcp snooping отображается конфигурация наблюдения по протоколу DHCP.

Далее приведен пример нескольких команд консоли.

```
Console# show ip dhcp snooping

DHCP snooping is enabled

DHCP snooping is configured on following VLANs: 2, 7-18

DHCP snooping database: enabled

Option 82 on untrusted port is allowed

Verification of hwaddr field is enabled
```

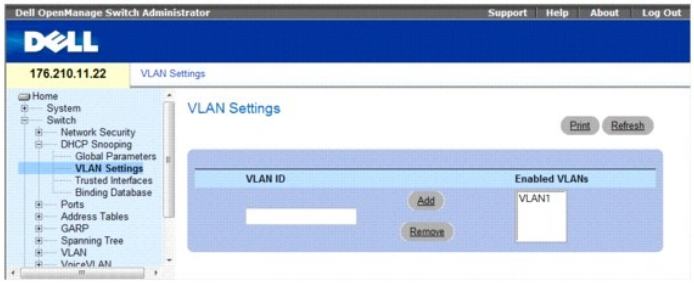
Interface	Trusted
----------	----------
g1	yes
g2	yes

Определение в сетях VLAN наблюдения по протоколу DHCP

С помощью страницы **DHCP Snooping VLAN Settings** (Параметры VLAN для наблюдения по протоколу DHCP) администраторы сети могут включать в сетях VLAN наблюдение по протоколу DHCP. Наблюдение по протоколу DHCP разделяет порты в сети VLAN. Чтобы включить наблюдение по протоколу DHCP в сети VLAN, убедитесь, что наблюдение по протоколу DHCP включено на устройстве.

Чтобы определить в сетях VLAN наблюдение по протоколу DHCP, выберите **Switch** (Коммутатор)→ **DHCP Snooping** (Наблюдение по протоколу DHCP)→ **VLAN Settings** (Параметры VLAN).

Рис. 7-17. Страница VLAN Settings (Параметры VLAN)



- **VLAN ID** (Идентификатор VLAN). Сеть VLAN, для которой можно включить наблюдение по протоколу DHCP.
- **Enabled VLANs** (Включенные сети VLAN). Список сетей VLAN, для которых включено наблюдение по протоколу DHCP.

Определение в сетях VLAN наблюдения по протоколу DHCP

1. Откройте страницу DHCP Snooping VLAN Settings (Параметры VLAN для наблюдения по протоколу DHCP).
2. Выберите **Add** (Добавить) или **Remove** (Удалить), чтобы добавить или удалить идентификаторы сети VLAN из списка включенных сетей VLAN.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Настройка в сетях VLAN наблюдения по протоколу DHCP с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для настройки в сетях VLAN **наблюдения по протоколу DHCP.**

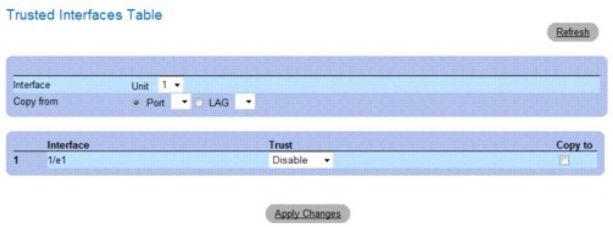
Команда консоли	Описание
ip dhcp snooping vlan *идентификатор_vlan* **no ip dhcp snooping** *идентификатор_vlan*	Команда настройки общих параметров ip dhcp snooping vlan используется для включения наблюдения по протоколу DHCP в сети VLAN. Чтобы отключить наблюдение по протоколу DHCP в сети VLAN, используйте форму no этой команды.

Определение доверенных интерфейсов

С помощью страницы **Trusted Interfaces** (Доверенные интерфейсы) администраторы сети могут определить доверенные интерфейсы. Если пакет поступает с интерфейса, находящегося за пределами сети или отсутствующего в правилах сетевого брандмауэра, такие интерфейсы считаются ненадежными. На доверенные интерфейсы пакеты поступают только из сети или от сетевого брандмауэра.

Чтобы определить доверенные интерфейсы, выберите **Switch** (Коммутатор)→ **DHCP Snooping** (Наблюдение по протоколу DHCP)→ **Trusted Interface** (Доверенный интерфейс)

Рис. 7-18. Страница Trusted Interfaces (Доверенные интерфейсы)



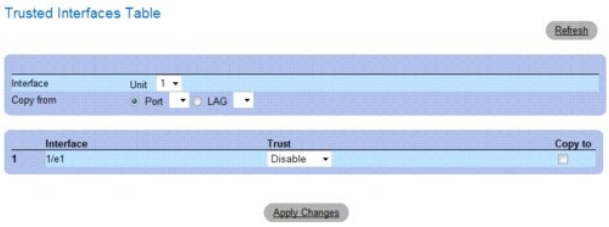
- **Interface** (Интерфейс). Обозначает порт или группу LAG, для которой включен режим доверия при использовании наблюдения по протоколу DHCP.
- **Trust Status** (Статус доверия). Обозначает, включен ли режим доверия для порта или группы LAG при использовании наблюдения по протоколу DHCP. Ниже указаны возможные значения:
  - **Enable** (Включить). Указывает, что режим доверия для порта или группы LAG при наблюдении по протоколу DHCP включен.
  - **Disable** (Отключить). Указывает, что режим доверия для порта или группы LAG при наблюдении по протоколу DHCP отключен.

Отображение таблицы доверенных интерфейсов

1. Откройте страницу **Trusted Interfaces** (Доверенные интерфейсы).
2. Нажмите кнопку **Show All** (Показать все).

   Отобразится таблица Trusted Interfaces (Таблица доверенных интерфейсов).

   Рис. 7-19. Таблица доверенных интерфейсов



Копирование параметров доверенных интерфейсов на другие интерфейсы

1. Откройте страницу **Trusted Interfaces** (Доверенные интерфейсы).
2. Нажмите кнопку **Show All** (Показать все). Отобразится таблица **Trusted Interfaces Table** (Таблица доверенных интерфейсов).

3. В полях **Unit** (Устройство) и **Copy from** (Копировать из) выберите порт или группу LAG, откуда необходимо скопировать параметры.
4. В таблице установите флажок **Copy to** (Копировать в) для каждой записи, для которой требуется скопировать параметры.
5. Нажмите кнопку **Apply Changes** (Применить изменения).

Назначение доверенных и ненадежных интерфейсов

1. Откройте страницу **Trusted Interfaces** (Доверенные интерфейсы).
2. Нажмите кнопку **Show All** (Показать все). Отобразится таблица **Trusted Interfaces Table** (Таблица доверенных интерфейсов).
3. В столбце **Trust** (Доверие) включите или отключите режим доверия для интерфейса.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Настройка наблюдения по протоколу DHCP для доверенных интерфейсов с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для настройки **наблюдения по протоколу DHCP для доверенных интерфейсов**.

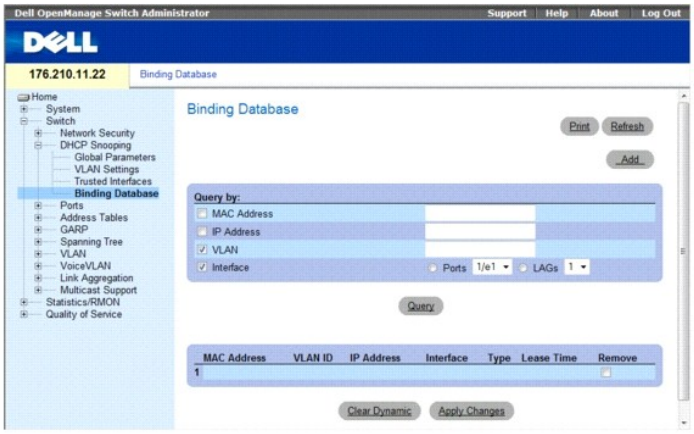
Команда консоли	Описание
ip dhcp snooping trust **no ip dhcp snooping trust**	Команда настройки доверия для интерфейса ip dhcp snooping trust используется для включения режима доверия для порта при наблюдении по протоколу DHCP. Чтобы восстановить значение по умолчанию, используйте форму no этой команды.

Добавление интерфейсов в базу данных для наблюдения по протоколу DHCP

На странице **DHCP Snooping Binding Database** (База данных привязки для наблюдения по протоколу DHCP) содержатся параметры для запроса и добавления IP-адресов в базу данных для наблюдения по протоколу DHCP.

Чтобы открыть страницу включения в базу данных, выберите **Switch** (Коммутатор)→ **DHCP Snooping** (Наблюдение по протоколу DHCP)→ **Binding Database** (База данных привязки)

Рис. 7-20. Страница Binding Database (База данных привязки)



Выполнение запроса к базе данных

1. Откройте страницу **Binding Database** (База данных привязки).
2. Выберите следующие категории:
   - **MAC Address** (MAC-адрес). MAC-адреса, включенные в базу данных для наблюдения по протоколу DHCP.
   - **IP Address** (IP-адрес). IP-адреса, включенные в базу данных для наблюдения по протоколу DHCP.

- **VLAN** (Сеть VLAN). Сети VLAN, включенные в базу данных наблюдения по протоколу DHCP.
- **Interface** (Интерфейс). Список интерфейсов, включенных в базу данных для наблюдения по протоколу DHCP. Ниже указаны возможные значения. Port (Порт) и LAG (Группа LAG).
- Кроме перечисленных выше полей, в таблице результатов запроса отображаются следующие поля:
- **VLAN ID** (Идентификатор сети VLAN). Идентификатор сети VLAN, с которой связан IP-адрес в базе данных для наблюдения по протоколу DHCP.
- **Type** (Тип). Тип назначения IP-адреса. Возможные значения: **Static** (Статический) - IP-адрес назначен статически; **Dynamic** (Динамический) - IP-адрес назначен динамически.
- **Lease Time** (Время использования). Время использования. Параметр Lease Time (время использования) указывает период времени, в течение которого запись в базе данных DHCP является активной. Коммутатор игнорирует записи с истекшим временем использования.

3. Нажмите кнопку **Query** (Запрос).

Удаление записи из базы данных

1. Откройте страницу **Binding Database** (База данных привязки).
2. В таблице установите флажок в столбце **Remove** (Удалить) рядом с нужной записью.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Очистка динамической базы данных

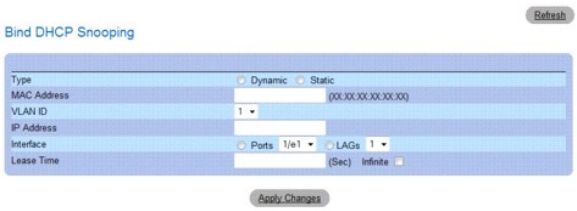
1. Откройте страницу **Binding Database** (База данных привязки).
2. Нажмите кнопку **Clear Dynamic** (Динамическая очистка).

Привязка базы данных для наблюдения по протоколу DHCP

1. Откройте страницу **Binding Database** (База данных привязки).
2. Нажмите кнопку **Add** (Добавить).

   Откроется страница **Bind DHCP Snooping** (Привязка для наблюдения по протоколу DHCP).

   Рис. 7-21. Страница Bind DHCP Snooping (Привязка для наблюдения по протоколу DHCP)



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

Настройка базы данных привязки для наблюдения по протоколу DHCP с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для настройки **базы данных привязки для наблюдения по протоколу DHCP**.

Команда консоли	**Описание**
ip dhcp snooping binding *mac-адрес идентификатор_vlan ip-адрес* {**ethernet** *интерфейс* | **port-channe**l *номер_порта-канала*} **expiry** *секунды* **no ip dhcp snooping binding** *mac-адрес идентификатор_vlan*	В режиме экрана Privileged EXEC с помощью команды **ip dhcp snooping binding** выполняется настройка базы данных для наблюдения по протоколу DHCP или добавление в базу данных записей привязки. Чтобы удалить записи из базы данных привязки, используйте форму no этой команды.

clear ip dhcp snooping database	В режиме экрана Privileged EXEC с помощью команды **clear ip dhcp snooping database** можно удалить базу данных привязки для наблюдения по протоколу DHCP.
show ip dhcp snooping binding [**mac-address** *mac-адрес*] [**ip-address** *ip-адрес*] [**vlan** *vlan*] [**ethernet** *интерфейс* | **port-channel** *номер_порта-канала*]	В режиме User EXEC помощью команды **show ip dhcp snooping binding** отображается база данных привязки для наблюдения по протоколу DHCP и информации о настройке для всех интерфейсов коммутатора.

Далее приведен пример нескольких команд консоли.

```
Console# show ip dhcp snooping binding

Update frequency: 1200

Total number of binding: 2
```

Mac Address	IP Address	Lease (sec)	Type	VLAN	Interface
----------	----------	----------	-------	-------	-------
0060.704C.73FF	10.1.8.1	7983	snooping	3	1/21
0060.704C.7BC1	10.1.8.2	92332	snooping	(s)3	1/22

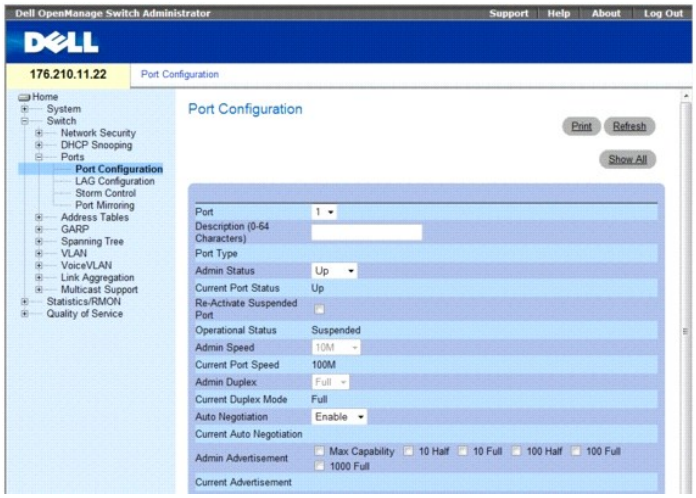
Настройка портов

На странице **Ports** (Порты) находятся ссылки для настройки работы портов, в том числе таких функций, как контроль «лавины» и зеркалирование портов. Чтобы открыть страницу **Ports** (Порты), выберите **Switch** (Коммутатор)→ **Ports** (Порты).

Определение параметров порта

Страница **Port Configuration** (Настройка порта) содержит поля, позволяющие определить параметры порта. Чтобы открыть страницу **Port Configuration** (Настройка портов), выберите **Switch** (Коммутатор)→ **Ports** (Порты)→ **Port Configuration** (Настройка портов) на панели дерева.

Рис. 7-22. Страница Port Configuration (Настройка портов)



- **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. Новое состояние порта отображается в поле **Current Port Status** (Текущее состояние порта).
- **Current Port Status** (Текущее состояние порта). Показывает, в работоспособном ли состоянии находится в настоящий момент порт.
- **Re-Activate Suspended Port** (Возврат к работе отключенного порта). Активизирует порт, если он был отключен с помощью функции безопасности блокировки портов.
- **Operational Status** (Рабочее состояние). Рабочее состояние порта. Возможные значения этого поля:
  - **Suspended** (Приостановлен). Порт активен, но 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 для порта отключено автоматическое согласование.
- **Current Port Speed** (Текущая скорость порта). Текущая скорость порта (бит/с).
- **Admin Duplex** (Администрирование дуплексного режима). Режим порта может быть **Full** (Дуплексный) или **Half** (Полудуплексный). Значение **Full** 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** (Текущий дуплексный режим). Текущий дуплексный режим порта.
- **Auto Negotiation** (Автоматическое согласование). Включает автоматическое согласование для порта. Автоматическое согласование - это протокол между двумя партнерами канала связи, который позволяет порту известить о своей скорости передачи, возможности работы в дуплексном режиме и управления потоком.
- **Current Auto Negotiation** (Текущее автоматическое согласование). Текущая настройка параметра автоматического согласования.
- **Admin Advertisement** (Объявление администрирования). Объявляемая портом скорость. Возможные значения: Maximum Capacity (Максимальная емкость), 10 MB Half-Duplex (Полудуплекс 10 МБ), 10 MB Full-Duplex (Полный дуплекс 10 МБ), 100 MB Half-Duplex (Полудуплекс 100 МБ), 100 MB Full-Duplex (Полный дуплекс 100 МБ) и 1000 MB Full-Duplex (Полный дуплекс 1000 MB).
- **Current Advertisement** (Текущее объявление). Порт объявляет скорость соседнему порту для начала согласования. Возможные значения полей указаны в поле **Admin Advertisement** (Объявление администрирования).
- **Neighbor Advertisement** (Объявление соседнего порта). Объявляемые параметры соседнего порта. Значения этого поля совпадают со значениями поля Admin Advertisement (Объявление администрирования).
- **Back Pressure** (Обратное давление). Включает режим обратного давления для порта. Режим обратного давления используется с полудуплексным режимом, чтобы отключить получение сообщений на порты.
- **Current Back Pressure** (Текущий режим обратного давления). Текущая настройка параметра режима обратного давления.
- **Flow Control** (Управление потоком). Включает или отключает управление потоком или включает автоматическое согласование управления потоком для порта. Работает, когда порт находится в режиме **Full** (Дуплексный).
- **Current Flow Control** (Текущее управление потоком). Текущая настройка параметра 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. Ниже указаны возможные значения.

- **Auto** (Автоматически). Используется для автоматического определения типа кабеля.
- **MDI (Media Dependent Interface)**. Используется для конечных станций.
- **MDIX (Media Dependent Interface with Crossover)**. Используется для концентраторов и коммутаторов.

- **Current MDI/MDIX** (Текущий MDI/MDIX). Текущие настройки параметров MDI/MDIX.
- **LAG**. Показывает, что порт входит в группу LAG.
- **PVE (Uplink)** (PVE (Групповое соединение)). Порт может быть задан как PVE (Private VLAN Edge) или как порт группового соединения. В этом случае он будет изолирован от других портов в сети VLAN.

Определение параметров порта

1. Откройте страницу **Port Configuration** (Настройка портов).
2. Выберите порт в поле **Port** (Порт).
3. Определите оставшиеся поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Параметры порта будут сохранены для этого устройства.

Изменение параметров порта

1. Откройте страницу **Port Configuration** (Настройка портов).
2. Выберите порт в поле **Port** (Порт).
3. Измените соответствующие поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

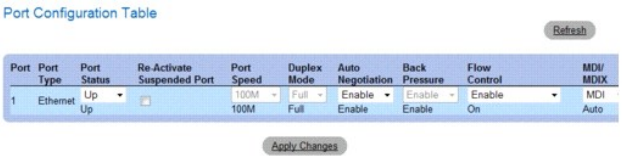
Параметры порта будут сохранены для этого устройства.

Отображение таблицы настройки портов

1. Откройте страницу **Port Configuration** (Настройка портов).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **Ports Configuration Table** (Таблица настройки портов) .

Рис. 7-23. Страница Ports Configuration Table (Таблица настройки портов)



Настройка портов с помощью команд консоли

В следующей таблице приведены команды консоли для настройки портов, как показано на странице **Ports Configuration Table** (Таблица настройки портов).

Табл. 7-12. Команды консоли для настройки портов

Команда консоли	**Описание**
interface ethernet *интерфейс*	Включает режим настройки интерфейса для настройки типа интерфейса Ethernet.
description *строка*	Добавляет описание в конфигурацию интерфейса.
shutdown	Выключает интерфейсы, которые входят в состав текущего заданного контекста.
set interface active {**ethernet** *интерфейс* | **port-channel** *номер_порта-канала}*	Вновь активизирует интерфейс, отключенный по причинам безопасности.
speed *бит/с*	Настраивает скорость заданного интерфейса Ethernet, если не используется автоматическое согласование.
autobaud	Устанавливает автоматическое определение скорости канала.
duplex {**half** | **full**}	Настраивает дуплексный или полудуплексный режим для заданного интерфейса Ethernet, если не используется автоматическое согласование.
negotiation	Включает автоматическое согласование для параметров скорости и дуплексного режима данного интерфейса.
back-pressure	Включает режим обратного давления для заданного интерфейса.
flowcontrol {**auto** | **on** | **off** | **rx** | **tx**}	Настраивает управление потоком для заданного интерфейса.
system flowcontrol (контроль пропускной способности системы)	Включает контроль потока данных системы на каскадных портах (между двумя ЦП). Эта команда относится только к устройствам с 48 портами.
mdix {**on** | **auto**}	Включает автоматическое использование перекрестного кабеля для заданного интерфейса или канала порта.
show interfaces configuration [**ethernet** *интерфейс* | **port-channel** *номер_порта-канала*]	Отображает конфигурацию для всех настроенных интерфейсов.
show interfaces status [**ethernet** *интерфейс* | **port-channel** *номер_порта-канала*]	Отображает состояние для всех настроенных интерфейсов.
show interfaces description [**ethernet** *интерфейс* | **port-channel** *номер_порта-канала*]	Отображает описание для всех настроенных интерфейсов.
show system flowcontrol (показать поток данных системы)	Отображает текущее состояние функции контроля пропускной способности системы на каскадных портах (между двумя ЦП). Эта команда относится только к устройствам с 48 портами.

Далее приведен пример команд консоли.

```
Console (config)# interface ethernet g5

Console (config-if)# description RD SW#3

Console (config-if)# shutdown
```

```
Console (config-if)# no shutdown

Console (config-if)# speed 100

Console (config-if)# duplex full

Console (config-if)# negotiation

Console (config-if)# back pressure

Console (config-if)# flowcontrol on

Console (config-if)# mdix auto

Console (config-if)# exit

Console (config)# exit

Console# show interfaces configuration ethernet g5
```

Port	Type	Duplex	Speed	Neg	Flow Control	Admin State	Back Pressure	Mdix Mode
g5	1G	Full	100	Enabled	On	Up	Enable	Auto
console#								

```
console# show interfaces status ethernet g5
```

Port	Type	Duplex	Speed	Neg	Flow Control	Link State	Back Pressure	Mdix Mode
g5	1G	Full	100	Enabled	On	Up	Disabled	on
console#								

```
Console# show interfaces status
```

Port	Type	Duplex	Speed	Neg	Flow Control	Link State	Back Pressure	Mdix Mode
g1	1G	Full	100	Auto	On	Up	Enable	On
g1	100	Full	100	Off	Off	Down	Disable	Off
g2	100	Full	1000	Off	Off	Up	Disable	On

Ch	Type	Duplex	Speed	Neg	Flow Control	Back Pressure	Link State	
1	1000	Full	1000	Off	Off	Disable	Up	

Настройка выравнивания нагрузки

Выравнивание нагрузки обеспечивает равномерное распределение данных и/или пакетов для обработки между доступными ресурсами сети. Например, в результате выравнивания нагрузки входящие пакеты равномерно распределяются между всеми серверами или направляются на следующий доступный сервер. Выравнивание нагрузки можно настроить на странице LAG Configuration (Настройка LAG).

Группы LAG можно настроить в соответствии со следующими типами выравнивания нагрузки: Layer 2 (Уровень 2), Layer 2-3 (Уровень 2-3) или Layer 3 (Уровень 3).

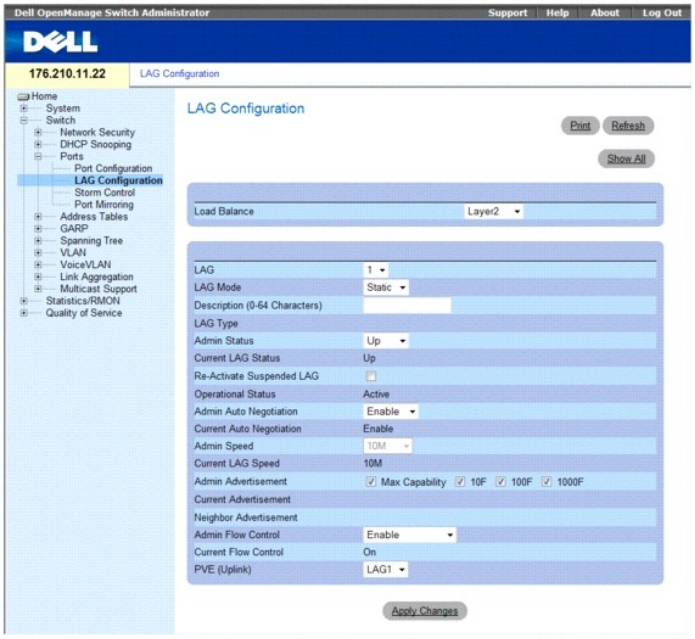
Страница **LAG Configuration** (Настройка LAG) содержит поля, позволяющие определить параметры настройки LAG. Устройство поддерживает до восьми портов на группу LAG и восьми групп LAG на систему.

Дополнительную информацию об объединенных **группах каналов (LAG)** и назначении им портов см. в разделе **Объединение портов**.

Чтобы открыть страницу **LAG Configuration** (Настройка LAG), выберите **Switch** (Коммутатор)→ **Ports** (Порты)→ **LAG Configuration** (Настройка LAG) на панели дерева.

При изменении конфигурации порта, входящего в группу LAG, изменения вступают в силу только после удаления порта из этой группы.

Рис. 7-24. Страница LAG Configuration (Настройка LAG)



Страница **LAG Configuration** (Настройка LAG) содержит следующие поля:

- **Load Balance** (Выравнивание нагрузки). Тип выравнивания нагрузки, включенный для LAG. Ниже указаны возможные значения.
  - **Layer 2** (Уровень 2). Выравнивание нагрузки на основе статических или динамических MAC-адресов.
  - **Layer 3** (Уровень 3). Выравнивание нагрузки на основе IP-адресов источника и места назначения.
  - **Layer 2-3** (Уровень 2-3). Выравнивание нагрузки на основе статических и динамических MAC-адресов и IP-адресов источника и места назначения.
- **LAG**. Номер группы LAG.
- **LAG Mode** (Режим LAG). Статический номер LAG или LACP.
- **Description (0-64 Characters)** (Описание (0-64 символов)). Описание группы LAG, задаваемое пользователем.
- **LAG Type** (Тип LAG). Типы портов, входящих в состав LAG.
- **Admin Status** (Состояние администрирования). Включает или отключает пересылку трафика через выбранную группу LAG.
- **Current LAG Status** (Текущее состояние LAG). Показывает, работает ли в данный момент группа LAG.
- **Re-Activate Suspended LAG** (Возврат к работе отключенной группы LAG). Заново активизирует отключенную группу LAG.
- **Operational Status** (Рабочее состояние). Рабочее состояние группы 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). Текущая настройка параметра автоматического согласования.
- **Admin Speed** (Администрирование скорости). Скорость, на которой работает LAG.
- **Current LAG Speed** (Текущая скорость группы LAG). Текущая скорость, на которой работает LAG.
- **Admin Advertisement** (Объявление администрирования). Объявляемая группой LAG скорость. Возможные значения: Maximum Capacity (Максимальная емкость), 10 MB Half-Duplex (Полудуплекс 10 МБ), 10 MB Full-Duplex (Полный дуплекс 10 МБ), 100 MB Full-Duplex (Полный дуплекс 100 МБ) и 1000 MB Full-Duplex (Полный дуплекс 1000 MB).
- **Current Advertisement** (Текущее объявление). Порт объявляет скорость соседнему порту для начала согласования. Возможные значения полей указаны в поле **Admin Advertisement** (Объявление администрирования).
- **Neighbor Advertisement** (Объявление соседнего порта). Объявляемые параметры соседнего порта. Значения этого поля совпадают со значениями поля Admin Advertisement (Объявление администрирования).
- **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.
- **PVE (Uplink)** (PVE (Групповое соединение)). Порт может быть задан как PVE (Private VLAN Edge) или как порт группового соединения. В этом

случае он будет изолирован от других портов в сети VLAN.

Определение параметров LAG

1. Откройте страницу **LAG Configuration** (Настройка LAG).
2. Выберите группу LAG в поле **LAG**.
3. Определите поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Параметры группы LAG будут сохранены для этого устройства.

Изменение параметров группы LAG

1. Откройте страницу **LAG Configuration** (Настройка LAG).
2. Выберите группу LAG в поле **LAG**.
3. Измените поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Параметры группы LAG будут сохранены для этого устройства.

Отображение таблицы настройки LAG

1. Откройте страницу **LAG Configuration** (Настройка LAG).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **LAG Configuration Table** (Таблица настройки LAG).

Рис. 7-25. Страница 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).

Табл. 7-13. Команды консоли для настройки LAG

Команда консоли	Описание
interface port-channel *номер_порта-канала*	Включает режим настройки интерфейса для указанного канала-порта.
port-channel load-balance {*уровень-2* | *уровень 2-3* | *уровень 2-3-4*}	Настройка политики выравнивания нагрузки каналов порта.
description *строка*	Добавляет описание в конфигурацию интерфейса.

shutdown	Выключает интерфейсы, которые входят в состав текущего заданного контекста.
speed *бит/с*	Настраивает скорость заданного интерфейса Ethernet, если не используется автоматическое согласование.
autobaud	Устанавливает автоматическое определение скорости канала.
negotiation	Включает автоматическое согласование для параметров скорости и дуплексного режима данного интерфейса.
back-pressure	Включает режим обратного давления для заданного интерфейса.
flowcontrol {**auto** | **on** | **off** | **rx** | **tx**}	Настраивает управление потоком для заданного интерфейса.
show interfaces configuration [**ethernet** *интерфейс* | **port-channel** *номер_порта-канала*]	Отображает конфигурацию для всех настроенных интерфейсов.
show interfaces status [**ethernet** *интерфейс* | **port-channel** *номер_порта-канала*]	Отображает состояние для всех настроенных интерфейсов.
show interfaces description [**ethernet** *интерфейс* | **port-channel** *номер_порта-канала*]	Отображает описание для всех настроенных интерфейсов.
show interfaces port-channel [*номер_порта-канала*]	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-if)# channel-group 1 mode on

console(config-if)# exit

console(config)# interface range e g21-24

console(config-if)# channel-group 1 mode on

console(config-if)# ex

console(config)# interface ethernet g5

console(config-if)# channel-group 2 mode on

console(config-if)# exit

console(config)# exit
```

```
console# show interfaces port-channel

Channel         Ports
---------       ---------
ch1             Inactive: g(21-24)
ch2             Active: g5
ch3
ch4
ch5
ch6
ch7
ch8
console#
```

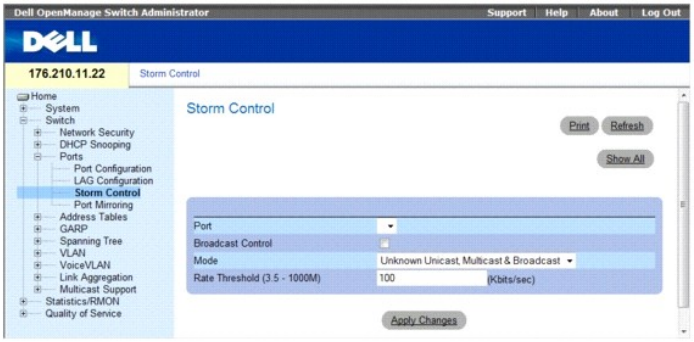
Включение контроля «лавины»

Широковещательная «лавина» - это результат чрезмерного количества широковещательных сообщений, одновременно передаваемых по сети через один порт. Ответы на пересылаемые сообщения являются причиной чрезмерной нагрузки на сеть, перегружая ее ресурсы или вызывая задержки в сети.

Система измеряет скорость входящих кадров одноадресной, широковещательной и многоадресной передачи отдельно для каждого порта и отбрасывает кадры, если скорость превышает значение, указанное пользователем.

Страница **Storm Control** (Контроль «лавины») содержит поля для включения и настройки контроля «лавины». Чтобы открыть страницу **Storm Control** (Контроль «лавины»), выберите **Switch** (Коммутатор)→ **Ports** (Порты)→ **Storm Control** (Контроль «лавины») на панели дерева.

Рис. 7-26. Страница Storm Control (Контроль «лавины»)



- **Port** (Порт). Порт, для которого включен контроль «лавины».
- **Broadcast Control** (Управление широковещательными передачами). Включает или отключает пересылку пакетов широковещательного типа на устройство.
- **Mode** (Режим). Указывает текущий режим широковещания, установленный для устройства. Возможны следующие значения поля.
  - **Unknown Unicast, Multicast & Broadcast** (Неизвестный одноадресный, многоадресный и широковещательный трафик). Выполняет подсчет одноадресного, многоадресного и широковещательного трафика.
  - **Multicast & Broadcast** (Многоадресный и широковещательный трафик). Выполняет подсчет широковещательного и многоадресного трафика одновременно.
  - **Broadcast Only** (Только широковещательный трафик). Выполняет подсчет только широковещательного трафика.
- **Rate Threshold (3.5-1000M)** (Порог скорости пакетов). Максимальная скорость (в килобитах в секунду), при которой пересылаются неизвестные пакеты. Диапазон значений: 3,5-1000 М.

Включение контроля «лавины» на устройстве

1. Откройте страницу **Storm Control** (Контроль «лавины»).
2. Выберите интерфейс, для которого хотите реализовать контроль «лавины».
3. Определите поля.
4. Нажмите кнопку **Show All** (Показать все).

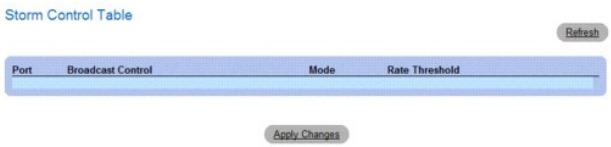
   Функция контроля «лавины» будет включена на устройстве.

Отображение страницы Storm Control Table (Таблица контроля «лавины»)

1. Откройте страницу **Storm Control** (Контроль «лавины»).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **Storm Control Table** (Таблица контроля «лавины»).

Рис. 7-27. Storm Control Table (Таблица контроля «лавины»)



Настройка контроля «лавины» с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для настройки контроля «лавины», как показано на странице **Storm Control** (Контроль «лавины»).

Таблица 7-14. Команды консоли для настройки контроля «лавины»

Команда консоли	Описание
port storm-control include-multicast	Позволяет устройству подсчитывать многоадресные пакеты вместе с широковещательными пакетами.
port storm-control broadcast enable	Включает контроль широковещательной «лавины».
port storm-control broadcast rate *скорость*	Настраивает максимальную скорость для широковещательных пакетов.
show ports storm-control [**ethernet** *интерфейс*]	Отображает конфигурацию контроля «лавины».

Далее приведен пример команд консоли.

```
console> enable

console# configure

Console(config)# port storm-control include-multicast

Console(config)# port storm-control broadcast rate 8000

Console(config)# interface ethernet g1

Console(config-if)# port storm-control broadcast enable

Console(config-if)# end

Console# show ports storm-control
```

Port	Broadcast Storm control [Packets/sec]
-----	----------
g1	8000
g2	Disabled
g4	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).

При настройке зеркалирования портов, выбирается определенный порт для копирования всех пакетов и разные порты, с которых копируются пакеты. Перед настройкой зеркалирования портов учтите следующее.

Если порт выбран в качестве порта назначения для сеанса с зеркалированием портов, все обычные операции с ним откладываются. К ним относятся операции Spanning Tree и LACP.

Перед настройкой зеркалирования портов учтите следующее.

- Контролируемые порты не могут работать быстрее, чем контролирующие.
- Все пакеты RX/TX должны контролироваться на одном порте.

К портам, настроенным как порты назначения, применяются следующие ограничения.

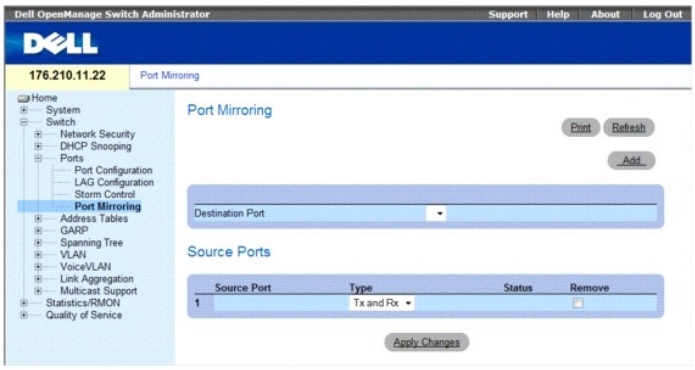
- Порты нельзя настроить в качестве портов-источников.
- Порты не могут входить в группу LAG.
- Для этого порта не настроены интерфейсы IP.
- Для этого порта не включен протокол GVRP.
- Порт не входит в сеть VLAN.
- Можно определить только один порт назначения.

К портам, настроенным как порты-источники, применяются следующие ограничения.

- Порты-источники не могут входить в группу LAG.
- Порты нельзя настроить в качестве портов назначения.
- Все пакеты помечаются при их передаче из порта назначения.
- Все пакеты RX/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. 7-28. Страница Port Mirroring (Зеркалирование портов)



- **Destination Port** (Порт назначения). Определяет номер порта, в который копируется трафик.
- **Source Port** (Порт-источник). Определяет номер порта, с которого копируется трафик.
- **Type** (Тип). Показывает, выполняет ли порт прием, передачу или и то, и другое.
- **Status** (Состояние). Показывает, выполняется ли в настоящий момент контроль порта (**Active**) или не выполняется (**Ready**).
- **Remove** (Удалить). Когда установлен этот флажок, удаляется сеанс зеркалирования портов.

Добавление сеанса с зеркалирования портов

1. Откройте страницу **Port Mirroring** (Зеркалирование портов).
2. Нажмите кнопку **Add** (Добавить).

   Откроется страница **Add Source Port** (Добавление порта-источника).
3. В раскрывающемся списке **Destination Port** (Порт назначения) выберите порт назначения.
4. В раскрывающемся списке **Source Port** (Порт-источник) выберите исходный порт.
5. Определите поле **Type** (Тип).
6. Нажмите кнопку **Apply Changes** (Применить изменения).

   Новый порт-источник будет определен, а устройство будет обновлено.

Удаление копии порта из сеанса с зеркалированием портов

1. Откройте страницу **Port Mirroring** (Зеркалирование портов).
2. Установите флажок **Remove** (Удалить).
3. Нажмите кнопку **Apply Changes** (Применить изменения).

   Выбранный сеанс с зеркалированием портов будет удален, а устройство обновлено.

Настройка сеанса с зеркалированием портов с помощью команд консоли

В следующей таблице приведены команды консоли, соответствующие полям страницы **Port Mirroring** (Зеркалирование портов) для настройки сеанса с зеркалированием портов.

Табл. 7-15. Команды консоли для настройки сеанса зеркалирования портов

Команда консоли	Описание
port monitor *интерфейс_src* [**rx** | **tx**]	Запускает сеанс с зеркалированием портов.

Далее приведен пример команд консоли.

```
Console (config)# interface ethernet g1

Console(config-if)# port monitor g8

Console# show ports monitor
```

Source Port	Destination Port	Type	Status	VLAN Tagging
g8	g1	RX, TX	Active	No
g2	g8	RX, TX	Active	No
g18	g8	Rx	Active	No

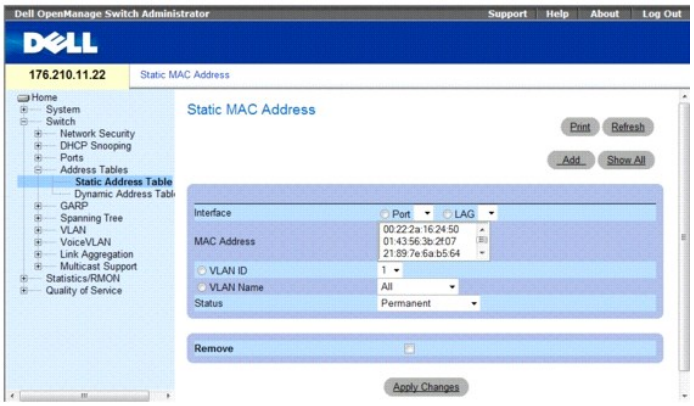
Настройка адресных таблиц

MAC-адреса хранятся в базах данных статических или динамических адресов. Пакет, адресованный приемнику, хранящемуся в одной из баз данных, немедленно пересылается на порт. Таблицы статических и динамических адресов могут быть отсортированы по интерфейсу, VLAN и типу интерфейса. MAC-адреса определяются динамически, когда пакеты от источников поступают на устройство. Адреса связываются с портами путем опознавания портов из исходного адреса кадра. Кадры, адресованные на MAC-адрес приемника, который не связан ни с каким портом, рассылаются «лавиной» на все порты соответствующей VLAN. Статические адреса настраиваются вручную. Чтобы предотвратить переполнение таблицы связей, динамические MAC-адреса, с которых не наблюдается трафик в течение определенного периода, удаляются. Чтобы открыть страницу **Address Tables** (Таблицы адресов), выберите **Switch** (Коммутатор)→ **Address Table** (Таблица адресов) на панели дерева.

Определение статических адресов

На странице Static MAC Address (Статический MAC-адрес) приведен список всех статических MAC-адресов. Статические адреса можно добавлять и удалять со страницы Static MAC Address (Таблица статических MAC-адресов). Кроме того, можно определить несколько MAC-адресов для одного порта. Чтобы открыть страницу **Static MAC Address** (Статический MAC-адрес), выберите **Switch** (Коммутатор)→ **Address Table** (Таблица адресов)→ **Static MAC Address** (Статический MAC-адрес) на панели дерева.

Рис. 7-29. Страница Static MAC Address (Статические MAC-адреса)



- **Interface** (Интерфейс). Порт или группа LAG, для которых назначены статические MAC-адреса.
- **MAC Address** (MAC-адрес). MAC-адрес из текущего списка статических адресов.
- **VLAN ID** (Идентификатор сети VLAN). Идентификатор сети VLAN, связанной с MAC-адресом.
- **VLAN Name** (Имя сети VLAN). Имя сети VLAN, определяемое пользователем.
- **Status** (Состояние). Состояние MAC-адреса. Возможные значения:
  - **Secure** (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** (Удалить по истечении времени ожидания). Показывает, что MAC-адрес удаляется по истечении времени ожидания.
- **Remove** (Удалить). Когда этот флажок установлен, MAC-адрес удаляется из таблицы MAC-адресов.

Добавление статического MAC-адреса

1. Откройте страницу **Static MAC Address** (Статический MAC-адрес).
2. Нажмите кнопку **Add** (Добавить).

   Откроется страница **Add Static MAC Address** (Добавление статического MAC-адреса).
3. Заполните поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Новый статический адрес будет добавлен в **Static MAC Address Table** (Таблицу статических MAC-адресов), а устройство обновлено.

Изменение статического MAC-адреса в таблице статических адресов

1. Откройте страницу **Static MAC Address** (Статический MAC-адрес).
2. 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** (Статический MAC-адрес).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **Static MAC Address Table** (Таблица статических MAC-адресов).
3. Выберите запись таблицы.
4. Установите флажок **Remove** (Удалить).
5. Нажмите кнопку **Apply Changes** (Применить изменения).

   Выбранный статический адрес будет удален, а устройство обновлено.

Настройка параметров статических адресов с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для настройки параметров статических адресов, как показано на странице Static MAC Address (Статический MAC-адрес).

Таблица 7-16. Команды консоли для настройки статических адресов

Команда консоли	**Описание**
bridge address *mac-адрес* {**ethernet** *interface* | **port-channel** *номер_канала_порта*} [**permanent** | **delete-on-reset** | **delete-on-timeout** | **secure**]	Добавляет статический MAC-адрес станции-источника в таблицу связей.
show bridge address-table [**vlan** *vlan*] [**ethernet** *interface* | **port-channel** *номер_канала_порта*]	Отображает записи базы данных, содержащей сведения о пересылке данных через мосты.

Далее приведен пример команд консоли.

```
Console# show bridge address-table
Aging time is 300 sec
vlan  mac address        port  type
----  ------------       ----  --------
1     00:60:70:4C:73:FF  g8    dynamic
1     00:60:70:8C:73:FF  g8    dynamic
200   00:10:0D:48:37:FF  g9    static
g8    00:10:0D:98:37:88  g8    dynamic
```

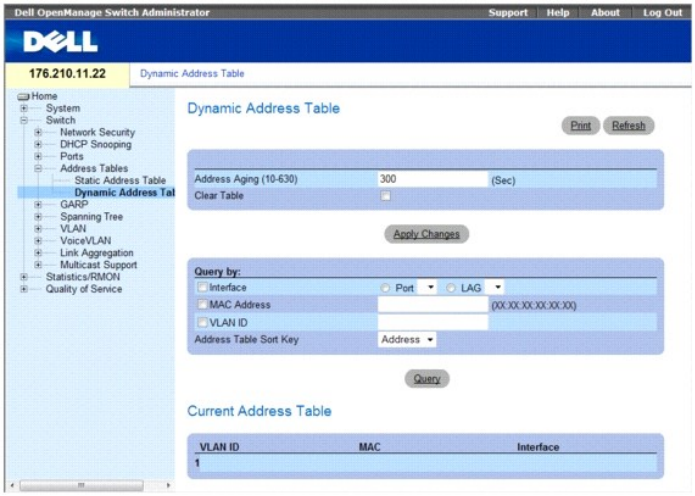
Просмотр динамических адресов

На странице **Dynamic Address Table** (Таблица динамических адресов) приведены сведения по запросу данных в таблице динамических адресов, в том числе типа интерфейса, MAC-адреса, VLAN и таблицы сортировки. Пакеты, которые пересылаются по адресам, хранящимся в таблице адресов, пересылаются непосредственно на эти порты.

Dynamic Address Table (Таблица динамических адресов) содержит информацию о сроке хранения, после которого динамические MAC-адреса удаляются, а также параметры для запросов и просмотра списка динамических адресов. Current Address Table (Таблица текущих адресов) содержит параметры динамических адресов, по которым пакеты передаются непосредственно на порты.

Чтобы открыть страницу **Dynamic Address Table** (Таблица динамических адресов), выберите **Switch** (Коммутатор)→ **Address Table** (Таблица адресов)→ **Dynamic Addresses Table** (Таблица динамических адресов) на панели дерева.

Рис. 7-30. Страница Dynamic Address Table (Таблица динамических адресов)



- **Address Aging (10-630)** (Срок хранения адреса). Определяет временной интервал, в течение которого MAC-адрес остается в **Dynamic Address Table** (Таблице динамических адресов) перед удалением, когда не обнаруживается трафик от источника. Значение по умолчанию: 300 секунд.
- **Interface** (Интерфейс). Определяет интерфейс, для которого будет выполнен запрос по таблице. Можно выбрать один из двух типов интерфейсов.
  - **Port** (Порт). Определяет номер порта, для которого будет выполнен запрос по таблице.
  - **LAG**. Определяет группу LAG, для которой будет выполнен запрос по таблице.
- **MAC Address** (MAC-адрес). Определяет MAC-адрес, для которого будет выполнен запрос по таблице.
- **VLAN ID** (Идентификатор сети VLAN). Определяет идентификатор сети VLAN, для которой будет выполнен запрос по таблице.
- **Address Table Sort Key** (Ключ для сортировки таблицы адресов). Определяет, по какому полю сортируется таблица динамических адресов.

Переопределение срока хранения

1. Откройте страницу **Dynamic Address Table** (Таблица динамических адресов).
2. Определите поле **Aging Time** (Срок хранения).
3. Нажмите кнопку Apply Changes (Применить изменения).

   Срок хранения будет изменен, а устройство обновлено.

Опрос таблицы динамических адресов

1. Откройте страницу **Dynamic Address Table** (Таблица динамических адресов).
2. Определите, по какому параметру нужно выполнить запрос таблицы **Dynamic Address Table** (Таблица динамических адресов).

   Записи запрашивать по полю **Port** (Порт), **MAC Address** (MAC-адрес) или **VLAN ID** (Идентификатор сети VLAN).

3. Нажмите кнопку **Query** (Запрос).

   Будет выполнен запрос по таблице **Dynamic Address Table** (Таблица динамических адресов).

Сортировка таблицы динамических адресов

1. Откройте страницу **Dynamic Address Table** (Таблица динамических адресов).
2. В падающем меню **Address Table Sort Key** (Ключ сортировки таблицы адресов) выберите поле, по которому будут отсортированы адреса - по адресу, идентификатору VLAN, или интерфейсу.
3. Нажмите кнопку **Query** (Запрос).

   Dynamic Address Table (Таблица динамических адресов) отсортирована.

Опрос и сортировка динамических адресов с помощью команд консоли

В следующей таблице приведены команды консоли, соответствующие полям для опроса и сортировки динамических адресов на странице **Dynamic Address Table** (Таблица динамических адресов).

Таблица 7-17. Команды консоли для опроса и сортировки динамических адресов

Команда консоли	**Описание**
bridge aging-time *секунды*	Задает срок хранения для таблиц адресов.
show bridge address-table [**vlan** *vlan*] [**ethernet** *интерфейс* | **port-channel** *номер_канала_порта*]	Отображает классы динамически созданных записей базы данных, содержащей сведения о пересылке данных через мосты.

Далее приведен пример команд консоли.

```
Console (config)# bridge aging-time 250

Console (config)# exit

Console# show bridge address-table
```

Aging time is 250 sec

vlan	mac address	port	type
----	-----------	----	----
1	00:60:70:4C:73:FF	g8	dynamic
1	00:60:70:8C:73:FF	g8	dynamic
200	00:10:0D:48:37:FF	g8	static

Настройка протокола GARP

Протокол GARP (Generic Attribute Registration Protocol) - это протокол общего назначения, регистрирующий любые возможности связи в сети или сведения о принадлежности. Протокол GARP определяет набор устройств, заинтересованных в данном атрибуте сети, например VLAN или адрес многоадресной передачи.

При настройке GARP выполняйте следующие инструкции:

- Время отключения должно быть больше или равно трехкратному времени соединения.
- Время полного отключения должно быть больше времени отключения.

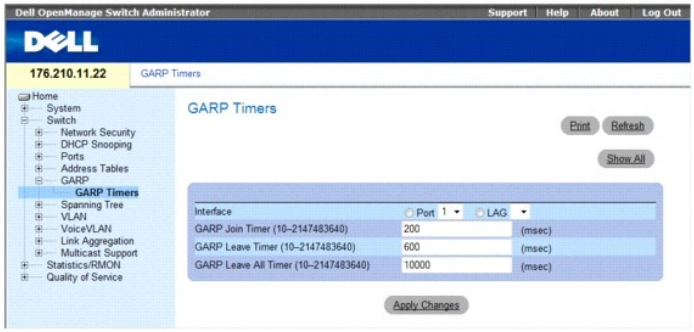
Устанавливает те же значения таймера GARP для всех устройство подключенных к уровню 2. Если таймеры GARP установлены по-разному на устройствах Layer 2, приложение GARP не сможет правильно работать.

Чтобы открыть страницу **GARP**, выберите **Switch** (Коммутатор)→ **GARP** на панели дерева.

Определение таймеров GARP

Страница **GARP Timers** (Таймеры GARP) содержит поля для включения протокола GARP на устройстве. Чтобы открыть страницу **GARP Timers** (Таймеры GARP), выберите **Switch** (Коммутатор)→ **GARP**→ **GARP Timers** (Таймеры GARP) на панели дерева.

Рис. 7-31. Страница GARP Timers (Таймеры GARP)



- **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 мс.
- **GARP Leave Timer (10 - 2147483640)** (Таймер отключения GARP). Время (в миллисекундах), в течение которого устройство ожидает, прежде чем выйти из состояния GARP. Отсчет времени Leave Time (Время отключения) активируется при отправке/получении сообщения Leave All Time (Время полного отключения) и отменяется при получении сообщения Join (Соединение). Время отключения должно быть больше или равно трехкратному времени соединения. 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).

   Откроется таблица **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 этой таблице приведены команды консоли для определения таймеров GARP, как показано на странице **Garp Timers** (Таймеры GARP).

Таблица 7-18. Команды консоли для определения таймеров GARP

Команда консоли	Описание
garp timer {**join** | **leave** | **leaveall**} *время*	Задает значения таймеров GARP для времени соединения, отключения и полного отключения приложений GARP.

Далее приведен пример команд консоли.

```
console(config)# interface ethernet g1

console(config-if)# garp timer leave 900

console(config-if)# end

console# show gvrp configuration ethernet g1



GVRP Feature is currently Disabled on the device.

Maximum VLANs: 223
```

Port(s)	GVRP-Status	Registration	Dynamic VLAN Creation	Timers Join	(milliseconds) Leave	Leave All
-------	--------	----------	----------	-------	------	--------
g1	Disabled	Normal	Enabled	200	900	10000
console#						

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 протоколы STP:

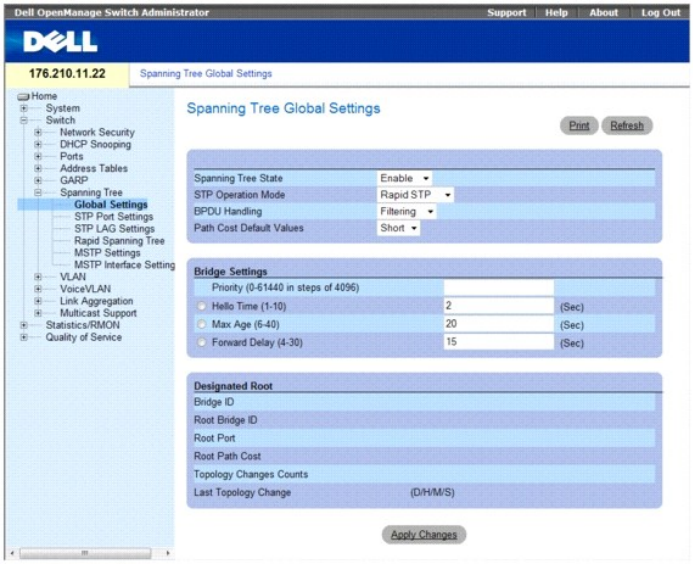
- **Classic STP** (Классический STP). Обеспечивает единственный путь между конечными станциями сети и исключает циклы. Дополнительную информацию о настройке классического STP см. в разделе Определение общих параметров STP.
- **Rapid STP** (Быстрый STP). Выявляет и использует топологию сети, обеспечивая лучшую сходимость для протокола STP без образования циклов пересылки. Дополнительную информацию о настройке быстрого STP см. в разделе Настройка протокола RSTP.

Чтобы открыть страницы **Spanning Tree**, выберите **Switch** (Коммутатор)→ **Spanning Tree** на панели дерева.

Определение общих параметров STP

Страница **STP Global Settings** (Общие параметры STP) содержит параметры для включения и настройки протокола STP на устройстве. Чтобы открыть страницу **STP Global Settings** (Общие параметры STP), выберите **Switch** (Коммутатор)→ **Spanning Tree**→ **Global Settings** (Общие параметры) на панели дерева.

Рис. 7-32. Страница STP Global Settings (Общие параметры STP)



- **Spanning Tree State** (Состояние Spanning Tree). Включает или отключает протокол STP для устройства. Ниже указаны возможные значения.
  - **Enable** (Включить). Включает протокол STP
  - **Disable** (Отключить). Отключает протокол STP
- **STP Operation Mode** (Режим работы STP). Режим включения протокола STP на устройстве. Ниже указаны возможные значения.
  - **Classic STP** (Классический STP). Включает классический STP на устройстве. Это значение по умолчанию.
  - **Rapid STP** (Быстрый STP). Включает быстрый STP на устройстве.
  - **Multiple STP** (Протокол MSTP). Включает множественный STP на устройстве.
- **BPDU Handling** (Обработка BPDU). Определяет, как будут обрабатываться пакеты BPDU, когда протокол STP отключен для порта или устройства. BPDU используется для передачи информации протокола STP. Ниже указаны возможные значения.
  - **Filtering** (Фильтр). Фильтрация пакетов BPDU, если протокол Spanning Tree отключен для интерфейса.
  - **Flooding** (Лавина). Оправка пакетов BPDU «лавиной», если протокол Spanning Tree отключен для интерфейса. Это значение по умолчанию.
- **Port Cost Default Values** (Значения по умолчанию определения стоимости порта). Определяет стоимость пути STP для порта. Ниже указаны возможные значения.
  - **Short** (Короткий). Определяет диапазон от 1 до 65535 для стоимости пути порта. Это значение по умолчанию.
  - **Long** (Длинный). Определяет диапазон от 1 до 200000000 для стоимости пути порта.
- **Priority (0-61440 in steps of 4096)** (Приоритет от 0 до 61440 с шагом 4096). Значение приоритета для моста. Когда коммутаторы или мосты работают по протоколу STP, каждому из них назначается приоритет. После обмена пакетами BPDU коммутатор с низшим значением приоритета становится корневым мостом. Значение по умолчанию: 32768. Значение приоритета моста предоставляется с шагом 4096 (4K). Например 0, 4096, 8192 и т.д.
- **Hello Time (1-10)** (Интервал приветствия). Определяет интервал приветствия для устройства. Это интервал отправки конфигурационных сообщений с корневого моста (в секундах). Значение по умолчанию: 2 секунды.
- **Max Age (6-40)** (Максимальное время). Определяет максимальное время для устройства. Это максимальное время (в секундах), которое мост ожидает перед отправкой конфигурационного сообщения. Значение по умолчанию: 20 секунд.
- **Forward Delay (4-30)** (Задержка пересылки). Определяет задержку пересылки для устройства. Это время, которое мост находится в состояниях распознавания (learning) и прослушивания (listening) перед пересылкой пакетов. Значение по умолчанию: 15 секунд.
- **Bridge ID** (Идентификатор моста). Идентификатор приоритета и MAC-адрес моста.
- **Root Bridge ID** (Идентификатор корневого моста). Идентификатор приоритета и MAC-адрес корневого моста.
- **Root Port** (Корневой порт). Номер порта, предлагающего путь от данного моста к корневому с наименьшими затратами. Этот параметр имеет значение, если мост не является корневым. Значение по умолчанию: 0.
- **Root Path Cost** (Стоимость пути до корневого). Стоимость пути от данного моста до корневого.
- **Topology Changes Counts** (Количество изменений топологии). Указывает общее количество изменений состояния STP с момента последней перезагрузки.
- **Last Topology Change** (Последнее изменение топологии). Время, прошедшее после инициализации или перенастройки моста и последнего изменения топологии. Выводится в формате «дни-часы-минуты-секунды», например: 0 дней 1 час 34 минуты и 38 секунд.

Определение общих параметров STP

1. Откройте страницу **STP Global Settings** (Общие параметры STP).

2. Выберите порт, который нужно включить, 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 **STP 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 **STP Global Settings** (Общие параметры STP).

Таблица 7-19. Команды консоли для определения общих параметров протокола STP

Команда консоли	Описание
spanning-tree	Включает функциональные возможности протокола STP.
spanning-tree mode {***stp*** | ***rstp*** | ***mstp***}	Настраивает протокол STP.
spanning-tree priority *приоритет*	Настраивает приоритет протокола STP.
spanning-tree hello-time *секунды*	Настраивает время Hello Time для моста протокола STP, определяющее, как часто устройство выполняет широковещательную передачу сообщений «Hello» другим коммутаторам.
spanning-tree max-age *секунды*	Настраивает максимальное время для моста протокола STP.
spanning-tree forward-time *секунды*	Настраивает время пересылки для моста протокола STP, определяющее, как долго порт находится в состоянии прослушивания и распознавания перед переключением в состояние пересылки.
show spanning-tree [**ethernet** *интерфейс* | **port-channel** *номер_канала_порта*] [**instance** *идентификатор_экземпляра*]	Отображает идентификатор конфигурации протокола STP.
show spanning-tree [**detail**] [**active** | **blockedports**] [**instance** *идентификатор_экземпляра*]	Отображает информацию о настройке протокола STP - подробную информацию об активных или заблокированных портах.
show spanning-tree mst-configuration	Отображает идентификатор конфигурации MST протокола STP.

Далее приведен пример команд консоли.

```
console(config)# spanning-tree

console(config)# spanning-tree mode rstp

console(config)# spanning-tree priority 12288

console(config)# spanning-tree hello-time 5

console(config)# spanning-tree max-age 15

console(config)# spanning-tree forward-time 25

console(config)# exit

console# show spanning-tree



Spanning tree enabled mode RSTP

Default port cost method: Short
```

Root ID		Priority		12288			
		Address		00:e8:00:b4:c0:00			
		This switch is the root					
		Hello Time 5 sec Max Age 15 sec Forward Delay 25 sec					
Number of topology changes 5 last change occurred 00:05:28 ago Times: hold 1, topology change 40, notification 5 hello 5, max age 15, forward delay 25							
Interfaces							
Name	State	Prio. Nbr	Cost	Sts	Role	PortFast	Type
-----	------	-----	----	------	------	---------	------
g1	enabled	128.1	100	DSBL	Dsbl	No	P2p (STP)
g2	enabled	128.2	100	DSBL	Dsbl	No	P2p (STP)
g3	enabled	128.3	100	DSBL	Dsbl	No	P2p (STP)

Определение параметров STP для порта

Страница **STP Port Settings** (Параметры STP для порта) содержит поля для назначения свойств STP для отдельных портов. 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. 7-33. Страница STP Port Settings (Параметры STP для порта)

- **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). разу 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.
- **Root Guard**. Когда функция отмечена флажком, это предотвращает назначение устройств за пределами ядра сети в качестве корня по протоколу STP.
- **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** (Отключен). Порт в настоящий момент отключен.
  - **Blocking** (Блокирование). Порт в данный момент заблокирован, и его нельзя использовать для передачи трафика или распознавания MAC-адресов. Параметр Blocking (Блокирование) отображается, когда включен режим Classic STP (Классический STP).
  - **Listening** (Прослушивание). Порт в данный момент находится в режиме прослушивания. Порт не может ни пересылать трафик, ни распознавать MAC-адреса.

- **Learning** (Распознавание). Порт в данный момент находится в режиме распознавания. Порт не может пересылать трафик, но может распознавать новые MAC-адреса.
- **Forwarding** (Пересылка). Порт в данный момент находится в режиме пересылки. Порт может пересылать трафик и распознавать новые MAC-адреса.

- **Role** (Роль). Отображение роли порта, назначаемого алгоритмом STP для указания для путей STP. Ниже указаны возможные значения.
  - **Root** (Корневой). Предоставляет путь с наименьшими затратами для пересылки пакетов в корневой коммутатор.
  - **Designated** (Назначенный). Указывает порт или группу LAG, с помощью которых назначенный коммутатор подключен к LAN.
  - **Alternate** (Альтернативный). Предлагает альтернативный путь к корневому коммутатору из корневого интерфейса.
  - **Backup** (Резервный). Предлагает резервный путь к указанному пути порта к «листьям» протокола STP. Резервные порты требуются только в том случае, когда два порта соединены в петлю с помощью соединения «точка-точка» или когда LAN имеет два или более соединений к сегменту с общим доступом.
  - **Disabled** (Отключено). Порт не участвует в соединении по протоколу STP.
- **Speed** (Скорость). Скорость, на которой работает порт.
- **Path Cost (1-200000000)** (Стоимость пути). Доля, которую этот порт вносит в стоимость пути к корню. Стоимость пути может иметь большее или меньшее значение и используется для пересылки трафика в случае переопределения маршрута пути.
- **Default Path Cost** (Стандартная стоимость пути). Стандартная стоимость пути для порта устанавливается автоматически с помощью скорости порта и метода определения стоимости стандартного пути для порта.

Ниже представлены значения по умолчанию для стоимости длинного пути.

- **Ethernet -** 2000000
- **Fast Ethernet** - 200000
- **Gigabit Ethernet** - 20000

Ниже представлены значения по умолчанию для стоимости короткого пути (стоимость короткого пути установлена по умолчанию).

- **Ethernet** - 100
- **Fast Ethernet** - 19
- **Gigabit Ethernet** - 4

- **Priority (0-240, in steps of 16)** (Приоритет от 0 до 240 с шагом 16). Значение приоритета для порта. Значение приоритета влияет на выбор порта, когда мост имеет два порта, соединенных в петлю. Значение приоритета находится в диапазоне: 0-240. Значения приоритета задаются с шагом 16.
- **Designated Bridge ID** (Идентификатор назначенного моста). Идентификатор приоритета и MAC-адрес назначенного моста.
- **Designated Port ID** (Назначенный порт). Приоритет и интерфейс 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 **Blocking** (Блокирование) на **Forwarding** (Пересылка).
- **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** (Включен) 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 7-20. Команды консоли для определения параметров STP для порта

Команда консоли	**Описание**
spanning-tree disable	Отключает протокол STP на определенном порте.
spanning-tree cost *стоимость*	Настройка стоимости пути для порта.
spanning-tree port-priority *приоритет*	Настраивает приоритет порта.
spanning-tree portfast	Включает режим PortFast.
show spanning-tree [ethernet *интерфейс* | **port-channel** *номер_канала_порта*]	Отображает конфигурацию протокола STP.
spanning-tree guard root	Включение функции Root Guard на всех экземплярах STP для данного интерфейса.

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)# exit

console(config)# exit

console# show spanning-tree ethernet g5
```

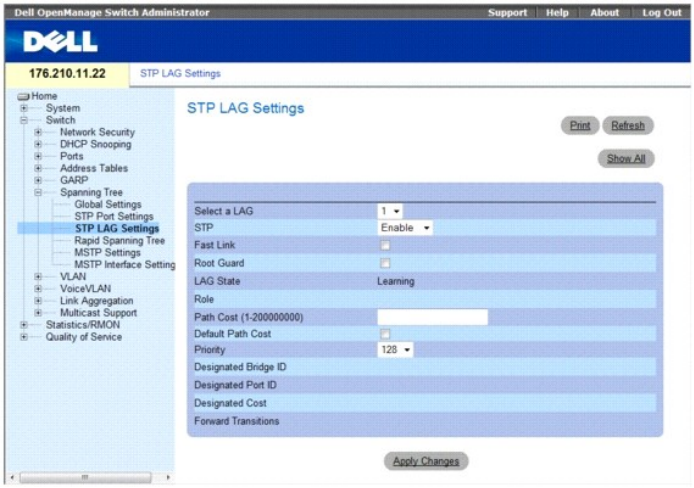
```
Port g5 disabled

State: disabled

Port id: 96.5

Type: P2p (configured: Auto) STP

Designated bridge Priority: 32768

Designated port id: 96.5

Number of transitions to forwarding
state: 0

BPDU: sent 0, received 0


console#
```

```
Role: disabled

Port cost: 35000

Port Fast: No (configured: No)

Address: 00:e8:00:b4:c0:00

Designated path cost: 19
```

Определение параметров STP для LAG

Страница **STP LAG Settings** (Параметры STP для LAG) содержит поля для назначения параметров STP для объединенных портов. 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. 7-34. Страница STP LAG Settings (Параметры STP для LAG)



- **Select a LAG** (Выбор LAG). Группа LAG, определенная пользователем. Дополнительную информацию см. в разделе Определение принадлежности к группе LAG.
- **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.
- **Root Guard.** Когда функция отмечена флажком, это предотвращает назначение устройств за пределами ядра сети в качестве корня по протоколу STP.
- **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** (Отключена). Группа LAG в данный момент отключена.
  - **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 неправильно, и ее нельзя использовать для пересылки трафика.
- **Role** (Роль). Отображение роли порта, назначаемого алгоритмом STP для указания для путей STP. Ниже указаны возможные значения.
  - **Root** (Корневой). Предоставляет путь с наименьшими затратами для пересылки пакетов в корневой коммутатор.
  - **Designated** (Назначенный). указывает порт или группу LAG, с помощью которых назначенный коммутатор подключен к LAN.
  - **Alternate** (Альтернативный). Предлагает альтернативный путь к корневому коммутатору из корневого интерфейса.
  - **Backup** (Резервный). Предлагает резервный путь к указанному пути порта к «листьям» протокола STP. Резервные порты требуются только в том случае, когда два порта соединены в петлю с помощью соединения «точка-точка» или когда LAN имеет два или более соединений к сегменту с общим доступом.
  - **Disabled** (Отключено). Порт не участвует в соединении по протоколу STP.
- **Path Cost (1-200000000)** (Стоимость пути). Доля, которую эта группа LAG вносит в стоимость пути к корню. Стоимость пути может иметь большее или меньшее значение и используется для пересылки трафика в случае переопределения маршрута пути. Стоимость пути может иметь значения от 1 до 200000000. Если выбран короткий метод стоимости пути, стоимость LAG по умолчанию будет иметь значение 4. Если выбран длинный метод стоимости пути, стоимость LAG по умолчанию будет иметь значение 20000.
- **Default Path Cost** (Стандартная стоимость пути). Когда установлен этот флажок, для стоимости пути LAG восстанавливается значение по умолчанию.
- **Priority** (Приоритет). Значение приоритета для группы LAG. Значение приоритета влияет на выбор LAG, когда на мосту два порта соединены в петлю. Значения приоритета находятся в диапазоне от 0 до 240 с шагом 16.
- **Designated Bridge ID** (Идентификатор назначенного моста). Идентификатор приоритета и MAC-адрес назначенного моста.

- **Designated Port ID** (Идентификатор назначенного порта). Приоритет порта и номер интерфейса назначенного порта.
- **Designated Cost** (Назначенная стоимость). Стоимость назначенного моста.
- **Forward Transitions** (Передача при пересылке). Показывает, сколько раз **LAG State** (Состояние LAG) изменялось с **Blocking** (Блокирование) на **Forwarding** (Пересылка).

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, соответствующие полям для определения параметров STP для LAG.

Таблица 7-21. Команды консоли для определения параметров STP для LAG

Команда консоли	Описание
spanning-tree	Включает STP.
spanning-tree disable	Отключает протокол STP для определенной группы LAG.
spanning-tree cost *стоимость*	Настраивает стоимость пути для группы LAG.
spanning-tree port-priority *приоритет*	Настраивает приоритет порта.
spanning-tree guard root	Включение функции Root Guard на всех экземплярах STP для данного интерфейса.
show spanning-tree [**ethernet** *интерфейс* | **port-channel** *номер_канала_порта*]	Отображает конфигурацию протокола STP.
show spanning-tree [**detail**] [**active** | **blockedports**]	Отображает подробную информацию протокола STP об активных или заблокированных портах.

Далее приведен пример команд консоли.

```
console(config)# interface port-channel 1

console(config-if)# spanning-tree port-priority 16
```

Настройка протокола RSTP

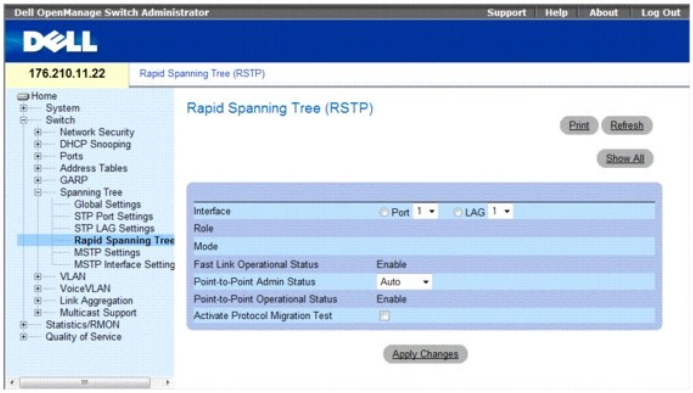
Если классический протокол STP не позволяет выполнить пересылку циклов Layer 2 в общей топологии сети, период сходимости может достигать от 30 до 60 секунд. Время сходимости рассматривается как слишком большое для многих приложений. Если топология сети позволяет, можно добиться лучшей сходимости. Протокол RSTP (Rapid Spanning Tree Protocol) выявляет и использует топологию сети, обеспечивая лучшую сходимость для протокола STP без образования циклов пересылки.

Протокол RSTP имеет несколько состояний портов:

- Disabled (Отключен)
- Learning (Распознавание)
- Discarding (Отбрасывание)
- Forwarding (Пересылка)

Протокол RSTP включается на странице **STP Global Settings** (Общие параметры STP). Чтобы открыть страницу **Rapid Spanning Tree (RSTP)**, выберите **Switch** (Коммутатор)→ **Spanning Tree** (Протокол STP)→ **Rapid Spanning Tree** (Протокол RSTP) на панели дерева.

Рис. 7-35. Страница Rapid Spanning Tree (RSTP)



- **Interface** (Интерфейс). Порт или LAG, для которого включен протокол RSTP.
- **Role** (Роль). Роль порта, назначаемого алгоритмом STP для указания для путей STP. Ниже указаны возможные значения.
  - **Root** (Корневой). Предоставляет путь с наименьшими затратами для пересылки пакетов в корневое устройство.
  - **Designated** (Назначенный). Порт или группа LAG, с помощью которых назначенное устройство подключено к LAN.
  - **Alternate** (Альтернативный). Предлагает альтернативный путь к корневому устройству из корневого интерфейса.
  - **Backup** (Резервный). Предлагает резервный путь к указанному пути порта к «листьям» протокола STP. Резервные порты требуется только в том случае, когда два порта соединены в петлю. Резервные порты также необходимы, когда LAN имеет два или более соединений к сегменту с общим доступом.
  - **Disabled** (Отключено). Порт не участвует в соединении по протоколу STP (соединение порта закрыто).
- **Mode** (Режим). Отображение режима включения протокола STP на устройстве. Ниже указаны возможные значения.
  - **Classic STP** (Классический STP). Включает классический STP на устройстве. Это значение по умолчанию.
  - **Rapid STP** (Быстрый STP). Включает быстрый STP на устройстве.
- **Multiple STP** (Протокол MSTP). Включает множественный STP на устройстве.
- **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 устройства. Он может отличаться от административного состояния.

- **Point-to-Point Operational Status** (Рабочее состояние соединения «точка-точка»). Показывает рабочее состояние соединения «точка-точка».
- **Activate Protocol Migrational 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 будет обновлено.

Определение параметров Rapid STP с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для определения параметров Rapid RSTP, как показано на странице **Rapid Spanning Tree (RSTP)**.

Таблица 7-22. Команды консоли для определения параметров Rapid STP

Команда консоли	Описание
spanning-tree link-type {**point-to-point** | **shared**}	Переопределяет тип связи по умолчанию.
spanning tree mode {**stp** | **rstp**}	Настраивает работающий в данный момент протокол STP.
clear spanning-tree detected-protocols [**ethernet** *интерфейс* | **port-channel** *номер_канала_порта*]	Перезапускает процесс миграции протоколов.
show spanning-tree [**ethernet** *интерфейс* | **port-channel** *номер_канала_порта*]	Отображает конфигурацию протокола STP.

Далее приведен пример команд консоли.

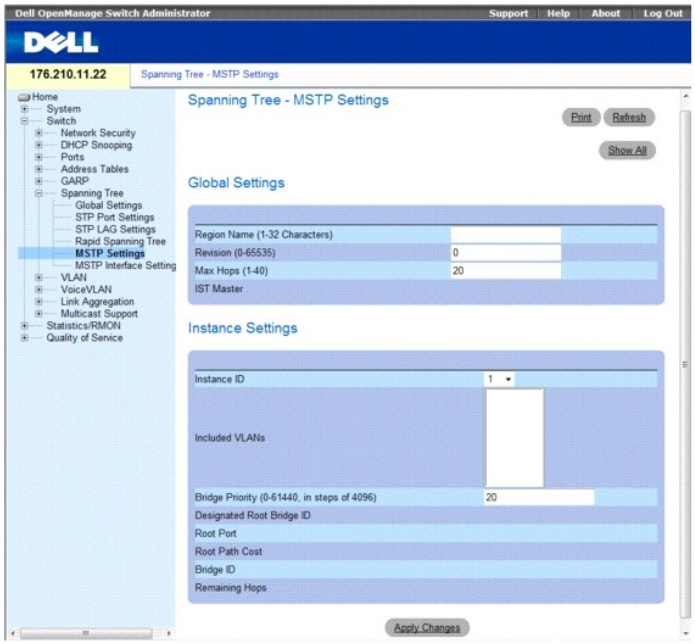
```
Console (config)# interface ethernet g5

Console(config-if)# spanning-tree link-type shared
```

Настройка протокола Multiple Spanning Tree

Протокол MSTP сопоставляет сети VLAN в экземплярах STP. Данный протокол обеспечивает другой сценарий выравнивания нагрузки. Например, при блокировке порта A в одном экземпляре STP этот порт переходит в состояние *Forwarding State* (состояние пересылки) в другом экземпляре STP.

Кроме того, пакеты, назначенные разным VLAN, передаются через разные пути в областях MST. Областями являются один или несколько мостов Multiple Spanning Tree, по которым передаются кадры. Чтобы открыть страницу **MSTP Settings** (Параметры MSTP), выберите **Switch** (Коммутатор)→ **Spanning Tree** (Протокол STP)→ **MSTP Settings** (Настройка области MSTP) на панели дерева.

Рис. 7-36. Страница MSTP Settings (Параметры MSTP)



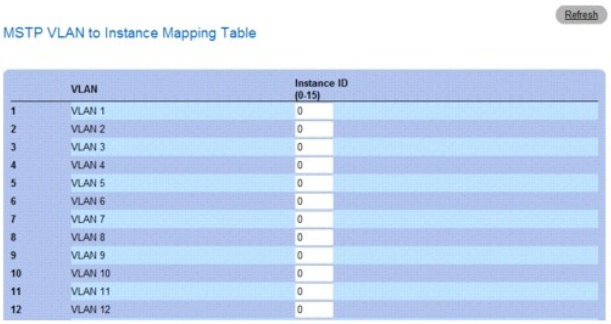
- **Region Name (1-32)** (Имя области). Указывает имя области MSTP, определяемое пользователем.
- **Revision (0-65535)** (Версия). Указывает 16-битное число без знака, определяющее версию текущей настройки MST. Номер версии необходим для настройки MST. Возможные значения поля: 0-65535.
- **Max Hops (1-40)** (Максимальное число узлов). Указывает общее число узлов, возникающих в определенной области, перед тем как пакеты BPDU будут отброшены. После того как пакеты BPDU будут отброшены, срок хранения информации о порте истечет. Возможные значения поля: 1-40. Значение по умолчанию: 2 узла.
- **IST Master** (Мастер IST). Указывает идентификатор мастера Internal Spanning Tree. IST Master (Мастер IST) - корень указанного экземпляра.
- **Instance ID** (Идентификатор экземпляра). Определяет экземпляр протокола MSTP. Диапазон значений поля: 0-15.
- **Included VLANs** (Включаемые VLAN). Привязка выбранных VLAN к выбранному экземпляру. Каждая сеть VLAN принадлежит одному экземпляру.
- **Bridge Priority (0-61440, in steps of 4096)** (Приоритет моста). Указывает приоритет устройства для выбора экземпляра протокола STP. Диапазон значений поля: 0-61440.
- **Designated Root Bridge ID** (Идентификатор назначенного корневого моста). Указывает идентификатор моста с самой низкой стоимостью пути к идентификатору экземпляра.
- **Root Port** (Корневой порт). Указывает корневой порт выбранного экземпляра.
- **Root Path Cost** (Стоимость пути к корю). Указывает стоимость пути выбранного экземпляра.

- **Bridge ID** (Идентификатор моста). Указывает идентификатор моста выбранного экземпляра.
- **Remaining Hops** (Осталось узлов). Указывает оставшееся число узлов до следующей сети назначения.

Отображение страницы MSTP Instance Table (Таблица экземпляров протокола MSTP)

1. Откройте страницу **MSTP Settings** (Параметры MSTP).
2. Нажмите кнопку **Show All** (Показать все), чтобы открыть страницу **MSTP Instance Table** (Таблица экземпляров протокола MSTP).

Рис. 7-37. MSTP Instance Table (Таблица экземпляров протокола MSTP)



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).

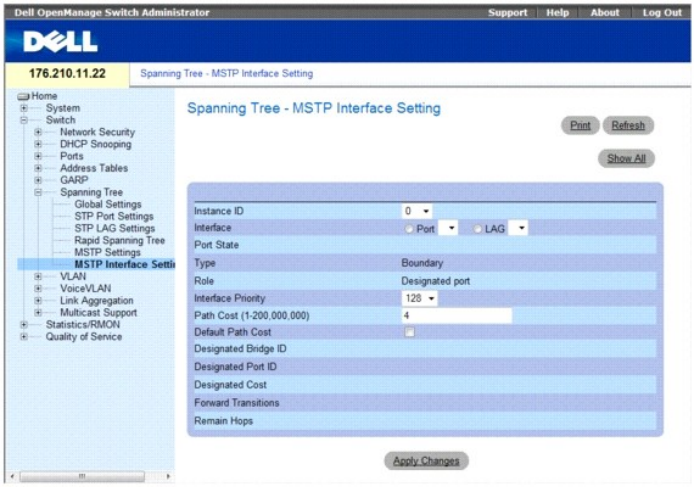
Таблица 7-23. Команды консоли для экземпляров MSTP

Команда консоли	Описание
spanning-tree mst configuration	Включает режим настройки MST.
instance *идентификатор_экземпляра* {**add** | **remove**} **vlan** *диапазон_vlan*	Привязывает VLAN к экземпляру MST.
name *строка*	Задает имя настройки.
revision *значение*	Задает номер версии настройки.
spanning-tree mst *идентификатор_экземпляра* **port-priority** *приоритет*	Устанавливает приоритет для порта.
spanning-tree mst *идентификатор_экземпляра* **priority** *приоритет*	Устанавливает приоритет устройства для указанного экземпляра протокола STP.
spanning-tree mst max-hops *число_узлов*	Устанавливает число узлов в области MST перед тем, как пакеты BPDU будут отброшены и срок хранения информации о порте истечет.
spanning-tree mst *идентификатор_экземпляра* стоимость *стоимость*	Устанавливает стоимость пути порта для вычислений MST.
exit	Выход из режима настройки области MST с сохранением изменений.
abort	Выход из режима настройки области MST без сохранения изменений.
show {**current** | **pending**}	Отображает текущую или незаконченную настройку области MST.

Определение параметров интерфейса MSTP

На странице **MSTP Interface Settings** (Параметры интерфейса MSTP) содержатся параметры, позволяющие назначить параметры MSTP для определенных интерфейсов. Чтобы открыть страницу **MSTP Interface Settings** (Параметры MSTP), выберите **Switch** (Коммутатор)→ **Spanning Tree** (Протокол STP)→ **MSTP Interface Settings** (Параметры интерфейса MSTP) на панели дерева.

Рис. 7-38. MSTP Interface Settings (Параметры интерфейса MSTP)



- **Instance ID** (Идентификатор экземпляра). Определяет группу VLAN, для которой назначен интерфейс. Возможные значения поля: 0-15.
- **Interface** (Интерфейс). Назначает порты или LAG для выбранного экземпляра MSTP.
- **Port State** (Состояние порта). Указывает, включен или выключен порт в определенном экземпляре.
- **Type** (Тип). Указывает, является ли порт для MSTP двухточечным или он подключен к концентратору, а также является ли порт внутренним для области MSTP или граничным. 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. Ниже указаны возможные значения:
  - **Root** (Корневой). Предоставляет путь с наименьшими затратами для пересылки пакетов в корневое устройство.
  - **Designated** (Назначенный). Указывает порт или группу LAG, с помощью которых назначенное устройство подключено к LAN.
  - **Alternate** (Альтернативный). Предлагает альтернативный путь к корневому устройству из корневого интерфейса.
  - **Backup** (Резервный). Предлагает резервный путь к указанному пути порта к «листьям» протокола STP. Резервные порты требуются только в том случае, когда два порта соединены в петлю с помощью соединения «точка-точка». Резервные порты также необходимы, когда LAN имеет два или более соединений к сегменту с общим доступом.
  - **Disabled** (Отключено). Указывает, что порт не участвует в соединении по протоколу STP.
- **Interface Priority (0-240 с шагом 16)** (Приоритет интерфейса). Определяет приоритет интерфейса для указанного экземпляра. Значение по умолчанию: 128.
- **Path Cost** (Стоимость пути). Указывает долю, которую порт вносит в стоимость корневого пути экземпляра протокола STP. Если выбран длинный метод стоимости пути на странице **STP Global Settings** (Общие параметры STP), значения поля могут быть в пределах от 1 до 200000000. Если выбран короткий метод стоимости пути, значения поля могут быть в пределах от 1 до 65535.
- **Default Path Cost (Стандартная стоимость пути)**— Iесли выбран длинный метод стоимости пути на странице **STP Global Settings** (Общие параметры STP), значения по умолчанию для стоимости пути могут быть следующими:
  - Ethernet (10 Мбит/с) - 2000000
  - Fast Ethernet (100 Мбит/с) - 200000
  - Gigabit Ethernet (1000 Мбит/с) - 20000
  - Порт-канал - 20000

Если выбран короткий метод стоимости пути, значения по умолчанию для стоимости пути могут быть следующими.

  - Ethernet (10 Мбит/с) - 100
  - Fast Ethernet (100 Мбит/с) - 19
  - Gigabit Ethernet (1000 Мбит/с) - 4
  - Порт-канал - 4

- **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.

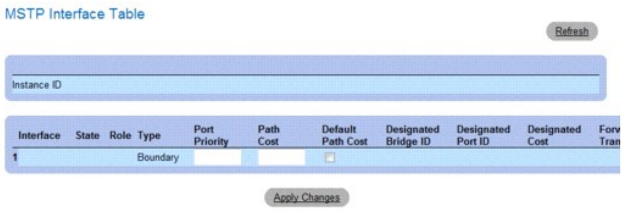
Просмотр страницы MSTP Interface Table (Таблица интерфейса MSTP)

1. Откройте страницу **MSTP Interface Settings** (Параметры интерфейса MSTP).

2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **MSTP Interface Table** (Таблица интерфейса MSTP) .

Рис. 7-39. Страница MSTP Interface Table (Таблица интерфейса MSTP)



Настройка сетей VLAN

VLAN - это логические подгруппы сети, созданные программным, а не аппаратным путем. Группы VLAN объединяют пользовательские станции и сетевые устройства в один домен 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 устройствам 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. Сети VLAN - это широковещательные и многоадресные домены. Широковещательный и многоадресный трафик передается только в той сети VLAN, где он создается.

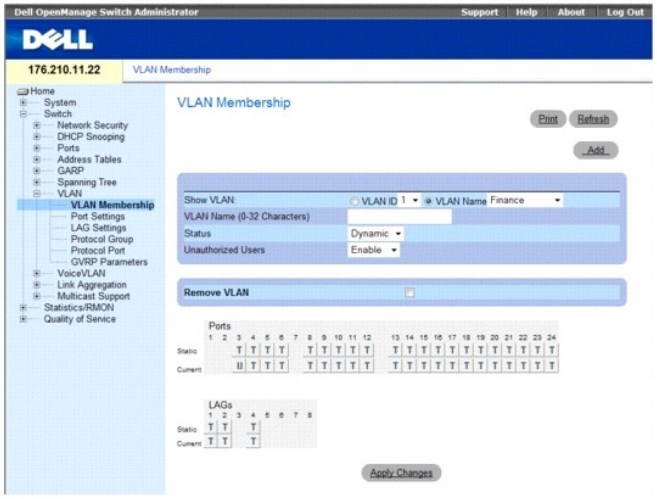
Маркировка сетей VLAN обеспечивает способ передачи информации VLAN между группами VLAN. При маркировке VLAN к заголовкам пакета присоединяется метка. Метка VLAN указывает, к какой сети VLAN принадлежит пакет. Метки VLAN присоединяются к пакету или конечной станцией, или сетевым устройством. Метки VLAN также содержат сведения о приоритете сетей VLAN. Объединение VLAN и GVRP обеспечивает автоматическое распределение данных VLAN. Чтобы открыть страницу **VLAN**, выберите **Switch** (Коммутатор)→ **VLAN** на панели дерева.

Маркировка пакетов QinQ позволяет сетевым администраторам добавлять дополнительные метки на предварительно помеченные пакеты. Клиентские сети VLAN настраиваются при использовании QinQ. Добавление дополнительных меток на пакеты помогает расширить пространство VLAN. Дополнительная метка является для каждого клиента идентификатором VLAN (VLAN ID), что обеспечивает частный характер сетевого трафика и его изолированность. Идентификатор VLAN ID назначается для порта клиента в сети поставщика услуг. Затем для назначенного порта предоставляются дополнительные услуги для пакетов с двойными метками. Это позволяет администраторам расширять обслуживание пользователей VLAN.

Определение членов сети VLAN

Страница **VLAN Membership** (Принадлежность VLAN) содержит поля для определения групп VLAN. Устройство поддерживает привязку идентификаторов VLAN 4094 к группам 256 VLAN. Все порты должны иметь определенный идентификатор PVID. Если не указано другое значение, то используется значение по умолчанию VLAN PVID. VLAN номер 1 - группа VLAN по умолчанию. Ее нельзя удалить из системы. Чтобы открыть страницу **VLAN Membership** (Принадлежность VLAN), выберите **Switch** (Коммутатор)→ **VLAN**→ **VLAN Membership** (Принадлежность VLAN) на панели дерева.

Рис. 7-40. Страница VLAN Membership (Принадлежность VLAN)



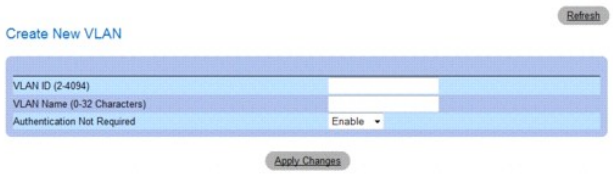
- **Show VLAN** (Отобразить VLAN). Выводит информацию по конкретной группе VLAN в соответствии с идентификатором VLAN или именем VLAN.
- **VLAN Name** (Имя сети VLAN). Имя сети VLAN, задаваемое пользователем.
- **Status** (Состояние). Тип VLAN. Возможные значения:
  - **Dynamic** (Динамическая). Показывает, что группа VLAN была динамически создана при использовании протокола GVRP.
  - **Static** (Статическая). Показывает, что группа VLAN определена пользователем.
  - **Default** (Стандартная). Показывает, что группа VLAN является стандартной.
- **Unauthorized Users** (Несанкционированные пользователи). Разрешает или запрещает несанкционированный доступ пользователей к группе VLAN.
- **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. Нажмите кнопку **Add** (Добавить).

   Откроется страница **Create New VLAN** (Создание новой VLAN).

   Рис. 7-41. 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).

   Выбранная группа VLAN будет удалена, а устройство будет обновлено.

Определение групп принадлежности VLAN с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для определения принадлежности групп VLAN, как показано на странице **VLAN Membership** (Принадлежность VLAN).

Таблица 7-24. 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)# vlan database

console(config-vlan)# vlan 1972

console(config-vlan)# exit

console(config)# interface vlan 1972

console(config-if)# name Marketing

console(config-if)# exit

console(config)#
```

Таблица принадлежности портов VLAN

Таблица портов VLAN содержит таблицу портов для назначения портов в группы VLAN. Принадлежность портов к VLAN определяется путем переключения параметров Port Control (Управление портом). Порты могут иметь следующие значения:

Таблица 7-25. Таблица принадлежности портов VLAN

Управление портом	Описание
T	Интерфейс входит в VLAN. Все пакеты, пересылаемые интерфейсом, помечаются. Пакеты содержат информацию о VLAN.
U	Интерфейс входит в VLAN. Пакеты, пересылаемые интерфейсом, не помечаются.
F	Интерфейсу отказано в принадлежности VLAN.
Blank	Интерфейс не входит в VLAN. Пакеты, связанные с интерфейсом, не пересылаются.

Таблица принадлежности портов **(VLAN Port Membership Table)** отображает порты и состояние портов, а также LAG. Порты, которые являются членами LAG, не будут отображаться в таблице VLAN Port Membership.

Назначение портов в группу VLAN

1. Откройте страницу **VLAN Membership** (Принадлежность VLAN).
2. Нажмите кнопку **VLAN ID** (Идентификатор VLAN) или **VLAN Name** (Имя VLAN) и выберите VLAN в раскрывающемся меню.
3. Выберите порт на странице **Port Membership Table** (Таблица портов сети VLAN) и назначьте значение для порта.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Порт будет назначен в группу VLAN, а устройство будет обновлено.

Удаление VLAN

1. Откройте страницу **VLAN Membership** (Принадлежность VLAN).
2. Нажмите кнопку **VLAN ID** (Идентификатор VLAN) или **VLAN Name** (Имя VLAN) и выберите VLAN в раскрывающемся меню.
3. Установите флажок **Remove VLAN** (Удалить VLAN).
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Выбранная группа VLAN будет удалена, а устройство будет обновлено.

Назначение портов в VLAN с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для назначения портов для групп VLAN.

Таблица 7-26. Команды консоли для назначения портов в группы VLAN

Команда консоли	Описание
switchport general acceptable-frame-types tagged-only	Отбрасывает входящие непомеченные кадры.
switchport forbidden vlan {**add** *список_сетей_vlan* | **remove** *список_сетей_ vlan*}	Запрещает добавление указанных VLAN для порта.
switchport mode {**customer** | **access** | **trunk** | **general**}	Настраивает режим принадлежности VLAN для порта.
switchport access vlan *идентификатор_vlan*	Настраивает идентификатор порта VLAN, если интерфейс работает в режиме доступа.
switchport trunk allowed vlan {**add** *список_сетей_vlan* | **remove** *список_сетей_vlan*}	Добавляет или удаляет группы VLAN из порта, работающего в режиме транк.
switchport trunk native vlan *идентификатор_vlan*	Определяет принадлежность порта к указанной группе VLAN, а также определяет идентификатор VLAN как «идентификатор VLAN по умолчанию для порта (PVID)».
switchport general allowed vlan add *список_сетей_vlan* [**tagged** | **untagged**]	Добавляет или удаляет группы VLAN из порта, работающего в общем режиме.
switchport general pvid идентифика **тор_vlan**	Настраивает идентификатор порта PVID, если интерфейс работает в общем режиме.

Далее приведен пример команд консоли.

```
Console (config)# vlan database

Console (config-vlan)# vlan 23-25

Console (config-vlan)# exit

Console (config)# interface vlan 23

Console (config-if)# name Marketing

Console (config-if)# exit

Console (config)# interface ethernet g8

Console (config-if)# switchport mode access

Console (config-if)# switchport access vlan 23
```

```
Console (config-if)# exit

Console (config)# interface ethernet g9

Console (config-if)# switchport mode trunk

Console (config-if)# swithport mode trunk allowed vlan
add 23-25



Console (config-if)# exit

Console (config)# interface ethernet g10

Console (config-if)# switchport mode general

Console (config-if)# switchport general allowed vlan add
23,25 tagged

Console (config-if)# switchport general pvid 25
```

В следующей таблице приведены эквивалентные команды консоли для настройки QinQ.

Команда консоли
Console> enable
Console#config
Console (config)#
Console (config)# vlan database
Console (config-vlan)# vlan 100
Console (config-vlan)# exit
Console (config)# interface ethernet e5
Console (config-if)# switchport mode customer
Console (config-if)# switchport customer vlan 100
Console (config-if)# exit
Console (config)# interface ethernet e10
Console (config-if)# switchport mode trunk
Console (config-if)# switchport trunk allowed vlan add 100
Console (config-if)# exit

Далее приведен пример команд настройки QinQ.

```
Console# show interfaces switchport ethernet
1/e5

Port: 1/e5

Port Mode: Customer

Gvrp Status: disabled

Ingress Filtering: true

Acceptable Frame Type: admitAll

Ingress UnTagged VLAN ( NATIVE ): 100

Protected: Disabled



Port is member in:
```

Vlan	Name	Egress rule	Port Membership Type
----	----------	----------	----------

100	100	Untagged	Static

Forbidden VLANS:

Vlan	Name
----	--------------------

Classification rules:

Protocol based VLANs:

Group ID	Vlan ID
--------	----------------

Mac based VLANs:

Group ID	Vlan ID
--------	----------------

Subnet based VLANs:

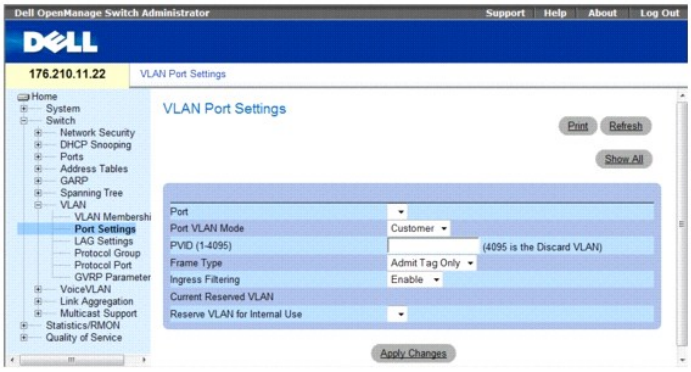
Group ID	Vlan ID
--------	----------------

Определение параметров портов VLAN

Страница **VLAN Port Settings** (Параметры VLAN для порта) содержит поля для управления портами, входящими в группу VLAN. Идентификатор Port Default VLAN ID (PVID) настраивается на странице **VLAN Port Settings** (Параметры VLAN для порта). Все непомеченные пакеты, поступающие на устройство, маркируются идентификатором PVID портов.

Чтобы открыть страницу **VLAN Port Settings** (Параметры VLAN для порта), выберите **Switch** (Коммутатор)→ **VLAN**→ **Port Settings** (Параметры порта) на панели дерева.

Рис. 7-42. Страница VLAN Port Settings (Параметры порта VLAN)



- **Port** (Порт). Номер порта, входящего в VLAN.
- **Port VLAN Mode** (Режим порта VLAN). 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, нельзя назначить. Невозможно включить или отключить входящий фильтр на порте доступа.
  - **Trunk** (Транк). Порты принадлежат группе VLAN, в которой все порты помечаются (кроме одного порта, который может остаться непомеченным).
  - **Customer** (Настраиваемый). Порт принадлежит к группе VLAN. Когда порт находится в режиме Customer (Настраиваемый), дополнительная метка является для каждого клиента идентификатором VLAN (VLAN ID), что обеспечивает частный характер сетевого трафика и его изолированность.
- **PVID (1-4095)**. Присваивает идентификатор VLAN непомеченным пакетам. Возможны следующие значения: 1-4094. VLAN 4095 определяется в соответствии со стандартом и принятой практикой в отрасли, как «discard VLAN». Пакеты, определенные в эту группу «Игнорируемая VLAN», опускаются.
- **Frame Type** (Тип кадра). Тип пакетов, принимаемый портом. Возможные значения:
  - **Admit Tag Only** (Разрешить только помеченные). Порт принимает только помеченные пакеты.

- **Admit All** (Разрешить все). Порт принимает и помеченные, и непомеченные пакеты.

- **Ingress Filtering** (Фильтрация на входе). Включает или отключает фильтрацию на входе для порта. При фильтрации на входе отклоняются пакеты, предназначенные для групп VLAN, к которым не принадлежит определенная группа LAG.
- **Current Reserve VLAN** (Текущая резервная группа VLAN). Группа VLAN в настоящее время выделенная системой в качестве резервной группы VLAN.
- **Reserve VLAN for Internal Use** (Резервная группа VLAN для внутреннего использования). Группа VLAN, выбранная пользователем в качестве резервной группы VLAN, если она не используется системой.

Назначение параметров порта

1. Откройте страницу **VLAN Port Settings** (Параметры VLAN для порта).
2. Выберите порт, для которого необходимо назначить параметры, в раскрывающемся списке **Port** (Порт).
3. Введите значения в необходимые поля
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Параметры порта VLAN будут определены, а устройство будет обновлено.

Отображение таблицы портов VLAN

1. Откройте страницу **VLAN Port Settings** (Параметры VLAN для порта).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **VLAN Port Table** (Таблица портов VLAN).

Рис. 7-43. VLAN Port Table (Таблица портов VLAN)

Назначение портов в VLAN с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для назначения портов для групп VLAN.

Таблица 7-28. Команды консоли для назначения портов в группы VLAN

Команда консоли	**Описание**
switchport mode {**customer** | **access** | **trunk** | **general**}	Настраивает режим принадлежности VLAN для порта.
switchport trunk native vlan *идентификатор_vlan*	Определяет принадлежность порт указанной группе VLAN, а идентификатор VLAN как «идентификатор VLAN по умолчанию для порта (PVID)».
switchport general pvid *идентификатор_vlan*	Настраивает идентификатор порта VLAN (PVID), если интерфейс работает в общем режиме.
switchport general allowed vlan add *список_сетей_vlan* [**tagged** | **untagged**]	Добавляет или удаляет группы VLAN из порта, работающего в общем режиме.
switchport general acceptable-frame-types tagged-only	Отбрасывает непомеченные входящие пакеты.
switchport general ingress-filtering disable	Отключает фильтрацию на входе для порта.
shutdown	Отключает интерфейсы.
set interface active {**ethernet** *интерфейс* | **port-channel** *номер_канала_порта*}	Вновь активизирует интерфейс, отключенный по причинам безопасности.

Далее приведен пример команд консоли.

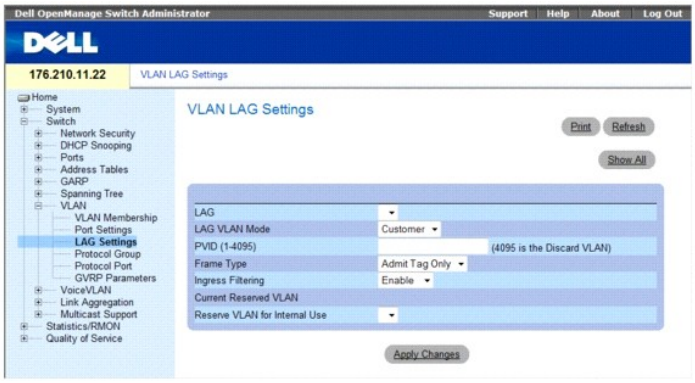
```
Console (config)# interface range ethernet g18 -20

Console (config-if)# switchport mode access
```

```
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 ingress-filtering disable
```

Определение параметров группы LAG группы VLAN

На странице **VLAN LAG Setting** (Параметры LAG для порта) приведены параметры для управления группами LAG, входящими в состав VLAN. Сети VLAN состоят из отдельных портов или групп LAG. Непомеченные пакеты, поступающие на устройство, помечаются с помощью идентификатора групп LAG в соответствии с идентификатором PVID. Чтобы открыть страницу **VLAN LAG Setting** (Параметры группы LAG сети VLAN), выберите **Switch** (Коммутатор) → **VLAN**→ **LAG Settings** (Параметры группы LAG) на панели дерева.

Рис. 7-44. Страница VLAN LAG Setting (Параметры группы LAG сети VLAN)



- **LAG**. Номер LAG, входящей в сеть VLAN.
- **LAG VLAN Mode** (Режим LAG VLAN). 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**. Присваивает идентификатор VLAN непомеченным пакетам. Возможные значения: 1-4095. VLAN 4095 определяется в соответствии со стандартом и принятой практикой в отрасли, как «discard VLAN». Пакеты, определенные в эту группу VLAN, опускаются.
- **Frame Type** (Тип кадра). Тип пакетов, принимаемый группой LAG. Возможные значения:
  - **Admit Tag Only** (Разрешить только помеченные). Группа LAG принимает только помеченные пакеты.
  - **Admit All** (Разрешить все). Группа LAG принимает и помеченные, и непомеченные пакеты.
- **Ingress Filtering** (Фильтрация на входе). Включает или отключает фильтрацию на входе для LAG. При фильтрации на входе отклоняются пакеты, предназначенные для групп VLAN, к которым не принадлежит определенный порт.
- **Current Reserve VLAN** (Текущая резервная группа VLAN). группа VLAN в настоящее время выделенная в качестве резервной группы VLAN.
- **Reserve VLAN for Internal Use** (Резервная группа VLAN для внутреннего использования). Группа VLAN, назначенная в качестве резервной группы VLAN после выполнения сброса устройства.

Назначение параметров группы LAG группы VLAN:

1. Откройте страницу **VLAN LAG Setting** (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 Setting** (Параметры группы LAG сети VLAN).

2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **VLAN LAG Table** (Таблица групп LAG для VLAN).

Назначение групп LAG в сети VLAN с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для назначения групп LAG для групп VLAN, как показано на странице **VLAN LAG Setting** (Параметры группы LAG VLAN).

Таблица 7-29. Команды консоли для назначения групп LAG VLAN

Команда консоли	Описание
switchport mode {**access	trunk	general**}	Настраивает режим принадлежности VLAN для порта.
switchport trunk native vlan *идентификатор_vlan*	Определяет принадлежность порт указанной группе VLAN и идентификатор VLAN как «идентификатор порта по умолчанию VLAN (PVID)».
switchport general pvid *идентификатор_vlan*	Настраивает идентификатор порта VLAN (PVID), если интерфейс работает в общем режиме.
switchport general allowed vlan add *список_сетей_vlan* [**tagged**	**untagged**]	Добавляет или удаляет группы VLAN из порта, работающего в общем режиме.
switchport general acceptable-frame-type tagged-only	Отбрасывает непомеченные входящие пакеты.
switchport general ingress-filtering disable	Отключает фильтрацию на входе для порта.

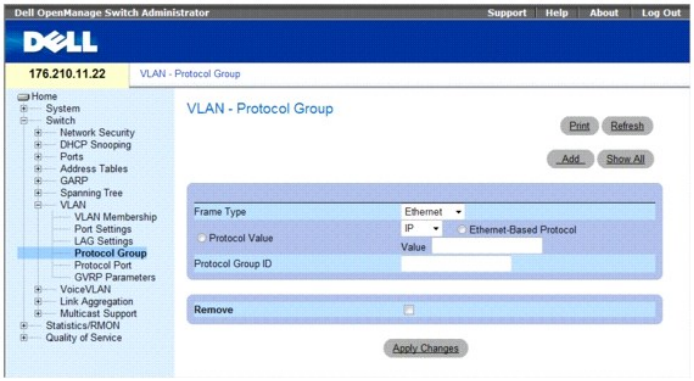
Далее приведен пример команд консоли.

```
console(config)# interface port-channel 1

console(config-if)# switchport mode access

console(config-if)# switchport access vlan 2

console(config-if)# exit



console(config)# interface port-channel 2

console(config-if)# switchport mode general

console(config-if)# switchport general allowed vlan add 2-3 tagged

console(config-if)# switchport general pvid 2

console(config-if)# switchport general acceptable-frame-type tagged-only

console(config-if)# switchport general ingress-filtering disable

console(config-if)# exit



console(config)# interface port-channel 3

console(config-if)# switchport mode trunk

console(config-if)# switchport trunk native vlan 3

console(config-if)# switchport trunk allowed vlan add 2

console(config-if)# exit
```

Определение групп протоколов VLAN

- На странице **Protocol Group** (Группа протокола) приведены параметры для настройки типов кадров для определенных групп протоколов. Чтобы открыть страницу **Protocol Group** (Группа протоколов), выберите **Switch** (Коммутатор)→ **VLAN**→ **Protocol Group** (Группа протоколов) на панели дерева.

Рис. 7-45. Страница Protocol Group (Группа протокола)



- **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. Допустимые значения поля: **IP**, **IPX** и **IPV6**.
- **Protocol Group ID** (Идентификатор группы протоколов). Номер идентификатора группы VLAN.
- **Remove** (Удалить). При установке этого флажка удаляется групповая привязка «кадр-протокол», если группа протоколов, которая должна быть удалена, не настроена на этом порту протокола.

Добавление группы протоколов

1. Откройте страницу **Protocol Group** (Группа протоколов).
2. Нажмите кнопку **Add** (Добавить).

   Откроется страница **Add Protocol to Group** (Добавить протокол в группу).
3. Заполните поля на этой странице.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Будет назначена группа протоколов, а устройство обновлено.

Назначение параметров группе протоколов VLAN

1. Откройте страницу **Protocol Group** (Группа протоколов).
2. Заполните поля на этой странице.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

   Параметры группы протоколов VLAN будут определены, а устройство обновлено.

Удаление протоколов из таблицы группы протоколов

1. Откройте страницу **Protocol Group** (Группа протоколов).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **Protocol Group Table** (Таблица группы протоколов).
3. Установите флажок **Remove** (Удалить) для тех групп протоколов, которые необходимо удалить.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Протокол будет удален, а устройство обновлено.

Определение групп протоколов VLAN с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для настройки групп протоколов.

Таблица 7-30. Команды консоли для определения групп протоколов VLAN

Команда консоли	Описание
map protocol *протокол [инкапсуляция]* **protocols-group** *группа*	Выполняет привязку протокола к группе протоколов. Группы протоколов используются для назначения группы VLAN, основанной на протоколах.

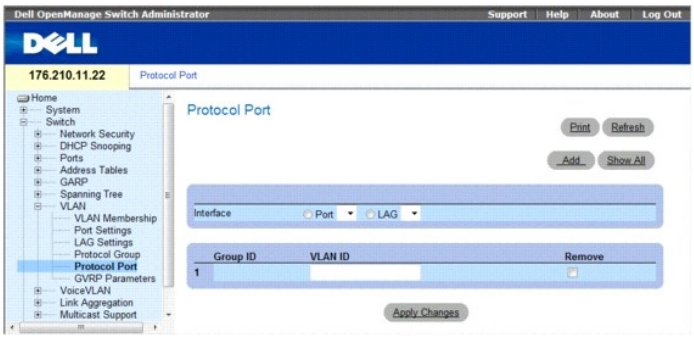
Следующий пример протокол ip-arp назначается для группы «213»:

```
Console (config)# vlan database

Console (config-vlan)# map protocol ip-arp protocols-group 213
```

Добавление 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. 7-46. Страница Protocol Port (Порт протокола)



- **Interface** (Интерфейс). Номер порта или группы LAG добавляемых в группу протоколов.
- **Group ID** (Идентификатор группы). Идентификатор группы протоколов, в которую добавляется интерфейс. Идентификатор группы протоколов определяется в таблице группы протоколов.
- **VLAN ID (1-4095)** (Идентификатор сети VLAN). Связывает интерфейс с определенным пользователем идентификатором VLAN. Идентификатор VLAN определяется на странице **Create a New VLAN** (Создание новой VLAN). Порт протокола может быть добавлен с использованием идентификатора VLAN или имени VLAN.

Добавление нового порта протокола

Порты протокола можно определить только на портах, которые определены как общие (**General**) на странице **VLAN Port Settings** (Параметры VLAN для порта).

1. Откройте страницу **Protocol Port** (Порт протокола).
2. Нажмите кнопку **Add** (Добавить).

   Откроется страница **Add Protocol Port** (Добавление порта протокола).
3. Введите значения в полях диалогового окна.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Новая группа протоколов VLAN будет добавлена в **Protocol Port Table** (Таблица группы протоколов), а устройство обновлено.

Определение портов протокола с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для определения портов протокола.

Таблица 7-31. Команды консоли для определения портов протокола

Команда консоли	Описание
switchport general map protocols-group *group* vlan *идентификатор_vlan*	Определяет правило классификации на основе протокола.

В следующем примере определяется правило классификации на основе протокола группы протоколов 1 для VLAN 8:

```
Console (config-if)# switchport general map protocols-group 1 vlan 8
```

Настройка 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 гарантировать правильную работу протокола GVRP, рекомендуется установить для максимального количества групп VLAN с протоколом GVRP значение, которое существенно больше суммы:

- количества всех статических групп VLAN, настроенных на данных момент или ожидающих настройки;
- количества всех динамических VLAN, входящих в протокол GVRP, настроенных на данных момент (начальное количество динамических сетей VLAN с протоколом GVRP равно 128) или ожидающих настройки.

Страница **GVRP Global Parameters** (Общие параметры GVRP) позволяет глобально включить GVRP. Протокол GVRP можно также включить для отдельных интерфейсов. Чтобы открыть страницу **GVRP Parameters** (Параметры GVRP), выберите **Switch** (Коммутатор)→ **VLAN**→ **GVRP Parameters** (Параметры GVRP) на панели дерева.

Рис. 7-47. Страница GVRP Parameters (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). 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 7-32. Команды консоли для настройки общих параметров протокола GVRP

Команда консоли	Описание
gvrp enable (global)	Включает протокол GVRP для системы в целом.
gvrp enable (interface)	Включает протокол GVRP для интерфейса.
gvrp vlan-creation-forbid	Включает или отключает динамическое создание VLAN.
gvrp registration-forbid	Отменяет регистрацию всех динамических сетей VLAN и предотвращает динамическую регистрацию VLAN для порта.
show gvrp configuration [**ethernet** *интерфейс* | **port-channel** *номер_канала_порта*]	Отображает сведения о конфигурации протокола GVRP, в том числе значения таймеров, разрешен ли протокол GVRP или динамическое создание сети VLAN, а также какие порты работают по протоколу GVRP.
show gvrp error-statistics [**ethernet** *интерфейс* | **port-channel** *номер_канала_порта*]	Отображает статистику ошибок протокола GVRP.
show gvrp statistics [**ethernet** *интерфейс* | **port-channel** *порт-канал-номер*]	Отображает статистику протокола GVRP.
clear gvrp statistics [**ethernet** *интерфейс* | **port-channel** *номер_канала_порта*]	Сбрасывает всю статистику протокола GVRP.

Далее приведен пример команд консоли.

```
console(config)# gvrp enable

console(config)# interface ethernet g1

console(config-if)# gvrp enable

console(config-if)# gvrp vlan-creation-forbid

console(config-if)# gvrp registration-forbid

console(config-if)# end

console# show gvrp configuration




GVRP Feature is currently Enabled on the device.

Maximum VLANs: 223
```

Port(s)	GVRP- Status	Registration	Dynamic VLAN Creation	Timers (milliseconds) Join	Leave	Leave All
-------	------	----------	--------	----------	-----	-----
g1	Enabled	Forbidden	Disabled	200	900	10000
g2	Disabled	Normal	Enabled	200	600	10000

Настройка голосовых сетей VLAN

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

Существуют два режима работы IP-телефонов:

- IP-телефон настраивается с поддержкой VLAN и обязательной пометкой пакетов при всех видах связи.
- При запрещенном режиме VLAN телефон будет использовать непомеченные пакеты. Телефон использует непомеченные пакеты во время получения начального IP-адреса через DHCP. Но затем телефон начинает использовать голосовую VLAN и посылает помеченные пакеты.

Раздел включает следующие темы:

- Страница определения параметров голосовой сети VLAN
- Определение параметров голосовой сети VLAN для порта
- Определение префиксов OUI

Определение общих параметров голосовой сети VLAN

Страница **Voice VLAN Global Parameters** (Общие параметры голосовой сети VLAN) содержит параметры которые применяются для всех голосовых VLAN на устройстве.

Чтобы открыть страницу **Voice VLAN Global Parameters** (Общие параметры голосовой сети VLAN) щелкните **Switch** (Коммутатор)→ **Voice VLAN** (Голосовая VLAN)→ **Global Parameters** (Общие параметры) на панели дерева.

Рис. 7-48. Страница Voice VLAN Global Parameters (Общие параметры голосовой сети VLAN)

- **Voice VLAN Status** (Состояние голосовой VLAN). Показывает, включена ли голосовая VLAN на устройстве. Ниже указаны возможные значения.
  - **Enable** (Включено). Включает голосовую VLAN на устройстве.
  - **Disable** (Отключено). Отключает голосовую VLAN на устройстве. Это значение по умолчанию.
- **Voice VLAN ID** (Идентификатор голосовой VLAN). Определяет идентификатор голосовой VLAN.
- **Class of Service** (Класс обслуживания). Включает добавление пометки CoS к непомеченным пакетам полученным в сети голосовой VLAN. Возможные значения от 0 до 7, где 0 означает наименьший приоритет, а 7 - высший.
- **Remark CoS** (Повторно пометить CoS). Повторно применить пометку CoS к пакетам полученным в сети голосовой VLAN. Возможные значения от 0 до 7, где 0 означает наименьший приоритет, а 7 - высший.
- **Voice VLAN Aging Time** (Срок действия голосовой VLAN). Указывает время, прошедшее с момента истечения срока действия последнего префикса OUI IP-телефона для указанного порта. Срок действия порта закончится после истечения срока действия связи и голоса. Время по умолчанию - один день. Формат поля - день:часы:минуты. Началом срока действия считается момент удаления MAC-адреса из таблицы «Dynamic MAC Address» (Динамические MAC-адреса) по истечении срока его действия. Время по умолчанию - 300 сек. Дополнительную информацию о сроке действия MAC-адресов см. в «Defining Aging Time» (Определение срока действия).

Configuring Voice VLAN Global Parameters (Настройка общих параметров голосовой сети VLAN):

1. Откройте страницу **Voice VLAN Global Parameters** (Общие параметры голосовой сети VLAN).

2. Заполните поля на этой странице.

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

   Общие параметры голосовой сети VLAN будут определены, а устройство обновлено.

Определение общих параметров голосовой сети VLAN с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для определения **Voice VLAN global parameters** (Общие параметры голосовой сети VLAN).

Таблица 7-33. Voice VLAN Global Parameters (Общие параметры голосовой сети VLAN) **Команды консоли**

Команда консоли	**Описание**
voice vlan id *vlan-id* **no voice vlan id**	Чтобы включить голосовую сеть VLAN и настроить идентификатор голосовой сети VLAN, используйте команду voice vlan id в режиме настройки общих параметров. Чтобы отключить голосовую сеть VLAN, используйте форму no этой команды.
voice vlan cos *cos* [**remark**] **no voice vlan cos**	Чтобы настроить класс обслуживания голосовой сети VLAN, используйте команду voice vlan cos в режиме настройки общих параметров. Чтобы восстановить значение по умолчанию, используйте форму no этой команды.
voice vlan aging-timeout *minutes* **no voice aging-timeout**	Чтобы установить тайм-аут срока использования голосовой VLAN, используйте команду voice vlan aging-timeout в режиме глобальной конфигурации. Чтобы восстановить значение по умолчанию, используйте форму no этой команды.
voice vlan enable	В режиме настройки интерфейса используйте команду voice vlan enable для включения автоматической настройки голосовой сети VLAN для порта. Чтобы отключить автоматическую настройку голосовой сети VLAN, используйте форму no этой команды.
show voice vlan [**ethernet** *interface* | **port-channel** *номер_порта-канала*]	В режиме EXEC используйте команду show voice vlan, чтобы отобразить состояние голосовой сети VLAN.

Далее приведен пример нескольких команд консоли.

Switch# show voice vlan Aging timeout: 1440 minutes OUI table			
MAC Address - Prefix	Description		
00:E0:BB	3COM		
00:03:6B	Cisco		
00:E0:75	Veritel		
00:D0:1E	Pingtel		
00:01:E3	Siemens		
00:60:B9	NEC/Philips		
00:0F:E2	Huawei-3COM		
Voice VLAN VLAN ID: 8 CoS: 6 Remark: Yes			
Interface	Enabled	Secure	Activated
------	------	------	------
g1	Yes	Yes	Yes
g2	Yes	Yes	Yes
g3	Yes	Yes	Yes
g4	Yes	Yes	Yes
g5	No	No	-
g6	No	No	-
g7	No	No	-
g8	No	No	-

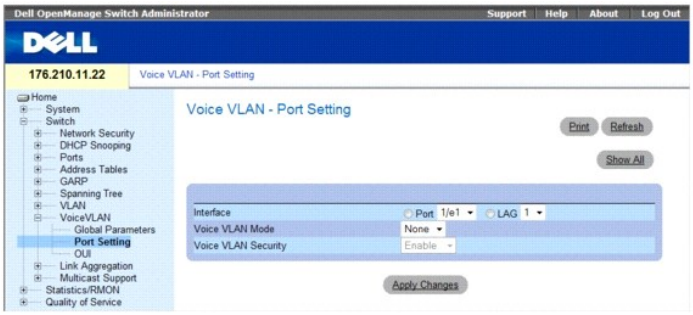
g9	No	No	-

Определение параметров голосовой сети VLAN для порта

Страница VLAN Port Settings (Параметры голосовой сети VLAN для порта) содержит поля для добавления портов или групп LAG в голосовую сеть VLAN.

Чтобы открыть страницу **Voice VLAN Port Setting** (Параметры голосовой сети VLAN для порта), щелкните **Switch** (Коммутатор)→ **Voice VLAN** (Голосовая сеть VLAN)→ **Port Setting** (Параметры порта) на панели дерева.

Рис. 7-49. Voice VLAN Port Setting (Параметры голосовой сети VLAN для порта)



- **Interface** (Интерфейс). Означает определенный порт или группу LAG, к которой применяются параметры голосовой сети VLAN.
- **Voice VLAN Mode** (Режим голосовой сети VLAN). Определяет режим голосовой сети VLAN. Ниже указаны возможные значения.
  - **None** (Нет). Выключает выбранный порт/группу LAG в голосовой сети VLAN.
  - **Static** (Статический). Поддерживает текущие параметры голосовой сети VLAN для порта/группы LAG. Это значение по умолчанию.
  - **Auto** (Авто). Означает, что если трафик с MAC-адресом IP-телефонов передается для порта/группы LAG, порт/группа LAG присоединяется к голосовой сети VLAN. Порт/группа LAG в голосовой сети VLAN устаревает, если MAC-адрес IP-телефонов (с префиксом OUI) устаревает и превышает заданное значение. Если префикс OUI MAC-адреса IP-телефонов был добавлен вручную для порта/группы LAG в голосовой сети VLAN, пользователь может добавить его в голосовую сеть VLAN только в ручном режиме, но не в режиме Auto (Авто).
- **Voice VLAN Port/LAG Security** (Безопасность портов/групп LAG голосовой сети VLAN). Означает, что безопасность портов/групп LAG в голосовой сети VLAN включена. Безопасность порта гарантирует, что пакеты, приходящие с нераспознанными префиксами OUI, отбрасываются.
  - **Enable** (Включено). Включение безопасности порта в голосовой сети VLAN.
  - **Disable** (Отключено). Отключение безопасности порта в голосовой сети VLAN. Это значение по умолчанию.

Настройка параметров порта

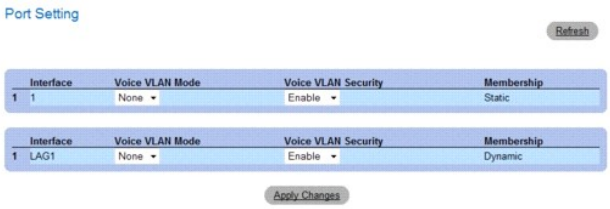
1. Откройте страницу **Voice VLAN Port Settings** (Параметры голосовой сети VLAN для порта).
2. Выберите порт или группу LAG.
3. Выполните необходимые изменения в полях.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Параметры будут изменены, а устройство обновлено.

Отображение таблицы параметров порта

1. Откройте страницу **Voice VLAN Port Settings** (Параметры голосовой сети VLAN для порта).
2. Нажмите кнопку **Show All** (Показать все). Откроется таблица параметров порта.

   Рис. 7-50. Таблица параметров голосовой сети VLAN для порта



В таблице параметров голосовой сети VLAN для порта имеется поле **Membership** (Принадлежность), в котором указывается, является элемент голосовой сети VLAN статическим или динамическим. Значение поля **Dynamic** (Динамическая) означает, что принадлежность VLAN была динамически создана при использовании протокола GARP. Значение поля **Static** (Статическая) показывает, что принадлежность VLAN определена пользователем.

3. Выполните необходимые изменения в полях.

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

Определение параметров голосовой сети VLAN для порта с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для определения параметров голосовой сети VLAN для порта.

Таблица 7-34. Команды консоли для определения параметров голосовой сети VLAN для порта

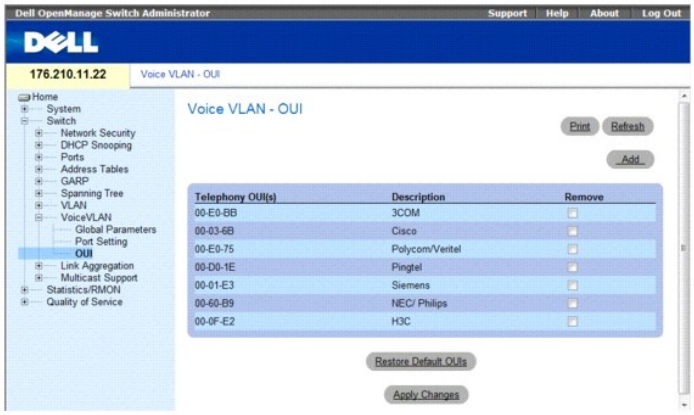
Команда консоли	Описание
voice vlan secure **no voice vlan secure**	Команда настройки интерфейса voice vlan secure используется для настройки режима безопасности для голосовой сети VLAN. Чтобы отключить режим безопасности, используйте форму no этой команды.

Определение префиксов OUI

На странице **Voice VLAN OUI** (Префикс OUI голосовой сети VLAN) перечисляются уникальные идентификаторы организации (OUI), относящиеся к голосовой сети VLAN. В первых трех байта MAC-адреса содержится идентификатор производителя. В последних трех байтах содержится уникальный идентификатор станции. Используя префиксы OUI, администраторы сети могут добавлять MAC-адреса определенных производителей в таблицу OUI. После добавления префиксов OUI весь трафик, полученный на портах голосовой сети VLAN со специального IP-телефона с указанным OUI, направляется в голосовую сеть VLAN.

Чтобы открыть страницу **Voice VLAN OUI** (Префикс OUI голосовой сети VLAN), щелкните **Switch** (Коммутатор)→ **Voice VLAN** (Голосовая сеть VLAN)→ **OUI** на панели дерева.

Рис. 7-51. Voice VLAN OUI (Префикс OUI голосовой сети VLAN)



- **Telephony OUI(s)** (Телефонные префиксы OUI). Перечислены префиксы OUI, которые в настоящий момент включены в голосовой сети VLAN. Следующие префиксы OUI включены по умолчанию:

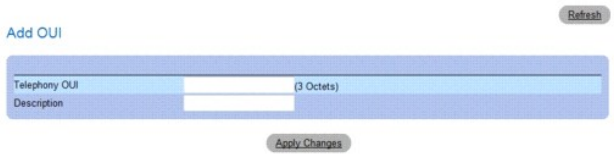
- 00-01-E3. Тедефон Siemens AG
- 00-03-6B. Телефон Cisco
- 00-0F-E2. Устройство H3C Aolynk
- 00-60-B9. Телефоны Philips и NEC AG
- 00-D0-1E. Телефон Pingtel
- 00-E0-75. Телефон Polycom/Veritel
- 00-E0-BB. Телефон 3COM

- **Description** (Описание). Предоставляет описание OUI размером до 32 символов.
- **Remove** (Удалить). Когда установлен этот флажок, удаляется префикс OUI из списка Telephony OUI (Телефонные префиксы OUI). Ниже указаны возможные значения.
  - **Checked** (Флажок установлен). Удаление выбранного префикса OUI.
  - **Unchecked** (Флажок снят). Оставляет текущий префикс OUI в списке Telephony OUI (Телефонные префиксы OUI). Это значение по умолчанию.
- **Restore Default OUIs** (Восстановить значения OUI по умолчанию). Восстанавливает значения OUI по умолчанию.

Добавление префиксов OUI

1. Откройте страницу **Voice VLAN OUI** (Префикс OUI голосовой сети VLAN).
2. Нажмите кнопку **Add** (Добавить). Откроется страница Add OUI (Добавление префикса OUI).

Рис. 7-52. Страница Voice VLAN Add OUI (Префикс OUI голосовой сети VLAN)



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

   Добавятся префиксы OUI.

Удаление префиксов OUI

1. Откройте страницу **Voice VLAN OUI** (Префикс OUI голосовой сети VLAN).
2. Установите флажок **Remove** (Удалить) рядом с префиксом OUI, который необходимо удалить.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

   Выбранные префиксы OUI будут удалены.

Восстановление префиксов OUI по умолчанию

1. Откройте страницу **Voice VLAN OUI** (Префикс OUI голосовой сети VLAN).
2. Щелкните **Restore Default OUIs** (Восстановить значения OUI по умолчанию).

   Префиксы OUI по умолчанию будут восстановлены.

Определение префиксов OUI голосовой сети VLAN с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для определения **Voice VLAN OUIs** (Префиксов OUI голосовой сети VLAN).

Таблица 7-35. Команды консоли для определения префиксов OUI голосовой сети VLAN

Команда консоли	Описание
voice vlan oui-table {**add** *префикс_mac-адреса* [**description** *текст*] | **remove** *префикс_mac-адреса*} **no voice vlan oui-table**	Чтобы настроить таблицу префиксов OUI голосовой сети, используйте команду voice vlan oui-table в режиме общей настройки. Чтобы восстановить значение по умолчанию, используйте форму no этой команды.

Объединение портов

Объединение портов оптимизирует использование портов, связывая между собой группу портов и формируя одну объединенную группу каналов (LAG). Объединение портов увеличивает пропускную способность между устройствами, увеличивает гибкость портов и обеспечивает избыточность каналов. Устройство поддерживает до восьми портов на каждую группу LAG и восьми групп LAG на каждое устройство.

Каждая группа LAG состоит из портов с одинаковой скоростью, работающих в дуплексном режиме. Порты в группе LAG могут быть разных типов (UTP/оптоволоконные и другие), но должны обеспечивать работу на одинаковой скорости.

Объединенные каналы можно назначить вручную или автоматически, включив протокол LACP (Link Aggregation Control Protocol) на соответствующих каналах. Устройство обеспечивает выравнивание нагрузки в группе LAG на основе MAC-адресов источника и MAC-адресов мест назначения.

Объединенные каналы рассматриваются системой как один логический порт. В частности, объединенный канал имеет атрибуты порта, аналогичные атрибутам необъединенного порта, включая автосогласование, скорость, настройки дуплексного режима и т.д.

Устройство поддерживает статические группы LAG и группы LAG с протоколом LACP. Группа LAG протокола LACP согласовывает объединенные каналы портов с LACP-портами других устройств. Если порты других устройств также являются LACP-портами, устройства формируют из них группу LAG.

При добавлении портов в группу LAG выполняйте следующие инструкции:

- Для порта не определен интерфейс уровня Layer 3.
- Порт не принадлежит ни одной группе VLAN.
- Порт не принадлежит ни одной другой группе LAG.
- Порт не является дублированным портом.
- Приоритет 802.1p порта равен приоритету 802.1p групп LAG.
- Режим доверия QoS не отключен на этом порте.
- Не включен протокол GVRP.

Порты могут быть сконфигурированы как LACP только в том случае, если они не являются частью предварительно настроенной группы LAG.

Устройство использует функцию хеширования, чтобы определить, какие кадры и по какой части объединенного канала передаются. Функция хеширования выравнивает статическую загрузку на компоненты объединенного канала. Устройство рассматривает объединенный канал как один логический порт.

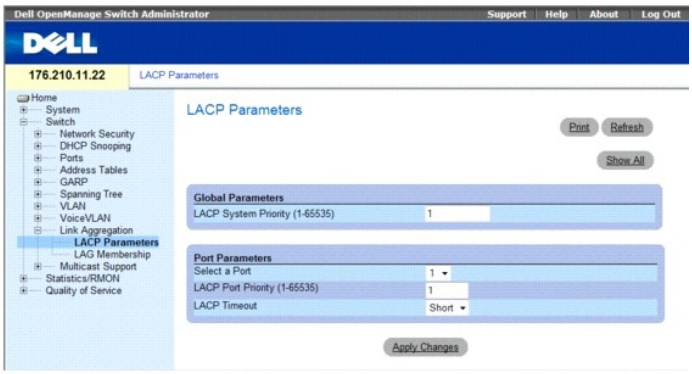
Каждый объединенный канал, включая порты Gigabit Ethernet, имеет тип порта объединенного канала. Порты могут быть добавлены в объединенный канал, только если они имеют одинаковый тип. Когда порты удаляются из объединенных портов, для них восстанавливаются первоначальные настройки. Чтобы открыть страницу **Link Aggregation** (Объединение каналов), выберите **Switch** (Коммутатор)→ **Link Aggregation** (Объединение каналов) на панели дерева.

Определение параметров протокола LACP

Страница **LACP Parameters** (Параметры LACP) содержит поля, позволяющие настроить группы LAG по протоколу LACP. Объединенные порты можно связать в группы портов объединенного канала. Каждая группа состоит из портов с одинаковой скоростью.

Объединенные каналы можно настроить вручную или установить автоматически, включив протокол LACP (Link Aggregation Control Protocol) на соответствующих каналах. Чтобы открыть страницу **LACP Parameters** (Параметры LACP), выберите **Switch** (Коммутатор)→ **Link Aggregation** (Объединение каналов)→ **LACP Parameters** (Параметры LACP) на панели дерева.

Рис. 7-53. Страница LACP Parameters (Параметры LACP)



- **LACP System Priority (1-65535)** (Приоритет системы LACP (1-65535)). Значение приоритета LACP для общих параметров. Возможные значения: от 1 до 65535. Значение по умолчанию: 1.
- **Select a Port** (Выбор порта). Номер порта, для которого назначены значения времени ожидания и приоритета.
- **LACP Port Priority (1-65535)** (Приоритет порта LACP (1-65535)). Значение приоритета LACP для порта.
- **LACP Timeout** (Тайм-аут LACP). Административный тайм-аут LACP. Ниже указаны возможные значения.
  - **Short** (Короткий). Определяет малое время ожидания.
  - **Long** (Длинный). Определяет большое время ожидания.

Определение общих параметров объединенных каналов

1. Откройте страницу **LACP Parameters** (Параметры LACP).
2. Укажите значение поля **LACP System Priority** (Приоритет системы LACP).
3. Нажмите кнопку **Apply Changes** (Применить изменения).

   Параметры будут определены, а устройство обновлено.

Определение параметров портов объединенного канала

1. Откройте страницу **LACP Parameters** (Параметры LACP).
2. Введите значения в полях в области **Port Parameters** (Параметры порта).
3. Нажмите кнопку **Apply Changes** (Применить изменения).

   Параметры будут определены, а устройство обновлено.

Отображение таблицы параметров LACP

1. Откройте страницу **LACP Parameters** (Параметры LACP).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется таблица параметров **LACP Parameters Table**.

Настройка параметров LACP с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для настройки параметров LACP, как показано на странице **LACP Parameters** (Параметры LACP).

Таблица 7-36. Команды консоли для настройки параметров LACP

Команда консоли	Описание
lacp system-priority *значение*	Настраивает приоритет системы.

lacp port-priority *значение*	Настраивает приоритет физических портов.
lacp timeout {**long** | **short**}	Задает административный тайм-аут LACP.
show lacp ethernet *интерфейс* [**parameters** | **statistics** | **protocol-state**]	Отображает информацию о протоколе LACP для порта Ethernet.

Далее приведен пример команд консоли.

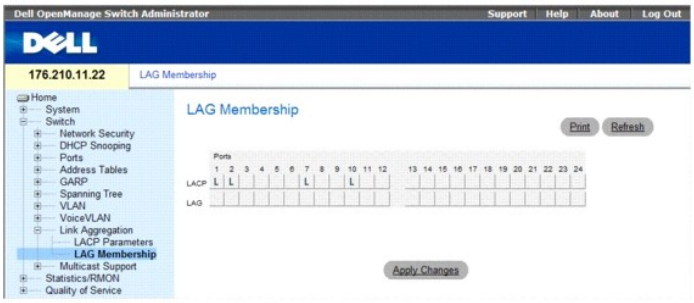
```
Console (config)# lacp system-priority 120

Console(config)# interface ethernet g1

Console (config-if)# lacp port-priority 247

Console (config-if)# lacp timeout long

Console(config-if)# end

Console# show lacp ethernet g1 statistics

Port g1 LACP Statistics:

LACP PDUs sent:2

LACP PDUs received:2
```

Определение принадлежности к группе LAG

Страница **LAG Membership** (Принадлежность LAG) содержит поля для назначения портов группам LAG. Группы LAG могут включать до 8 портов. Когда порт добавляется в LAG, он приобретает свойства LAG. Если невозможно настроить порт, используя свойства LAG, создается системное прерывание и порт работает с использованием своих настроек по умолчанию.

Страница **LAG Membership** (Принадлежность LAG) содержит поля для назначения портов группам LAG. Чтобы открыть страницу **LAG Membership** (Принадлежность LAG), выберите **Switch** (Коммутатор)→ **Link Aggregation** (Объединение каналов)→ **LAG Membership** (Принадлежность LAG) на панели дерева.

Рис. 7-54. Страница LAG Membership (Принадлежность LAG)



- **LACP**. Добавляет порт в группу LAG, используя протокол LACP.
- **LAG**. Добавляет порт в группу LAG и указывает LAG, к которой принадлежит порт.

Настройка принадлежности порта группе LAG или LACP

1. Откройте страницу **LAG Membership** (Принадлежность LAG).
2. В строке LAG (вторая строка) переключите кнопку на определенный номер, чтобы добавить или удалить порт из этого номера LAG.
3. В строке LACP (первая строка) переключите кнопку под номером порта, чтобы назначить либо LACP, либо статическую группу LAG.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Порт будет добавлен в группу LAG или LACP, а устройство обновлено.

Включение портов в группы LAG с помощью команд консоли

В следующей таблице приведены команды консоли, соответствующие полям для включения портов в группы LAG на странице **LAG Membership** (Принадлежность LAG).

Таблица 7-37. Команды консоли для определения принадлежности LAG

Команда консоли	Описание
interface port-channel *номер_канала_порта*	Включает режим настройки интерфейса для указанного канала-порта.
channel-group *номер_канала_порта* **mode** {**on** | **auto**}	Связывает порт с каналом порта. Для удаления конфигурации группы канала из интерфейса используйте форму по этой команды.
show interfaces port-channel [*номер_канала_порта*]	Отображает информацию о канале порта.

Далее приведен пример команд консоли.

```
console# config
console(config)# interface ethernet g1
console(config-if)# channel-group 1 mode on
console(config-if)# 01-Jan-2000 01:47:18 %LINK-W-Down: ch1

console(config-if)#
```

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.

Устройство поддерживает:

- **Forwarding L2 Multicast Packets** (Пересылка многоадресных пакетов L2). Включена по умолчанию и не настраивается.
- Система поддерживает фильтр многоадресной рассылки для 256 групп многоадресной рассылки.
- **Filtering L2 Multicast Packets** (Фильтрация многоадресных пакетов L2). Включает пересылку пакетов Layer 2 на интерфейсы. Если фильтрация многоадресного трафика отключена, многоадресные пакеты «лавиной» рассылаются на все соответствующие порты.

Чтобы открыть страницу **Multicast Support** (Поддержка многоадресного трафика), выберите **Switch** (Коммутатор)→ **Multicast Support** (Поддержка многоадресного трафика) на панели дерева.

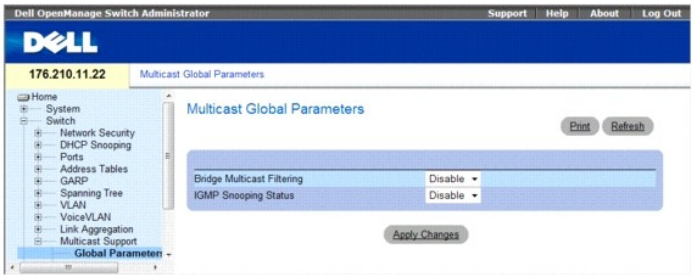
Определение общих параметров многоадресной передачи

Переключение Layer 2 пересылает многоадресные пакеты на все соответствующие порты VLAN по умолчанию, обрабатывая пакет как многоадресную передачу. Когда это работает, в том смысле, что все соответствующие порты или узлы получают копию кадра, это потенциально является неприемлемым, поскольку порты или узлы могут получать несоответствующие кадры, которые необходимы только для некоторого поднабора портов этой группы VLAN. Фильтр многоадресной пересылки позволяет выполнять пересылку пакетов Layer 2 на набор портов, определенных в базе данных фильтров многоадресной передачи.

Когда наблюдение на базе IGMP включено глобально для всей системы, при переключении ASIC запрограммирована пересылка всех пакетов IGMP 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, какие протоколы маршрутизации передают пакеты и многоадресный трафик. Порты, запрашивающие добавление в определенную группу многоадресной передачи, выдает отчет IGMP, в котором указана эта группа многоадресной передачи. В результате этого создается база данных фильтров многоадресной передачи.

Страница **Multicast Global Parameters** (Общие параметры передачи многоадресного трафика) содержит поля для включения наблюдения на базе протокола IGMP на устройстве. 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. 7-55. Страница Multicast Global Parameters (Общие параметры передачи многоадресного трафика)



- **Bridge Multicast Filtering** (Фильтрация многоадресного трафика через мост). Включает или отключает фильтрацию многоадресного трафика через мост. Значение по умолчанию: отключено. Наблюдение по протоколу IGMP можно включить только в том случае, если включена **фильтрация многоадресной передачи моста**.
- **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 Global Parameters** (Общие параметры передачи многоадресного трафика).

Таблица 7-38. Команды консоли для включения передачи многоадресного трафика и наблюдения на базе IGMP

Команда консоли	Описание
bridge multicast filtering	Включает фильтрацию многоадресных адресов.
ip igmp snooping	Включает наблюдение по протоколу IGMP.

Далее приведен пример команд консоли.

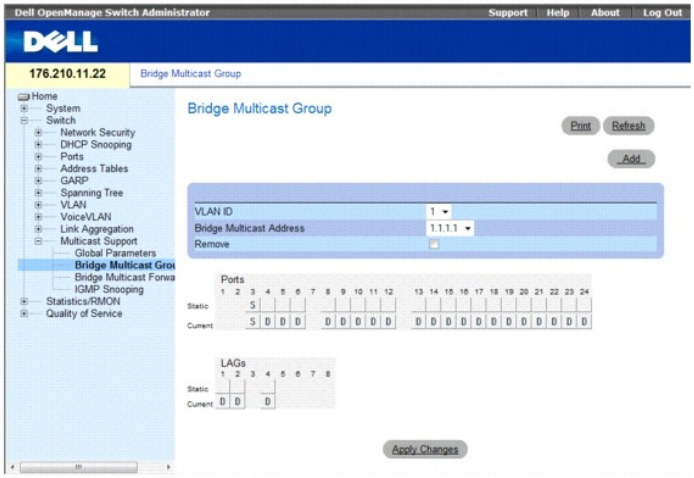
```
Console (config)# bridge multicast filtering

Console (config)# ip igmp snooping
```

Добавление записей адресов многоадресной передачи моста

На странице **Bridge Multicast Group** (Группа многоадресной передачи моста) показаны порты и группы LAG, связанные с группой службы многоадресной передачи, в таблицах **Ports** (Порт) и **LAG**. Таблицы Port и LAG также отражают принцип добавления порта или LAG в группу многоадресной передачи. Порты можно добавлять в существующую группу или в новые группы службы многоадресной передачи. Страница **Bridge Multicast Group** (Группа многоадресной передачи моста) позволяет создавать новые группы службы многоадресной передачи. На странице **Bridge Multicast Group** (Группа многоадресной передачи моста) также можно присвоить порты определенной группе многоадресной передачи.

Чтобы открыть страницу **Bridge Multicast Group** (Группа многоадресной передачи моста), выберите **Switch** (Коммутатор)→ **Multicast Support** (Поддержка многоадресного трафика)→ **Bridge Multicast Address** (Адрес многоадресной передачи моста) на панели дерева.

Рис. 7-56. 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:

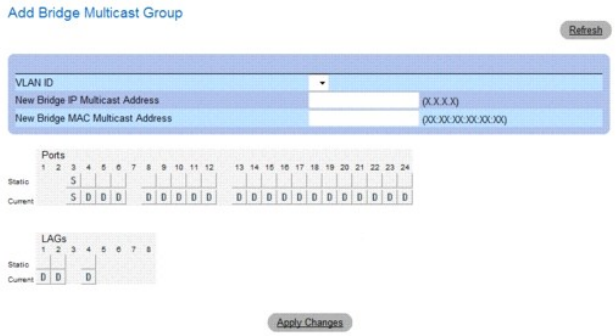
D	Показывает, что порт/группа LAG добавлена в группу многоадресной передачи динамически в строке *Current* (Текущий).
S	Связывает порт с многоадресной группой в качестве статического члена в строке *Static* (Статический). Порт/группа LAG присоединена к многоадресной группе статически в строке *Current* (Текущий).
F	Запрещено.
Пусто	Порт не связан с группой многоадресной передачи.

Добавление адресов многоадресной передачи моста

1. Откройте страницу **Bridge Multicast Group** (Группа многоадресной передачи моста).
2. Нажмите кнопку **Add** (Добавить).

   Откроется страница **Add Bridge Multicast Group** (Добавление группы многоадресной передачи моста).

   Рис. 7-57. Страница Add Bridge Multicast Group (Добавление группы многоадресной передачи моста)



3. Определите поля **VLAN ID** (Идентификатор VLAN) и **New Bridge Multicast Address** (Новый адрес многоадресной передачи моста).
4. Переключите порт на значение **S**, чтобы добавить его в выбранную группу многоадресной передачи.
5. Переключите порт на значение **F**, чтобы запретить добавление определенных адресов многоадресной передачи для определенного порта.

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

   Адрес многоадресной передачи моста будет добавлен в многоадресную группу, а устройство обновлено.

Определение портов для получения службы многоадресной пересылки

1. Откройте страницу **Bridge Multicast Group** (Группа многоадресной передачи моста).
2. Определите поля **VLAN ID** (Идентификатор VLAN) и **Bridge Multicast Address** (Адрес многоадресной передачи моста).
3. Переключите порт на значение **S**, чтобы добавить его в выбранную группу многоадресной передачи.
4. Переключите порт на значение **F**, чтобы запретить добавление определенных адресов многоадресной передачи для определенного порта.
5. Нажмите кнопку **Apply Changes** (Применить изменения).

   Порт будет назначен в группу многоадресной передачи, а устройство обновлено.

Назначение групп LAG для получения службы многоадресной пересылки

1. Откройте страницу **Bridge Multicast Group** (Группа многоадресной передачи моста).
2. Определите поля **VLAN ID** (Идентификатор VLAN) и **Bridge Multicast Address** (Адрес многоадресной передачи моста).
3. Переключите LAG на значение **S**, чтобы добавить его в выбранную группу многоадресной передачи.
4. Переключите LAG на значение **F**, чтобы запретить добавление определенных адресов многоадресной передачи для определенной группы LAG.
5. Нажмите кнопку **Apply Changes** (Применить изменения).

   Группа LAG будет назначена в группу многоадресной передачи, а устройство обновлено.

Управление записями службы многоадресной пересылки с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для управления записями службы многоадресной пересылки, как показано на странице **Bridge Multicast Group** (Группа многоадресной передачи моста).

Таблица 7-39. Команды консоли для управления записями службы многоадресной пересылки

Команда консоли	Описание
bridge multicast address {*mac_адрес_многоадресной_передачи* | *ip_адрес_многоадресной_передачи*}	Регистрирует адреса для многоадресной передачи на уровне MAC-адресов для таблицы мостов и добавляет в группу статические порты.
bridge multicast forbidden address {*mac_адрес_многоадресной_передачи* | *ip_адрес_многоадресной_передачи*}[**add** | **remove**] {**ethernet** *список_интерфейсов* | **port-channel** *список_номеров_каналов_портов*}	Запрещает добавление определенного адреса многоадресной передачи для определенных портов. Для возврата к значениям по умолчанию используйте форму no этой команды
show bridge multicast address-table [**vlan** *vlan-id*] [**address** *mac_адрес_многоадресной_передачи* | *ip_адрес_многоадресной_передачи*] [**format ip** | **mac**]	Отображает информацию таблицы MAC-адресов для многоадресной передачи.

Далее приведен пример команд консоли.

```
Console> enable

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)# exit

Console(config-if)# bridge multicast address 0100.5e02.0203

add ethernet g1,g2

Console(config-if)# exit

Console(config)# exit

Console # show bridge multicast address-table
```

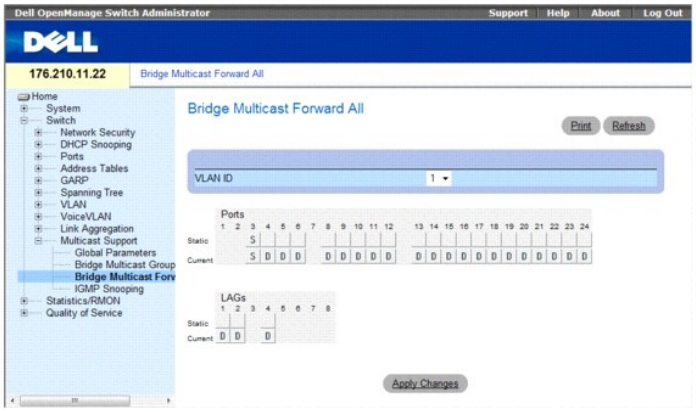
Vlan	MAC Address	Type	Ports
----	----------	-----	----------
1	0100.5e02.0203	static	g1, g2
19	0100.5e02.0208	static	g1-8
19	0100.5e02.0208	dynamic	g9-11
Forbidden ports for multicast addresses:			
Vlan	MAC Address	Ports	
----	----------	----------	
1	0100.5e02.0203	g8	
19	0100.5e02.0208	g8	
Console # **show bridge multicast address-table format ip**			
Vlan	IP Address	Type	Ports
----	----------	-----	----------
1	224-239.130 | 2.2.3	static	g1, g2
19	224-239.130 | 2.2.8	static	g1-8
19	224-239.130 | 2.2.8	dynamic	g9-11
Forbidden ports for multicast addresses:			
Vlan	IP Address	Ports	
----	----------	----------	
1	224-239.130 | 2.2.3	g8	
19	224-239.130 | 2.2.8	g8	

Назначение параметров многоадресной пересылки всем

Страница **Bridge Multicast Forward All** (Многоадресная передача моста всем) позволяет включить привязку портов или групп LAG к устройству, связанному с соседним маршрутизатором или коммутатором для многоадресной пересылки. После того как наблюдение по протоколу IGMP включено, многоадресные пакеты пересылаются соответствующему порту или группе VLAN.

Чтобы открыть страницу **Bridge Multicast Forward All** (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. 7-58. Страница Bridge Multicast Forward All (Многоадресная передача моста всем)



- **VLAN ID** (Идентификатор VLAN). Определяет VLAN.
- **Ports** (Порты). Порты, которые можно добавить в службу многоадресной передачи.
- **LAGs** (Группы LAG). Группы LAG, которые можно добавить в службу многоадресной передачи.

В таблице показаны установки для управления маршрутизатором и установки портов.

Управление портом	Описание
D	Связывает порт с многоадресным маршрутизатором или коммутатором как динамический порт.
S	Связывает порт с многоадресным маршрутизатором или коммутатором как статический порт.
F	Запрещено.
Пусто	Порт не подключен к маршрутизатору или коммутатору многоадресной передачи.

Привязка порта к маршрутизатору или коммутатору многоадресной передачи

1. Откройте страницу **Bridge Multicast Forward All** (Многоадресная передача моста всем).
2. Определите поле **VLAN ID** (Идентификатор VLAN).
3. Выберите порт в таблице **Ports** (Порты) и назначьте значение для порта.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Порт не подключен к маршрутизатору или коммутатору многоадресной передачи.

Привязка группы LAG к маршрутизатору или коммутатору многоадресной передачи

1. Откройте страницу **Bridge Multicast Forward All** (Многоадресная передача моста всем).
2. Определите поле **VLAN ID** (Идентификатор VLAN).
3. Выберите порт в таблице **LAGs** (Группы LAG) и укажите значение LAG.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Группа LAG привязывается к маршрутизатору или коммутатору многоадресной передачи.

Управление группами LAG и портами, связанными с маршрутизаторами многоадресной передачи с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для управления группами LAG и портами, привязанными к маршрутизаторам многоадресной передачи, как показано на странице **Bridge Multicast Forward All** (Многоадресная передача моста всем).

Таблица 7-40. Команды консоли для управления группами LAG и портами, привязанными к маршрутизаторам многоадресной передачи

Команда консоли	Описание
show bridge multicast filtering *идентификатор_vlan*	Отображает настройку фильтра многоадресной передачи.
no bridge multicast forbidden forward-all	Запрещает пересылку многоадресных пакетов для порта.
bridge multicast forward-all {**add** | **remove**} {**ethernet** *список_интерфейсов* | **port-channel** *список_номеров_каналов_портов*}	Разрешает пересылку всех многоадресных пакетов для порта. Для возврата к значениям по умолчанию используйте форму по этой команды

Далее приведен пример команд консоли.

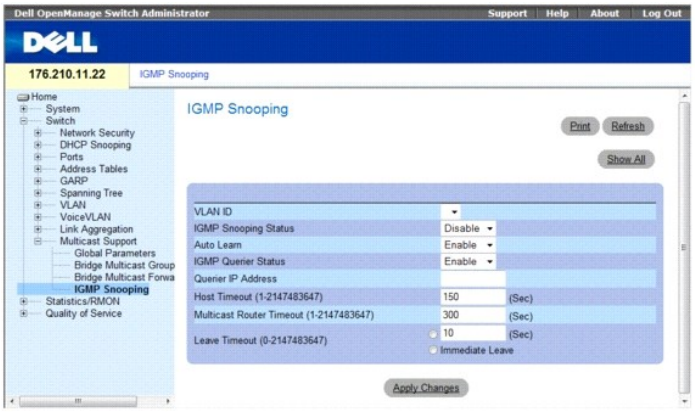
```
console(config)#vlan database

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-if)# exit

console(config)#interface vlan 8

Console(config-if)# bridge multicast address 0100.5e02.0203

add ethernet g1-9

Console(config-if)# exit

Console (config)# interface VLAN 1

Console (config-if)# bridge multicast forward-all add ethernet g8

Console(config-if)# end

Console # show bridge multicast filtering 1
```

Filtering: Enabled		
VLAN:	Forward-All	
Port	Static	Status
-------	-----------------	-----------
g1	Forbidden	Filter
g2	Forward	Forward(s)
g3	-	Forward(d)

Наблюдение по протоколу IGMP

Страница **IGMP Snooping** (Наблюдение по протоколу IGMP) содержит поля для добавления записей IGMP. Чтобы открыть страницу **IGMP Snooping** (Наблюдение по протоколу IGMP), выберите **Switch** (Коммутатор)→ **Multicast Support** (Поддержка многоадресного трафика)→ **IGMP Snooping** (Наблюдение по протоколу IGMP) на панели дерева.

Рис. 7-59. Страница IGMP Snooping (Наблюдение по протоколу IGMP)



- **VLAN ID** (Идентификатор сети VLAN). Указывает идентификатор VLAN.
- **IGMP Snooping Status** (Состояние наблюдения по протоколу IGMP). Включает или отключает наблюдение по протоколу IGMP для VLAN.
- **Auto Learn** (Автоматическое распознавание). Включает или отключает автоматическое распознавание на устройстве.
- **IGMP Querier Status** (Состояние опрашивающего устройства IGMP). Включает или отключает опрашивающее устройство IGMP. Опрашивающее устройство IGMP имитирует работу маршрутизатора многоадресной передачи, обеспечивая отслеживание многоадресного домена Layer 2 даже при отсутствии маршрутизатора многоадресной передачи.
- **Querier IP Address** (IP-адрес опрашивающего устройства). IP-адрес опрашивающего устройства. Используется, чтобы назначить использование адреса IP-интерфейса сети VLAN или определить уникальный IP-адрес, который будет использоваться в качестве адреса источника опрашивающего устройства.
- **Host Timeout (1-2147483647)** (Время ожидания хоста). Время, по истечении которого запись наблюдения по протоколу IGMP устаревает. Значение по умолчанию: 260 секунд.
- **Multicast Router Timeout (1-2147483647)** (Время ожидания многоадресного маршрутизатора). Время, по истечении которого запись многоадресного маршрутизатора устаревает. Значение по умолчанию: 300 секунд.
- **Leave Timeout (0-2147483647)** (Время старения). Время в секундах после получения сообщения портом и до истечения срока хранения. **User-defined** (Определено пользователем) позволяет определить интервал времени ожидания, а **Immediate Leave** (Немедленно) определяет время ожидания немедленного выхода. Значение по умолчанию: 10 секунд.

Включение на устройстве наблюдения на базе IGMP

1. Откройте страницу **IGMP Snooping** (Наблюдение по протоколу IGMP).
2. Выберите идентификатор VLAN для устройства, на котором будет включено наблюдение на базе протокола IGMP.
3. Выберите **Enable** (Включено) в поле **IGMP Snooping Status** (Состояние наблюдения на базе IGMP).
4. Заполните поля на этой странице.
5. Нажмите кнопку **Apply Changes** (Применить изменения).

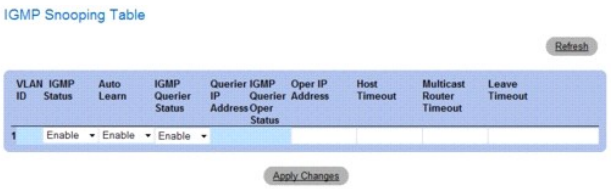
   Наблюдение на базе IGMP будет включено на этом устройстве.

Отображение таблицы наблюдения по протоколу IGMP

1. Откройте страницу **IGMP Snooping** (Наблюдение по протоколу IGMP).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **IGMP Snooping Table** (Таблица наблюдения по протоколу IGMP).

   Рис. 7-60. Таблица наблюдения по протоколу IGMP



Настройка наблюдения по протоколу IGMP с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для настройки на устройстве IGMP Snooping (Наблюдение по протоколу IGMP):

Таблица 7-41. Команды консоли для настройки наблюдения по протоколу IGMP

Команда консоли	Описание
ip igmp snooping	Включает наблюдение по протоколу IGMP.
ip igmp snooping mrouter learn-pim-dvmrp	Включает автоматическое распознавание портов многоадресного маршрутизатора в контексте определенной VLAN.
ip igmp snooping host-time-out *количество_секунд*	Настраивает время ожидания хоста.
ip igmp snooping mrouter-time-out *количество_секунд*	Настраивает время ожидания маршрутизатора.
ip igmp snooping leave-time-out {*количество_секунд* | *immediate-leave*}	Настраивает время старения хоста.
ip igmp snooping querier enable **no ip igmp snooping querier enable**	Включает опрашивающее устройство, использующее протокол управления группами Интернета (Internet Group Management Protocol (IGMP)) в конкретной VLAN. Чтобы отключить устройство, используйте форму по этой команды.
ip igmp snooping querier address *ip-адрес* **no ip igmp snooping querier address**	Определяет IP-адрес источника, который должен использоваться опрашивающим устройством, выполняющим наблюдение на базе протокола IGMP. Для возврата к значениям по умолчанию используйте форму по этой команды
show ip igmp snooping groups [**vlan** *идентификатор_vlan*] [**address** *ip_адрес_многоадресной_передачи*]	Отображает группы многоадресной передачи, полученные во время наблюдения по протоколу IGMP.
show ip igmp snooping interface *идентификатор_vlan*	Отображает конфигурацию наблюдения по протоколу IGMP.
show ip igmp snooping mrouter [**interface** *идентификатор_vlan*]	Отображает информацию о динамически распознаваемых интерфейсах многоадресного маршрутизатора.

Далее приведен пример команд консоли.

```
Console> enable

Console# config

Console (config)# ip igmp snooping

Console (config)# interface vlan 1

Console (config-if)# ip igmp snooping mrouter learn-pim-dvmrp

Console (config-if)# ip igmp snooping host-time-out 300

Console (config-if)# ip igmp snooping mrouter-time-out 200

Console (config-if)# exit

Console (config)# interface vlan 1

Console (config-if)# ip igmp snooping leave-time-out 60

Console (config-if)# exit

Console (config)# exit

Console # show ip igmp snooping groups

Vlan IP Address Querier Ports

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

1 224-239.130 | 2.2.3 Yes g1, g2

19 224-239.130 | 2.2.8 Yes g9-11
```

```
Console # show ip igmp snooping interface 1000

IGMP Snooping is globally enabled
```

```
IGMP Snooping admin: Enabled

Hosts and routers IGMP version: 2

IGMP snooping oper mode: Enabled

IGMP snooping querier admin: Enabled

IGMP snooping querier oper: Enabled

IGMP snooping querier address admin:

IGMP snooping querier address oper: 172.16.1.1

IGMP snooping querier version admin: 3

IGMP snooping querier version oper: 2




IGMP host timeout is 300 sec

IGMP Immediate leave is disabled. IGMP leave timeout is 10 sec

IGMP mrouter timeout is 300 sec

Automatic learning of multicast router ports is enabled



Console # show ip igmp snooping mrouter
```

VLAN	Ports
----	------
1	g1

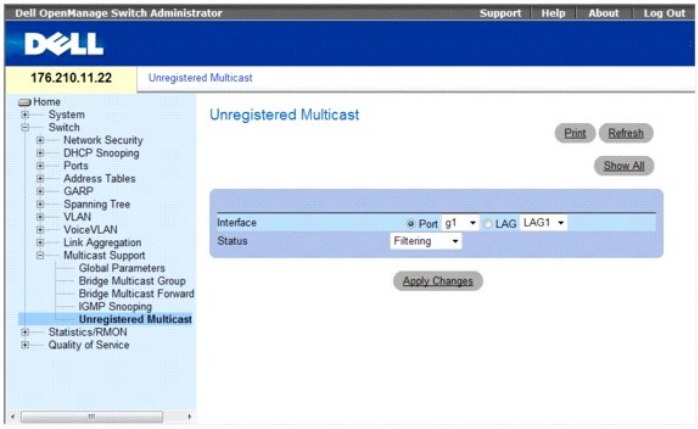
Незарегистрированная групповая передача

Кадры групповой (многоадресной) передачи обычно направляются на все порты VLAN. Если включен режим наблюдения по протоколу (IGMP Snooping), устройство получает информацию о наличии групп многоадресной передачи и проверяет, какие порты присоединились к этой группе многоадресной передачи. Группы многоадресной передачи могут также быть задействованы в статическом режиме. Это позволяет устройству направлять кадры многоадресной передачи (от зарегистрированной группы многоадресной передачи) только к портам, которые зарегистрированы в этой группе.

Страница **Unregistered Multicast** (Незарегистрированная многоадресная передача) содержит поля, которые предназначены для обработки кадров передачи, принадлежащих к незарегистрированным группам многоадресной передачи. Незарегистрированные группы многоадресной передачи - это группы, которые пока «неизвестны» устройству. Все кадры незарегистрированных групп по прежнему направляются на все порты VLAN. После установки для порта функции переадресации / фильтрации, конфигурация этого порта становится действительной для любой VLAN, членом которой он является (или будет являться).

Чтобы открыть страницу **Unregistered Multicast** (Незарегистрированная многоадресная передача), выберите **Switch** (Коммутатор)→ **Multicast Support** (Поддержка многоадресного трафика)→ **Unregistered Multicast** (Незарегистрированная многоадресная передача)на панели дерева.

Рис. 7-61. Незарегистрированная многоадресная передача



- **Interface** (Интерфейс). Позволяет осуществить выбор порта или группы LAG.
- **Status** (Состояние). Указывает состояние переадресации для выбранного интерфейса. Возможные значения:
  - **Forwarding** (Переадресация)**.** Обеспечивает переадресацию кадров незарегистрированного многоадресного трафика на указанный порт или канал порта. Это значение по умолчанию.
  - **Filtering** (Фильтрация). Обеспечивает отфильтровывание кадров незарегистрированного многоадресного трафика выбранного интерфейса VLAN.

Установки состояния незарегистрированного многоадресного трафика интерфейса

1. Откройте страницу **Unregistered Multicast** (Незарегистрированная многоадресная передача) .
2. Выберите интерфейс, для которого необходимо установить незарегистрированный многоадресный трафик.
3. В поле **Status** (Состояние) выберите состояние.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Состояние незарегистрированного многоадресного трафика установлено.

Отображается таблица незарегистрированного многоадресного трафика (Unregistered Multicast Table)

1. Откройте страницу **Unregistered Multicast** (Незарегистрированная многоадресная передача) .
2. Нажмите кнопку **Show All** (Показать все).

   Отображается таблица незарегистрированного многоадресного трафика (Unregistered Multicast Table)

Рис. 7-62. Таблица незарегистрированного многоадресного трафика

Копирование установок незарегистрированного многоадресного с одного интерфейса на другой

1. Откройте страницу **Unregistered Multicast** (Незарегистрированная многоадресная передача) .
2. Нажмите кнопку **Show All** (Показать все). Отображается таблица незарегистрированного многоадресного трафика (Unregistered Multicast Table)

3. Выберите интерфейс, из которого необходимо копировать параметры, в поле **Copy Parameters from** (Копировать параметры из).

4. Для каждого из интерфейсов, в который вы хотите скопировать параметры, установите галочку в клетке поля **Copy to** (Копировать в). В противном случае, выберите **Select All** (Выбрать все) для автоматического выбора всех интерфейсов.

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

   Параметры незарегистрированного многоадресного трафика скопированы с одного интерфейса на другой.

Настройка незарегистрированного многоадресного трафика командами консоли

В следующей таблице приведены эквивалентные команды консоли для настройки незарегистрированного многоадресного трафика на устройстве:

Таблица 7-42. Команды консоли для незарегистрированного многоадресного трафика

Команда консоли	Описание
bridge multicast unregistered (Незарегистрированная мостовая многоадресная передача)	Настраивает состоение переадресации незарегистрированных адресов многоадресного трафика.
show bridge multicast unregistered (Показать незарегистрированные мостовые передачи)	Отображает настройку фильтра незарегистрированной мостовой передачи.

Далее приведен пример команд консоли.

```
Console # show bridge multicast unregistered


Port Unregistered

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

g1   Forward

g2   Filter

g3   Filter
```

Назад на страницу «Содержание»:

Назад на страницу содержания

Информация о настройке системы

Руководство пользователя систем Dell™ PowerConnect™ 54xx

В этом разделе содержатся инструкции для определения параметров системы, включая функции безопасности, загрузку программного обеспечения и восстановление заводских параметров устройства. Чтобы открыть страницу **System** (Система), на панели дерева выберите **System** (Система).

Рис. 6-1. Система

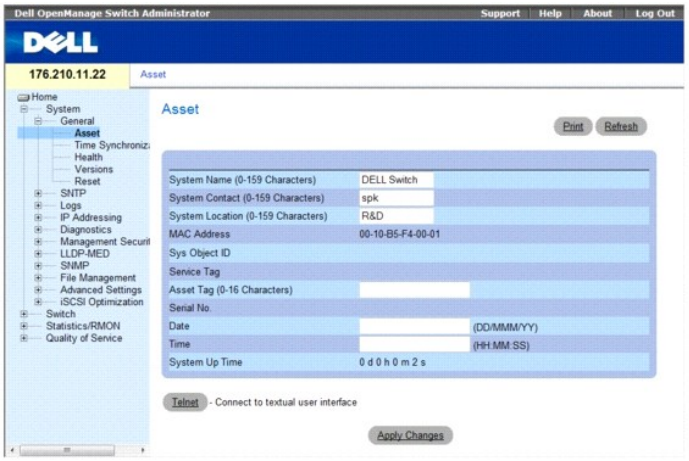
Определение общих сведений об устройстве

Страница **General** (Общее) содержит ссылки на страницы, позволяющие настраивать параметры устройства.

Просмотр сведений об устройстве

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

Рис. 6-2. Ресурсы



- **System Name (0-159 Characters) (Имя системы (0-159 символов)).** Определенное пользователем имя устройства.
- **System Contact (0-159 Characters) (Контактное лицо системы (0-159 символов)).** Указывает имя контактного лица.
- **System Location (0-159 Characters) (Местоположение системы (0-159 символов)).** Определяет место, где работает система.

- **MAC Address (MAC-адрес).** определяет MAC-адрес устройства.
- **Sys Object ID (Системный идентификатор объекта).** определяет утвержденный поставщиком идентификатор подсистемы сетевого управления, содержащийся в объекте.
- **Service Tag (Метка производителя).** определяет справочный номер, используемый при обслуживании устройства.
- **Asset Tag (0-16 Characters) (Метка ресурса (от 0 до 16 символов)).** определяет ссылку на устройство, задаваемую пользователем.
- **Serial No. (Серийный номер).** определяет серийный номер устройства.
- **Date (DD/MMM/YY) (Дата (ММ/ДД/ГГ).** определяет текущую дату. Формат этого поля: месяц, день, год. Например, 10/NOV/02 соответствует 10 ноября 2002 года.
- **Time (HH:MM:SS) (Время (ЧЧ:ММ:СС)).** определяет системное время. Формат времени: час, минуты, секунды; например: 20:12:03 означает восемь часов двенадцать минут и три секунды вечера.
- **System Up Time (Время работы системы).** показывает, сколько времени прошло с момента последней перезагрузки системы. Формат отображения системного времени: дни, часы, минуты и секунды. Например, 41 день 2 часа 22 минуты 15 секунд.

Определение сведений о системе:

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

   Системные параметры будут определены, а устройство обновлено.

Запуск сеанса Telnet:

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

   Будет запущен сеанс Telnet.

Настройка сведений об устройстве с помощью команд консоли

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

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

Далее приведен пример команд консоли.

```
Console (config)# hostname dell

Console (config)# snmp-server contact Dell_Tech_Supp

Console (config)# snmp-server location New_York

Console(config)# exit

Console# exit

Console (config)# asset-tag 1qwepot

Console> clock set 13:32:00 7 Dec 2004
```

```
Console> show clock

13:32:00 (UTC+0) Dec 7 2004

No time source
```

```
DELL Switch# show system

System Description:                 Kenan 24
System Up Time (days,hour:min:sec): 0,00:04:17
System Contact:                     spk
System Name:                        RS1
System Location:                    R&D
System MAC Address:                 00:10:b5:f4:00:01
Sys Object ID:                      1.3.6.1.4.1.674.10895.3000

Type:                               PowerConnect 5400
Main Power Supply Status ok

Redundant Power Supply Status: OK

Fan 1 Status: OK
Fan 2 Status: OK
```

Определение параметров системного времени

Страница **Time Synchronization** (Синхронизация по времени) содержит поля для определения параметров системного времени для часов локального оборудования и внешних часов SNTP. Если управление системным временем осуществляется по внешним часам SNTP, то случае сбоя внешних часов SNTP в качестве системного времени используется время по часам локального оборудования. На устройстве можно включить переход на летнее время. Следующий список содержит начало и конец периода летнего времени для определенных стран:

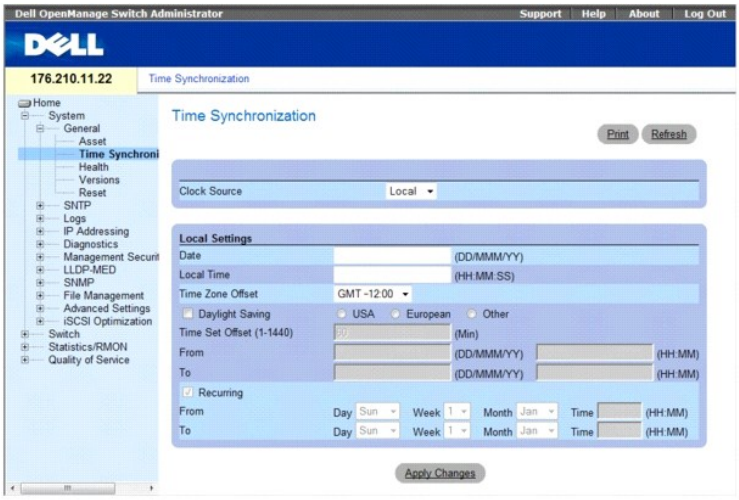
- **Албания.** с последних выходных марта по последние выходные октября.
- **Австралия.** с конца октября по конец марта.
- **Австралия** - **Тасмания.** с начала октября по конец марта.
- **Армения.** с последних выходных марта по последние выходные октября.
- **Австрия.** с последних выходных марта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

- **Ирак.** с 1-го апреля по 1-е октября.
- **Ирландия.** с последних выходных марта по последние выходные октября.
- **Израиль.** в разные годы по-разному.
- **Италия.** с последних выходных марта по последние выходные октября.
- **Япония.** Япония не переходит на летнее время.
- **Иордания.** с последних выходных марта по последние выходные октября.
- **Латвия.** с последних выходных марта по последние выходные октября.
- **Ливан.** с последнего воскресенья марта по последнее воскресенье октября.
- **Литва.** с последних выходных марта по последние выходные октября.
- **Люксембург.** с последних выходных марта по последние выходные октября.
- **Македония.** с последних выходных марта по последние выходные октября.
- **Мексика.** с первого воскресенья апреля в 02:00 по последнее воскресенье октября в 02:00.
- **Молдавия.** с последних выходных марта по последние выходные октября.
- **Черногория.** с последних выходных марта по последние выходные октября.
- **Нидерланды.** с последних выходных марта по последние выходные октября.
- **Новая Зеландия.** с первого воскресенья октября по первое воскресенье 15-го марта или после этой даты.
- **Норвегия.** с последних выходных марта по последние выходные октября.
- **Парагвай.** с 6-го апреля по 7-е сентября.
- **Польша.** с последних выходных марта по последние выходные октября.
- **Португалия.** с последних выходных марта по последние выходные октября.
- **Румыния.** с последних выходных марта по последние выходные октября.
- **Россия.** с 29-го марта по 25-е октября.
- **Сербия.** с последних выходных марта по последние выходные октября.
- **Словацкая республика.** с последних выходных марта по последние выходные октября.
- **ЮАР.** ЮАР не переходит на летнее время.
- **Испания.** с последних выходных марта по последние выходные октября.
- **Швеция.** с последних выходных марта по последние выходные октября.
- **Швейцария.** с последних выходных марта по последние выходные октября.
- **Сирия.** с 31-го марта по 30-е октября.
- **Тайвань.** Тайвань не переходит на летнее время.
- **Турция.** с последних выходных марта по последние выходные октября.
- **Великобритания.** с последних выходных марта по последние выходные октября.
- **США.** со второго воскресенья марта в 02:00 по первое воскресенье ноября в 02:00.

Дополнительную информацию о протоколе SNTP см. в разделе Настройка параметров SNTP.

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

Рис. 6-3. Синхронизация по времени



- **Clock Source (Источник синхронизации).** источник, используемый для установки системных часов. Возможные значения:
  - **SNTP.** определяет, что системное время будет установлено через сервер SNTP. Дополнительную информацию см. в разделе Configuring SNTP Settings (Настройка параметров SNTP).
  - **None (Нет).** определяет, что системное время не устанавливается с помощью внешнего источника.

Local Settings (Локальные настройки)

- **Date (Дата).** определяет системную дату. Формат поля даты: день:месяц:год, например, 04 мая 2050.
- **Local Time (Локальное время).** определяет системное время. Формат поля ЧЧ:ММ:СС, например, 21:15:03.
- **Time Zone Offset (Смещение часового пояса).** разница между временем по Гринвичу (GMT) и местным временем. Например, смещение часового пояса для Парижа - GMT +1, а локальное время в Нью-Йорке - GMT -5.
- Существуют два типа параметров перехода на летнее время: в определенный день в определенный год или в один день каждый год. Чтобы определить параметр перехода в определенный год, укажите значение в области **Daylight Savings** (Переход на летнее время). Чтобы настроить ежегодный переход введите значение в области **Recurring** (Повторяющийся).
- **Daylight Savings (Летнее время).** включает переход на летнее время на устройстве в зависимости от его местоположения. Возможные значения:

  USA (США). устройство переключается на летнее время в 2 часа ночи во второе воскресенье марта, а на стандартное время - в 2 часа ночи в первое воскресенье ноября.

  European (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. Параметр *European* (Европейское) применяется для членов Европейского Союза и других стран Европы, использующих стандарты Европейского Союза.

  Other (Другое). переход на летнее время определяется пользователем на основе местоположения устройства. Если выбран параметр Other (Другое), то должны быть определены поля **From** (С) и **To** (По).

- **From (С).** определяет время перехода на летнее время для всех стран, кроме США и стран Европы. Формат: ДеньМесяцГод в одном поле и время в другом поле. Например, если переход на летнее время должен быть выполнен 25 октября 2007 года в 5:00 утра, в поля необходимо ввести следующие значения: 25Oct07 и 5:00. Возможные значения:
  - **Date (Дата).** дата, когда выполняется переход на летнее время. Возможные значения поля: 1-31.
  - **Month (Месяц).** месяц, с которого начинается переход к летнему времени. Возможные значения поля: Jan-Dec (Янв-Дек).
  - **Year (Год).** год, для которого настраивается переход на летнее время.
  - **Time (Время).** время, когда выполняется переход на летнее время. Формат поля часы:минуты, например, 05:30.
- **To (По).** определяет окончание действия летнего времени для стран отличных от США и Европы. Формат: ДеньМесяцГод в одном поле и время в другом поле. Например, если действие летнего времени должно закончится 23 марта 2008 года в 12:00, в поля необходимо ввести следующие значения: 23Mar08 и 12:00. Возможные значения:
  - **Date (Дата).** дата окончания действия летнего времени. Возможные значения поля: 1-31.
  - **Month (Месяц).** месяц окончания действия летнего времени. Возможные значения поля: Jan-Dec (Янв-Дек).
  - **Year (Год).** год, для которого настраивается окончание действия летнего времени.
  - **Time (Время).** время окончания действия летнего времени. Формат поля часы:минуты, например, 05:30.
- **Recurring (Повторение).** определяет время перехода на летнее время для всех стран, кроме США и стран Европы, в которых переход на летнее время повторяется каждый год. Возможные значения:
- **From (С).** определяет время перехода на летнее время каждый год. Например, переход на летнее время выполняется во вторую субботу апреля в 5:00. Возможные значения:
  - **Day (День).** день недели, в который каждый год выполняется переход на летнее время. Возможные значения поля: Sunday-Saturday (Воскресенье-Суббота).
  - **Week (Неделя).** неделя месяца, течение которой каждый год выполняется переход на летнее время. Возможные значения поля: 1-5.

- **Month (Месяц).** месяц года, в течение которого каждый год осуществляется переход на летнее время. Возможные значения поля: Jan-Dec (Янв-Дек).
- **Time (Время).** время, когда каждый год осуществляется переход на летнее время. Формат поля - «часы:минуты», например, 02:10.

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

Выбор источника синхронизации

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

   Будет выбран источник синхронизации, а устройство обновлено.

Определение параметров локальных часов

1. Откройте страницу **Time Synchronization** (Синхронизация по времени).
2. Укажите значение для полей **Recurring** (Повторение).
3. Нажмите кнопку **Apply Changes** (Применить изменения).

   Будут использоваться локальные часы.

Определение параметров внешних часов SNTP

1. Откройте страницу **Time Synchronization** (Синхронизация по времени).
2. Укажите значение для полей.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

   Будут изменены параметры внешних часов.

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 определения параметров часов

Консоль	**Описание**
clock source {**sntp**}	Определяет внешний источник времени для системных часов.
clock timezone *разница_в_часах* [**minutes** *разница_в_минутах*][**zone** *сокращение*]	Устанавливает часовой пояс для отображения.
clock summer-time	Настраивает в системе автоматическое переключение на летнее время.
clock summer-time recurring {**usa** | **eu** | {*день недели месяц чч:мм день недели месяц чч:мм*}} [**offset** *разница*] [**zone** *сокращение*]	Настраивает систему для автоматического переключения на летнее время (в соответствии со стандартами США и Европы).
clock summer-time date *дата месяц год чч:мм дата месяц год чч:мм* [**offset** *разница*] [**zone** *сокращение*]	Настраивает систему для автоматического переключения на летнее время для указанного периода в формате день/месяц/год.

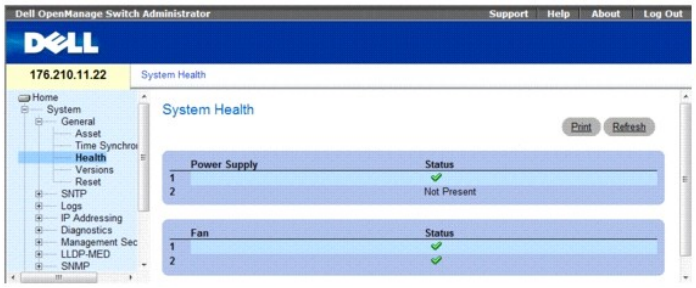
Далее приведен пример команд консоли.

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

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

Просмотр сведений о состоянии системы

На странице **System Health** (Состояние системы) отображается информация о физических параметрах устройства. Чтобы открыть страницу **System Health** (Состояние системы), на панели дерева выберите **System** (Система)→ **General** (Общие)→ **Health** (Состояние).

Рис. 6-4. Состояние системы



- **Power Supply Status (Состояние источника питания).** отображается состояние основного источника питания. Возможные значения:
  - . основной источник питания устройства работает нормально
  - . основной источник питания устройства работает неправильно.
  - **Not Present (Не установлен).** источник питания не установлен для указанного устройства.
- **Fan (Вентилятор).** состояние вентилятора устройства. Возможные значения:
  - . вентиляторы устройства работают нормально.
  - . вентиляторы устройства работают неправильно.
  - **Not Present (Не установлены).** вентиляторы не установлены для указанного 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 относительно состояния системы

Команда консоли	**Описание**
show system (показать состояние системы)	Отображает информацию о системе.

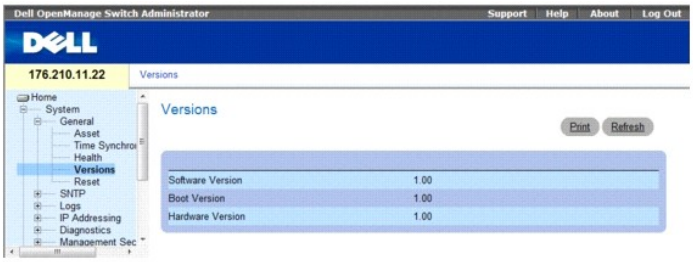
```
DELL Switch# show system
System Description:                 Ethernet Routing Switch
System Up Time (days,hour:min:sec): 0,00:04:17
System Contact:                     spk
System Name:                        DELL Switch
System Location:                    R&D
System MAC Address:                 00:10:b5:f4:00:01
Sys Object ID:                      1.3.6.1.4.1.674.10895.3000
Type: PowerConnect 5400

Power Supply                        Status
-------------                       --------
Main                                OK
```

Redundant	OK	
FAN	Status	
----------	--------	
1	OK	
2	OK	
DELL Switch#		

Просмотр страницы Versions (Версии)

Страница **Versions** (Версии) содержит сведения об используемом оборудовании и версиях программного обеспечения. Чтобы открыть страницу **Versions** (Версии), на панели дерева выберите **System** (Система)→ **General** (Общие)→ **Versions** (версии).

Рис. 6-5. Версии



- **Software Version (Версия программы).** текущая версия программного обеспечения, запущенного на устройстве.
- **Boot Version (Версия загрузчика).** текущая версия загрузчика, используемого на устройстве.
- **Hardware Version (Версия аппаратного обеспечения).** текущая версия аппаратного обеспечения устройства.

Отображение версий устройств с помощью команд консоли

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

Таблица 6-4. Команды консоли для отображения версий

Команда консоли	Описание
show version (показать версию)	Отображает сведения о версии системы.

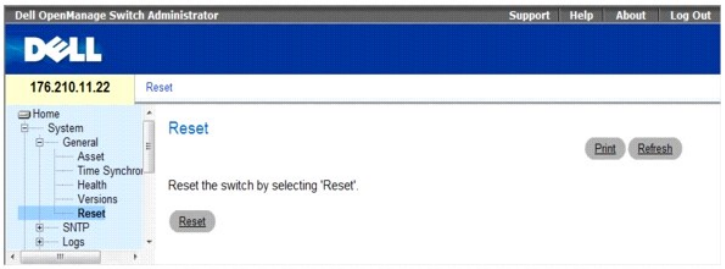
Далее приведен пример команд консоли.

```
Console> show version

SW version x.xxx (date 23-Jul-xxxx time 17:34:19)

Boot version x.xxx (date 17-Jan-xxxx time 11:48:21)

HW version x.x.x
```

Восстановление заводских параметров устройства

Страница **Reset** (Сброс) позволяет удаленно произвести сброс установок устройства. Прежде чем выполнять сброс устройства, сохраните все изменения в файле Running Configuration (Рабочая конфигурация). Это позволит сохранить текущую конфигурацию устройства. Дополнительные сведения о сохранении файлов конфигурации см. в разделе Managing Files (Управление файлами).Чтобы открыть страницу **Reset** (Сброс), на панели дерева выберите **System** (Система)→ **General** (Общие)→ **Reset** (Сброс).

Рис. 6-6. Сброс



Восстановление заводских параметров устройства

1. Откройте страницу **Reset** (Сброс)
2. Нажмите кнопку **Reset** (Сброс).

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

   Будут восстановлены заводские настройки устройства. После этого появится окно, в котором пользователь должен ввести имя пользователя и пароль.
4. Введите имя пользователя и пароль, чтобы снова подключиться к веб-интерфейсу.

Восстановление заводских параметров устройства с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для восстановления параметров устройства с помощью команд консоли:

Таблица 6-5. Команды консоли для сброса

Команда консоли	Описание
reload	Перезагрузка операционной системы.

Далее приведен пример команды консоли:

```
Console >reload

This command will reset the whole system and disconnect your current

session. Do you want to continue (y/n) [n] ?
```

Настройка параметров 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.

Устройство может запрашивать настройку времени у следующих типов серверов:

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

Источники времени устанавливаются по уровням. Уровни определяют точность источника времени. Чем выше уровень (где нуль - это самый высокий уровень), тем более точным является встроенный генератор синхроимпульсов (часы). Устройство коммутатора получает время с уровня 1 и выше.

Далее приведен пример уровней:

- **Stratum 0 (Уровень 0).** в качестве источника времени используются часы реального времени, например система GPS.
- **Stratum 1 (Уровень 1).** используется сервер, который напрямую связан с источником времени уровня 0. Серверы времени уровня 1

предоставляют основные стандарты времени в сети.

- **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:

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

Опрос данных времени у серверов одноадресной рассылки

Опрос данных одноадресной рассылки используется для опроса сервера, для которого известен IP-адрес. T1 - T4 используются для определения времени сервера. Это предпочтительный метод для синхронизации времени коммутатора.

Опрос данных времени у серверов рассылки любого типа

Опрос данных рассылки любого типа используется в том случае, если известен IP-адрес. Для установки значения времени используется первый сервер, который возвратил ответ. Уровни времени T3 и T4 используются для определения времени сервера. Использование данных времени рассылки любого типа для синхронизации времени коммутатора является более предпочтительным, чем использование данных времени серверов широковещательной рассылки.

Данные времени серверов широковещательной рассылки

Данные серверов широковещательной рассылки используются в том случае, если IP-адрес сервера неизвестен. Если сообщение широковещательной рассылки отправляется с сервера SNTP, то клиент SNTP ожидает ответа от сервера. Клиент SNTP ни передает запросы данных времени, ни получает ответы от сервера широковещательной рассылки.

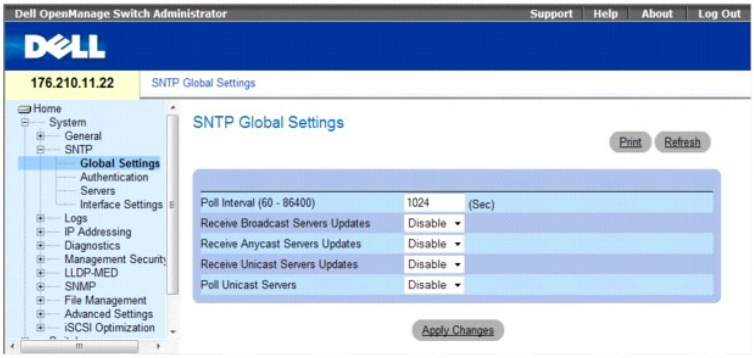
Проверка подлинности MD5 (Message Digest 5) обеспечивает синхронизацию линий связи коммутатора с серверами SNTP. MD5 - это алгоритм, создающий 128-разрядную хеш-строку. MD5 является разновидностью алгоритма MD4, который обеспечивает большую безопасность по сравнению с MD4. MD5 проверяет целостность передаваемых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

На панели дерева щелкните **System** (Система)→ **SNTP**, чтобы открыть страницу **SNTP**.

Определение общих параметров SNTP

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

Рис. 6-7. Общие параметры SNTP



- **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 рассылки).** опрашивает серверы SNTP для получения данных о времени от сервера широковещательной рассылки для выбранных интерфейсов.
- **Receive Anycast Servers Updates (Принимать обновления от серверов рассылки любого типа).** опрашивает сервер SNTP для получения данных о времени от сервера рассылки любого типа для выбранных интерфейсов. Если включены оба поля **Receive Anycast Servers Update** (Принимать обновления от серверов рассылки любого типа) и **Receive Broadcast Servers Update** (Принимать обновления от серверов широковещательной рассылки), системное время устанавливается в соответствии с данные о времени, полученными от сервера рассылки любого типа.

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

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

Далее приведен пример команд консоли.

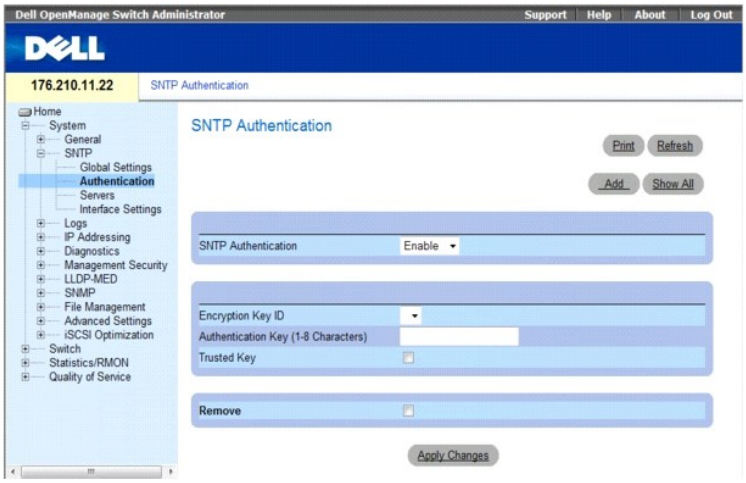
```
console> enable

console# configure

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

Определение методов проверки подлинности SNTP

Страница **SNTP Authentication** (Проверка подлинности SNTP) позволяет включить проверку подлинности SNTP между устройством и сервером SNTP. Это означает, что на странице **SNTP Authentication** (Проверка подлинности SNTP) также выбирается сервер, который выполняет проверку подлинности.

Выберите **System** (Система)→ **SNTP**→ **Authentication** (Проверка подлинности), чтобы открыть страницу **SNTP Authentication** (Проверка подлинности SNTP).

Рис. 6-8. Проверка подлинности SNTP



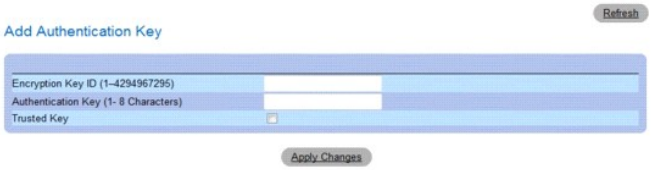
- **SNTP Authentication (Проверка подлинности SNTP).** включает проверку подлинности сеанса SNTP между устройством и сервером SNTP.
- **Encryption Key ID (Идентификатор ключа шифрования).** определяет идентификатор ключа, который используется для проверки подлинности сервера SNTP и устройства. Максимальная длина значения в этом поле составляет 4294967295 символов.
- **Authentication Key (1-8 Characters) (Ключ проверки подлинности от (1 до 8 символов)).** определяет ключ, используемый для проверки подлинности.
- **Trusted Key (Доверенный ключ).** определяет ключ шифрования, используемый для проверки подлинности сервера SNTP.
- **Remove (Удалить).** удаление выбранной проверки подлинности SNTP.

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. Добавление ключа проверки подлинности



3. Укажите значение для полей.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

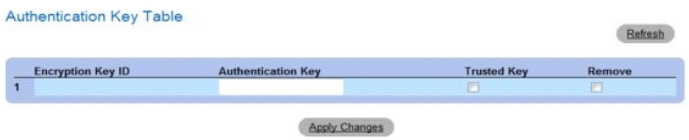
   Будет добавлен ключ проверки подлинности SNTP, а устройство будет обновлено.

Отображение таблицы ключей проверки подлинности

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

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

   Рис. 6-10. Таблица ключей проверки подлинности



Удаление ключа проверки подлинности

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

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

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

   Запись будет удалена, а устройство обновлено.

Определение параметров проверки подлинности SNTP с помощью команд консоли

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

Команда консоли	Описание
sntp authenticate	Определяет проверку подлинности для полученного трафика NTP (Network Time Protocol) от серверов.
sntp authentication-key *число* **md5** *значение*	Определяет ключ проверки подлинности для SNTP.

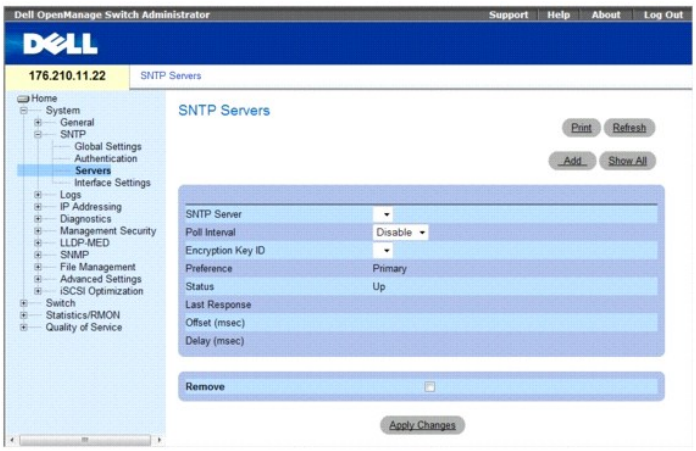
Далее приведен пример команд консоли.

```
console> enable

console# configure

Console(config)# sntp authentication-key 8 md5 ClkKey

Console(config)# sntp trusted-key 8

Console(config)# sntp authenticate
```

Определение серверов SNTP

Страница **SNTP Servers** (Серверы SNTP) содержит информацию для выбора сервера SNTP, а также позволяет добавить новый сервер SNTP. Кроме того, на странице **SNTP Servers** (Серверы SNTP) можно разрешить устройству выполнять запросы и получать трафик от серверов SNTP. *Чтобы открыть страницу* **SNTP Servers** (Серверы SNTP), на панели дерева выберите **System** (Система)→ **SNTP**→ **SNTP Servers** (Серверы SNTP).

Рис. 6-11. Серверы SNTP



- **SNTP Server (Сервер SNTP).** определяемый пользователем IP-адрес сервера SNTP или имя хоста. Можно определить до восьми серверов SNTP. Это поле может содержать от 1 до 158 символов.
- **Poll Interval (Интервал опроса).** когда этот флажок установлен, включается опрос сервера SNTP для получения данных о времени.
- **Encryption Key ID (Идентификатор ключа шифрования).** определяет идентификатор ключа, который используется для обмена данными между сервером SNTP и устройством. Диапазон значений: 1 - 4294967295.
- **Preference (Настройка).** сервер SNTP, предоставляющий данные о системном времени SNTP. Возможные значения:
  - **Primary(Основной).** основной сервер, предоставляющий информацию SNTP.
  - **Secondary (Дополнительный).** резервный сервер, предоставляющий информацию SNTP.
- **Status (Состояние).** отображает рабочее состояние сервера SNTP. Возможные значения этого поля:
  - **Up (Работает).** сервер SNTP работает надлежащим образом.
  - **Down (Отключен).** сервер SNTP не работает надлежащим образом.
  - **Unknown (Неизвестно).** состояние сервера SNTP в настоящее время неизвестно.
- **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).** когда этот флажок установлен, сервер SNTP, выбранный в списке **SNTP Server** (Сервер SNTP), удаляется.

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

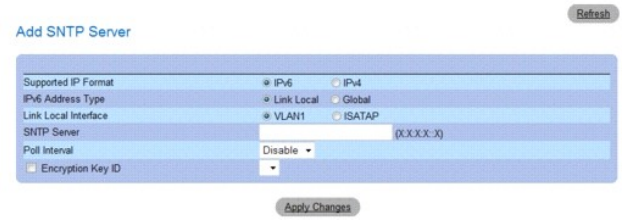
- **Supported IP Format (Поддерживаемый формат IP-адресов).** Отображает формат IP-адресов, поддерживаемый сервером SNTP. Возможные значения:
  - **IPv6.** поддержка IP версии 6.
  - **IPv4.** поддержка IP версии 4.
- **IPv6 Address Type.** В случае, если сервер поддерживает систему IPv6 (см. предыдущий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

Добавление сервера SNTP

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

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

Рис. 6-12. Добавление сервера SNTP



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

   Будет добавлен сервер SNTP, а устройство будет обновлено.

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

Таблица 6-8. Команды консоли для сервера SNTP

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

Далее приведен пример команд консоли.

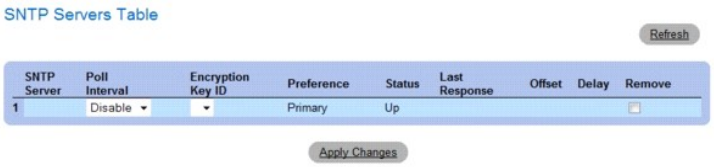
```
console> enable

console# configure

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

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. Таблица серверов SNTP



Изменение сервера SNTP

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

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

   Информация сервера SNTP будет обновлена.

Удаление сервера SNTP

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

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

   Запись будет удалена, а устройство обновлено.

Определение параметров серверов SNTP с помощью команд консоли

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

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

Далее приведен пример команд консоли.

```
console> enable

console# configure

Console(config)# sntp server 100.1.1.1 poll key 10

Console# show sntp status
```

```
Clock is synchronized, stratum 4, reference is 176.1.1.8
```

```
Reference time is AFE2525E.70597B34 (00:10:22.438 PDT Jul 5 1993)
```

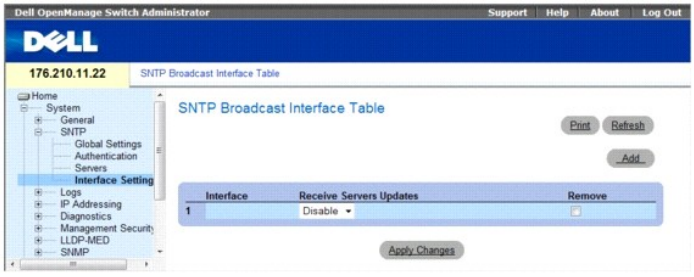
```

```

```
Unicast servers:
```

Server	Preference	Status	Last response	Offset [mSec]	Delay [mSec]
---------	----------	-------	---------------	------	------
176.1.1.8	Primary	Up	AFE252C1.6DBDDFF2	7.33	117.79
176.1.8.179	Secondary	Unknown	AFE21789.643287C9	8.98	189.19
Anycast server:					
Server	Preference	Status	Last response	Offset	Delay
				[mSec]	[mSec]
-------	----------	-------	-------------	-----	------
VLAN 119	Secondary	Up	19:53:21.789 PDT Feb 19 2002	7.19	119.89
Broadcast:					
Interface	IP address	Last response			
----------	----------	------------------------			
176.1.1.8	Primary	AFE252C1.6DBDDFF2			
176.1.8.179	Secondary	AFE21789.643287C9			

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**, выберите **System** (Система)→ **SNTP**→ **Interfaces Settings** (Параметры интерфейсов).



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

- **Interface (Интерфейс).** содержит список интерфейсов, для которых можно включить протокол SNTP.
- **Receive Servers Updates (Принимать обновления сервера).** показывает, включена ли для данного интерфейса функция обновления сервера SNTP.
- **Remove (Удалить).** когда этот флажок установлен, протокол SNTP для указанного интерфейса будет отключен.

Добавление интерфейса SNTP

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

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

Рис. 6-14. Добавление интерфейса SNTP

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

   Интерфейс SNTP будет добавлен, а устройство обновлено.

Определение параметров интерфейса SNTP с помощью команд консоли

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

Команда консоли	Описание
sntp client enable	Включает клиента SNTP (Simple Network Time Protocol) для интерфейса.
show sntp configuration	Отображает настройку протокола SNTP (Simple Network Time Protocol).

Далее приведен пример команд консоли.

```
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, g3
```

Управление журналами

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

Определение общих параметров журналов

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

Сообщения событий имеют уникальный формат в соответствии с рекомендациями SYSLOG RFC относительно формата сообщений для всех сообщениях об ошибках. Например, для сообщений Syslog и сообщений локальных устройств назначается код уровня ошибки, а также добавляется мнемоника сообщения, которая определяет исходное приложение, создавшее сообщение. Это позволяет фильтровать сообщения на основе срочности или важности. Уровень важности каждого сообщения определяет набор устройств регистрации событий, которым выполняется рассылка при каждой регистрации события.

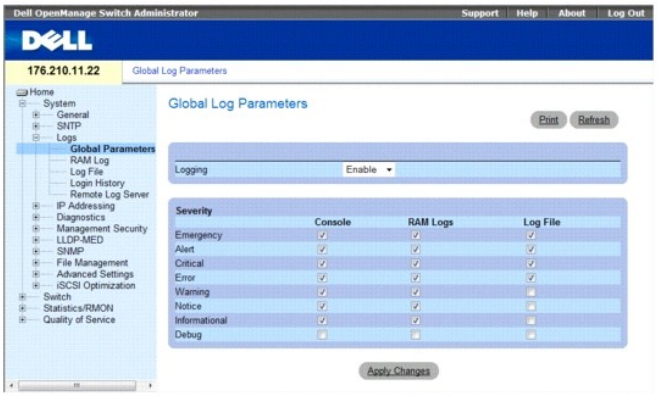
В следующей таблице приведены уровни важности ошибок журнала:

Тип важности	Уровень важности	Описание
Аварийное	0	Система не работает.

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

Страница **Global Log Parameters** (Общие параметры журналов) содержит поля, позволяющие определить события и журналы, в которые они должны быть записаны. Она содержит поля для общего включения журналов и поля параметров журналов. Сообщения журнала Severity (Важность) перечисляются в порядке от большей важности к меньшей. Чтобы открыть страницу **Global Log Parameters** (Общие параметры журналов), на панели дерева выберите **System** (Система)→ **Logs** (Журналы)→ **Global Parameters** (Общие параметры).

Рис. 6-15. Общие параметры журналов



- **Logging (Регистрация).** включает функции создания глобальных журналов для кэширования, файлов и серверов на устройстве. Вывод журнала на консоль по умолчанию включен.
- **Severity (Уровень важности).** далее приведены имеющиеся журналы уровня важности:
  - **Emergency (Аварийное).** наивысший уровень предупреждения. Если устройство выключено или работает неправильно, сообщение аварийного журнала сохраняется в определенном местоположении журнала.
  - **Alert (Сигнал о сбое).** второй уровень аварийного предупреждения. Журнал сохраняется при серьезных отклонениях в работе устройства, например, если все функции устройства отключены.
  - **Critical (Критическое).** третий уровень аварийного предупреждения. Критический журнал сохраняется в том случае, если происходят критические отклонения в работе устройства, например, если не работают два порта устройства, в то время как остальные по-прежнему работают.
  - **Error (Ошибка).** произошла ошибка устройства, например, если порт отключен.
  - **Warning (Предупреждение).** самый низкий уровень предупреждения устройства. Устройство работает, но имеется ошибка в работе.
  - **Notice (Уведомление).** предоставляет информацию об устройстве.
  - **Informational (Информационное).** предоставляет информацию об устройстве.
  - **Debug (Отладка).** предоставляет отладочные сообщения.

Если выбирается уровень важности, автоматически выбираются все уровни важности выше указанного.

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

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

Включение журналов:

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

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

   Параметры журналов будут сохранены, а устройство обновлено.

Включение журналов с помощью команд консоли

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

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

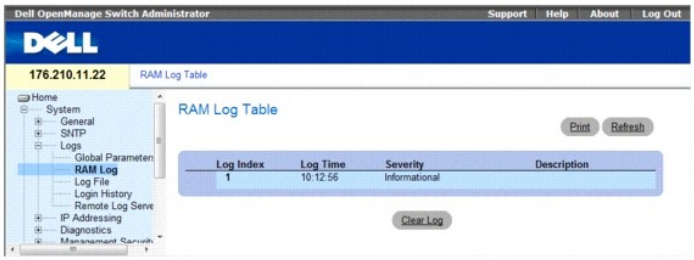
Далее приведен пример команд консоли.

```
Console (config)# logging on

Console (config)# logging console errors

Console (config)# logging buffered debugging

Console (config)# logging file alerts

Console (config)# clear logging

Console (config)# exit

Console# clear logging file

Clear Logging File [y/n]y



Console# show syslog-servers

Device Configuration

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

IP
address     Port  facility  Severity  Description

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

  1.1.1.1       514 local7    info

fe80::11%vlan1  514 local7    info

  3211::22      514 local7    info
```

Отображение таблицы журнала ОЗУ

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

Рис. 6-16. Таблица журнала ОЗУ



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

Удаление данных журнала:

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

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

Просмотр и очистка таблицы журнала ОЗУ с помощью команд консоли

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

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

Далее приведен пример команд консоли.

```
console# show logging

Logging is enabled.

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

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

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

1 messages were not logged

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

01-Jan-2000 01:01:36 :%LINK-W-Down: g24

01-Jan-2000 01:01:36 :%LINK-W-Down: g23

01-Jan-2000 01:01:36 :%LINK-W-Down: g22

01-Jan-2000 01:01:36 :%LINK-W-Down: g21

01-Jan-2000 01:01:36 :%LINK-W-Down: g20

01-Jan-2000 01:01:36 :%LINK-W-Down: g19

01-Jan-2000 01:01:36 :%LINK-W-Down: g18

01-Jan-2000 01:01:36 :%LINK-W-Down: g17

01-Jan-2000 01:01:36 :%LINK-W-Down: g13

1-Jan-2000 01:01:36 :%LINK-W-Down: g2
```

```
01-Jan-2000 01:01:36 :%LINK-W-Down: g1

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

Console # clear logging

clear logging buffer [y/n]?

Console#
```

Отображение таблицы файла журнала

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

Рис. 6-17. Таблица файла журнала

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

Отображение таблицы файла журналов с помощью команд консоли

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

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

Далее приведен пример команд консоли.

```
Console # show logging file

Logging is enabled.

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

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

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

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

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

1 messages were not logged

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

01-Jan-2000 01:11:49 :%LINK-I-Up: g21

01-Jan-2000 01:11:49 :%2SWPHY-I-CHNGCOMBOMEDIA: Media changed from copper media
```

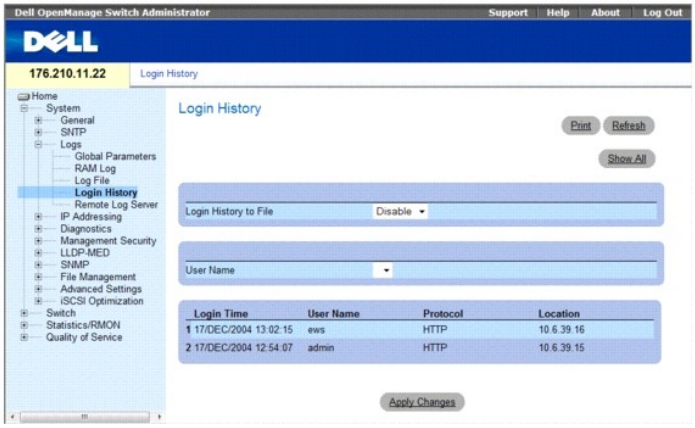
```
to fiber media (1000BASE-SX) on port g21.

01-Jan-2000 01:11:48 :%2SWPHY-I-CHNGCOMBOMEDIA: Media changed from fiber media to copper media on port g21.

01-Jan-2000 01:11:48 :%LINK-W-Down: g21

01-Jan-2000 01:11:46 :%LINK-I-Up: g19

01-Jan-2000 01:11:42 :%LINK-W-Down: g14

01-Jan-2000 01:11:41 :%LINK-I-Up: g14

01-Jan-2000 01:11:36 :%LINK-W-Down: g9

01-Jan-2000 01:11:35 :%LINK-I-Up: g1

01-Jan-2000 01:11:34 :%LINK-W-Down: g1

console#
```

Просмотр журнала входов устройств

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

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

Рис. 6-18. Журнал входов



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

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

Просмотр журнала входов

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

   Отобразятся сведения о входе выбранного пользователя.

Отображение журнала входов в устройство с помощью команд консоли

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

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

Далее приведен пример команд консоли.

```
console# show users login-history

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

Страница настройки параметров удаленного сервера журналов

Страница **Remote Log Server Settings** (Параметры удаленного сервера журналов) содержит поля для просмотра и настройки доступных серверов журналов. Кроме того, можно определить новые серверы журналов и важность журналов, отправляемых на каждый сервер. Чтобы открыть страницу **Remote Log Server Settings** (Параметры удаленного сервера журналов), на панели дерева выберите **System** (Система)→ **Logs** (Журналы)→ **Remote Log Server** (Удаленный сервер журналов).

Рис. 6-19. Параметры удаленного сервера журналов

- **Available Servers (Доступные серверы).** список серверов, на которые можно отправить журналы.
- **UDP Port (1-65535) (Порт UDP).** порт UDP, на который посылаются журналы для выбранного сервера. Возможные значения: от 1 до 65535. Значение по умолчанию: 514.
- **Facility (Приложение).** определяемое пользователем приложение, из которого отправляются журналы на удаленный сервер. Для одного сервера можно назначить только одно приложение. Если назначен второй уровень приложения, первый уровень приложения отменяется. Все приложения, определенные для устройства, используют одно и то же приложение на сервере. Возможные значения: Local 0 - Local 7.
- **Description (0-64 Characters) (Описание (0-64 символов)).** описание сервера, задаваемое пользователем.
- **Severity to Include (Указываемая важность).** далее приведены имеющиеся уровни важности:
  - **Emergency (Аварийное).** система не работает.

- **Alert (Сигнал о сбое).** система требует немедленного вмешательства.
- **Critical (Критическое).** система находится в критическом состоянии.
- **Error (Ошибка).** произошла ошибка системы.
- **Warning (Предупреждение).** появилось предупреждение системы.
- **Notice (Примечание).** система работает правильно, но появилось уведомление системы.
- **Informational (Информационное).** предоставляет информацию об устройстве.
- **Debug (Отладка).** предоставляет подробные сведения о журнале. При возникновении ошибки отладки обратитесь в службу технической поддержки клиентов.

- **Delete Server (Удалить сервер).** когда флажок установлен, выбранный сервер удаляется из списка *Available Servers* (Доступные серверы).
- **Severity to Include (Указываемая важность).** отображение уровня важности журнала, сообщаемого удаленным сервером. Возможные значения поля:
  - **Emergency** (Аварийное). наивысший уровень предупреждения. Если устройство выключено или работает неправильно, сообщение аварийного журнала сохраняется в определенном местоположении журнала.
  - **Alert (Сигнал о сбое).** второй уровень аварийного предупреждения. Журнал сохраняется при серьезных отклонениях в работе устройства, например, если все функции устройства отключены.
  - **Critical (Критическое).** третий уровень аварийного предупреждения. Критический журнал сохраняется в том случае, если происходят критические отклонения в работе устройства, например, если не работают два порта устройства, в то время как остальные по-прежнему работают.
  - **Error (Ошибка).** произошла ошибка устройства, например, если порт отключен.
  - **Warning (Предупреждение).** самый низкий уровень предупреждения устройства. Устройство работает, но имеется ошибка в работе.
  - **Notice (Уведомление).** предоставляет информацию об устройстве.
  - **Informational (Информационное).** предоставляет информацию об устройстве.
  - **Debug (Отладка).** предоставляет отладочные сообщения.

Страница **Remote Log Server Settings** (Параметры удаленного сервера журналов) также содержит список важности. Определения важности такие же, как и для страницы Global Log Parameters (Общие параметры журналов).

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

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

Отправка журналов на сервер

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

   Параметры журналов будут сохранены, а устройство обновлено.

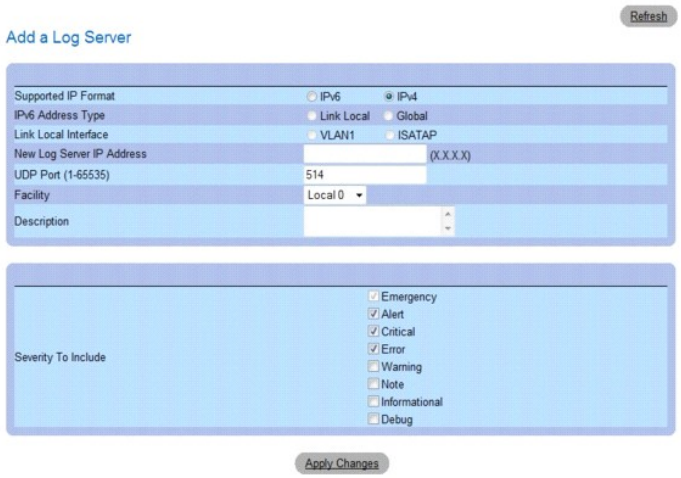
Определение нового сервера:

1. Откройте страницу **Remote Log Server Settings** (Параметры удаленного сервера журналов).

2. Нажмите кнопку **Add** (Добавить).

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

Рис. 6-20. Добавление сервера журналов



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

3. Определите поля.

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

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

Отображение таблицы удаленных серверов журналов:

1. Откройте страницу **Remote Log Server Settings** (Параметры удаленного сервера журналов).

2. Нажмите кнопку **Show All** (Показать все).

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

Рис. 6-21. Таблица удаленных серверов журналов.

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

1. Откройте страницу **Remote Log Server Settings** (Параметры удаленного сервера журналов).

2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **Remote Log Servers Table** (Таблица удаленных серверов журналов).

3. Выберите запись **Remote Log Servers Table** (Таблица удаленных серверов журналов).

4. Установите флажок **Remove** (Удалить), чтобы удалить серверы.

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

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

Работа с удаленным сервером журналов с помощью команд консоли

В таблице перечислены эквивалентные команды консоли для работы с журналами удаленного сервера.

Команда консоли	**Описание**
logging (*ipv4-address*|*ipv6-addres* (*ip-адрес*) | *hostname* (*имя хоста*)) [**port** *порт*] [**severity** *уровень*] [**facility** *приложение*] **description** *текст*]	Регистрирует сообщения на удаленном сервере.
no logging	Удаляет сервер syslog.
show logging	Отображает состояние журнала и системные сообщения.

Далее приведен пример команд консоли.

```
console> enable

console# configure

console (config) # logging 10.1.1.1 severity critical



Console# show logging

Logging is enabled.

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

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

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

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

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

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

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

1 messages were not logged

03-Mar-2004 12:02:03 :%LINK-I-Up: g1

03-Mar-2004 12:02:01 :%LINK-W-Down: g2

03-Mar-2004 12:02:01 :%LINK-I-Up: g3
```

Определение IP-адресов устройств

Страница **IP Addressing** (IP-адресация) содержит ссылки для назначения IP адресов интерфейса и шлюза по умолчанию, а также определения параметров ARP и DHCP для интерфейсов.

Настройка интернет-протокола версии 6 (IPv6)

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

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

Синтаксис системы IPv6

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

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

Префиксы системы IPv6

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

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

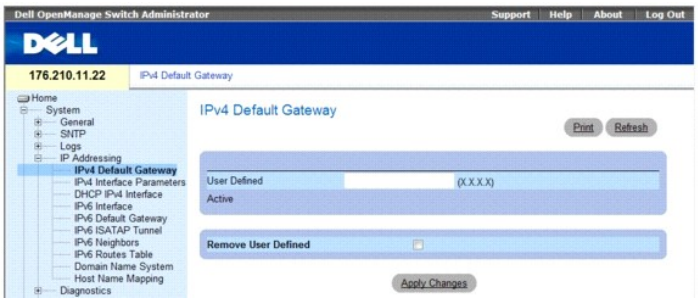
Промежуточный механизм переноса требуется для связи узлов, использующих только систему IPv6, с узлами системы IPv6 по инфраструктуре системы IPv4. Туннельный механизм использует туннельный протокол ISATAP. Этот протокол обрабатывает сеть IPv4 как виртуальную местную связь сети IPv6, при этом каждый адрес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

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

Определение шлюзов по умолчанию для адресов IPv4

Страница **IPv4 Default Gateway** (Шлюз адреса IPv4 по умолчанию) содержит поля для назначения устройств шлюза. 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. Чтобы открыть страницу **IPv4 Default Gateway** (Шлюз адреса IPv4 по умолчанию), на панели дерева выберите **System** (Система)→ **IP Addressing** (IP-адресация)→ **IPv4 Default Gateway** (Шлюз по умолчанию).

Рис. 6-22. Шлюз адреса IPv4 по умолчанию



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

- **User Defined (Шлюз по умолчанию, определяемый пользователем).** отображает IP-адрес шлюза по умолчанию.
- **Active (Активный).** Отображает шлюз по умолчанию, настройка которого производится в настоящее время.
- **Remove User Defined (Удалить заданное пользователем)**. Удаляет устройства шлюза из падающего списка **IPv4 Default Gateway** (Шлюзы IPv4 по умолчанию), если установлен флажок.

Выбор устройства шлюза IPv4 по умолчанию:

1. Откройте страницу **IPv4 Default Gateway** (Шлюз адреса IPv4 по умолчанию).
2. Выберите IP-адрес в падающем списке **IPv4 Default Gateway** (Шлюзы IPv4 по умолчанию).
3. Установите флажок **Active** (Активный).
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Устройство шлюза будет выбрано, а устройство обновлено.

Удаление устройства шлюза IPv4 по умолчанию:

1. Откройте страницу **IPv4 Default Gateway** (Шлюз адреса IPv4 по умолчанию).

2. Установите флажок **Remove** (Удалить), чтобы удалить шлюзы по умолчанию.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

   Запись шлюза пол умолчанию будет удалена, а устройство обновлено.

Определение устройств шлюза IPv4 с помощью команд консоли

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

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

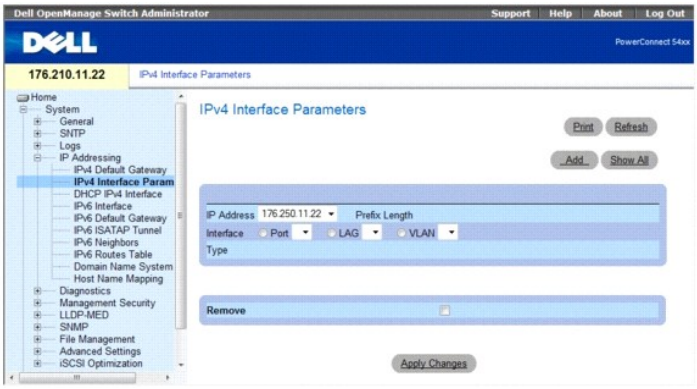
Далее приведен пример команд консоли.

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

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

Определение интерфейсов IPv4

Страница **IPv4 Interface Parameters** (Параметры интерфейса IPv4) содержит поля для назначения IP-параметров для интерфейсов. Чтобы открыть страницу **IPv4 Interface Parameters** (Параметры интерфейса IPv4), выберите **System** (Система)→ **IP Addressing** (IP-адресация)→ IPv4 Interface Parameters (Параметры интерфейса IPv4).на панели дерева.

Рис. 6-23. Параметры интерфейса IPv4



- **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. Выберите **Port** (Порт), **LAG** или **VLAN**.
- **Type (Тип).** показывает, был ли IP-адрес определен как статический.
- **Remove (Удалить).** когда установлен этот флажок, удаляется интерфейс, выбранный в раскрывающемся меню **IP Address** (IP-адрес).

Добавление интерфейса

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

   Откроется страница **IPv4 Interface Parameters** (Параметры интерфейса IPv4).

Рис. 6-24. Добавление статического интерфейса IPv4

3. Заполните поля на этой странице.

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

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

   Новый интерфейс будет добавлен, а устройство обновлено.

Изменение параметров IP-адреса

1. Откройте страницу **IPv4 Interface Parameters** (Параметры интерфейса IPv4).
2. Выберите IP-адрес в раскрывающемся списке **IP Address** (IP-адрес).
3. Измените необходимые поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

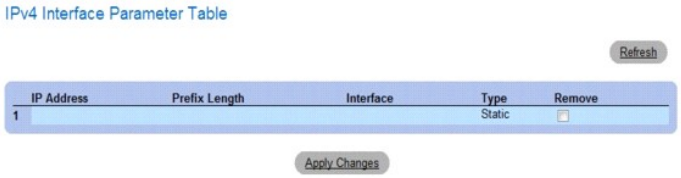
   Параметры будут изменены, а устройство обновлено.

Удаление IP-адресов

1. Откройте страницу **IPv4 Interface Parameters** (Параметры интерфейса IPv4).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница с таблицей **IPv4 Interface Parameters Table** (Параметры интерфейса IPv4).

Рис. 6-25. Таблица параметров интерфейса IPv4



3. Выберите IP-адрес и установите флажок **Remove** (Удалить).
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Выбранный IP-адрес будет удален, а устройство обновлено.

Определение интерфейсов IPv4 с помощью команд консоли

В следующей таблице приведены команды консоли для настройки полей, отображаемых на странице **IPv4 Interface Parameters** (Параметры интерфейса IPv4).

Команда консоли	**Описание**
ip address *ip-адрес {маска | длина_префикса}*	Задает IP-адрес.
no ip address [*ip-адрес*]	Удаляет IP-адрес.
show ip interface [**ethernet** *номер_интерфейса* | **vlan** *идентификатор_vlan* | **port-channel** *номер*]	Выводит состояние готовности настроенных IP-интерфейсов.

Далее приведен пример команд консоли.

```
      Console (config)# interface vlan1

      Console (config-if)# ip address 131.108.1.27 255.255.255.0

      Console (config-if)# no ip address 131.108.1.27

      Console (config-if)# exit

console# show ip interface vlan 1

Output

Gateway IP Address Activity status

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

192.168.1.1 Active

IP address Interface Type

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

192.168.1.123/24 VLAN 1 Static
```

Определение параметров DHCP интерфейса IPv4

Страница **DHCP IPv4 Interface** (интерфейс IPv4 DHCP) содержит поля для определения клиентов DHCP, подключенных к устройству. Выберите **System** (Система)→ **IP Addressing** (IP-адресация)→ **DHCP IPv4 Interface** (IPv4 интерфейс DHCP) на панели дерева. Чтобы открыть страницу **DHCP Interface** (IPv4 интерфейс DHCP) .

Рис. 6-26. IPv4 - интерфейс DHCP

- **Interface (Интерфейс).** Специфический интерфейс, по которому произошла конфигурация клиента DHCP. Для выбора интерфейса, подключенного к устройству, выберите параметр **Port** (Порт), **LAG** или **VLAN**.
- **Host Name (Имя хоста).** Системное имя, в том виде, в котором оно определено на сервере DHCP (не более 20 символов).
- **Remove (Удалить).** когда установлен этот флажок, клиенты DHCP удаляются.

Добавление клиента DHCP

1. Откройте страницу **DHCP IPv4 Interface** (IPv4 интерфейс DHCP).
2. Нажмите кнопку **Add** (Добавить).

   Откроется страница **Add DHCP IPv4 Interface** (Добавить IPv4 интерфейс DHCP).
3. Введите значения в поля на этой странице.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   IP-интерфейс DHCP будет добавлен, а устройство обновлено.

Изменение IPv4 интерфейса

1. Откройте страницу **DHCP IPv4 Interface** (IPv4 интерфейс DHCP).
2. Измените поля.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

   Запись будет изменена, а устройство обновлено.

Удаление IPv4 - интерфейса DHCP

1. Откройте страницу **DHCP IPv4 Interface** (IPv4 интерфейс DHCP).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница с таблицей **DHCP IPv4 Interface Table** (Параметры интерфейса IPv4).
3. Выберите запись клиента DHCP.
4. Установите флажок **Remove** (Удалить).
5. Нажмите кнопку **Apply Changes** (Применить изменения).

   Выбранная запись будет удалена, а устройство обновлено.

Определение IPv4-интерфейсов DHCP с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для определения клиентов DHCP.

Команда консоли	**Описание**
ip address dhcp [**hostname** *имя_хоста*]	Чтобы получать IP-адрес для интерфейса Ethernet по протоколу DHCP (Dynamic Host Configuration Protocol)

Далее приведен пример команды консоли:

```
console> enable

console# config

console (config#) interface ethernet g1

console (config-if)# ip address dhcp 10.0.0.1 /8
```

Определение интерфейсов IPv6

Система поддерживает хосты IPv6. Страница **IPv4 Interface Parameters** (Параметры интерфейса IPv4) содержит поля для назначения интерфейсов IPv6. Чтобы открыть страницу **IPv4 Interface Parameters** (Параметры интерфейса IPv4), выберите **System** (Система)→ **IP Addressing** (IP-адресация)→ **IPv6 Interface** (Интерфейс IPv6) на панели дерева.

Рис. 6-27. Интерфейс IPv6

- **Interface (Интерфейс).** Интерфейс IPv6, который выбран для настройки.
- **Remove (Удалить).** При выборе этого параметра, происходит удаление атрибутов IPv6 интерфейса.
- **DAD Attempts (Количество попыток определения уникальности адресов).** Определяет количество последовательных сообщений определения уникальности соседних адресов, которые были посланы на интерфейс при работе алгоритма обнаружения дублирующихся адресов (DAD) над адресами одноадресной передачи IPv6 данного интерфейса. Новые адреса остаются в промежуточном состоянии до окончания процесса обнаружения дублирующихся адресов. Если в поле введено значение 0, алгоритм обнаружения дублирующихся адресов на указанном интерфейсе будет отключен. Если в поле введено значение 1, произойдет однократная передача без последующих пересылок. Диапазон значений поля: 0-600, значение по умолчанию: 1.
- **Autoconfiguration (Автоматическая конфигурация).** Указывает, была ли проведена процедура назначения IPv6-адресов интерфейса с помощью автоматической конфигурации, не использующей информацию о состоянии. При включении этой функции, запускается процедура поиска соседних узлов маршрутизатора (предназначенная для определения маршрутизатора для назначения IP-адреса интерфейсу с использованием префиксов, полученных в сообщении автоконфигурации). Если автоконфигурация отключена, автоматическое назначение адресов IPv6 глобальной одноадресной пересылки выполняться не будет, и существующие автоматически назначенные адреса IPv6 глобальной одноадресной пересылки будут удалены из интерфейса. Состояние параметра по умолчанию - *Enabled (Включено)*.
- **Send ICMP Unreachable (Пересылка сообщения о недоступности адреса ICMP).** Указывает, включена или выключена передача сообщения «ICMPv6 Address Unreachable». При включении, сообщения о недоступном адресе будут генерироваться для любого пакета, приходящего от интерфейса с неназначенным портом TCP/UDP. Значение по умолчанию - *Enabled* (Включено).
- **ICMP Error Rate Limit Interval (Интервал ошибки скорости ICMP).** Интервал скорости для подачи сообщения об ошибке ICMPv6 в миллисекундах. Значение этого параметра и параметра Bucket Size (см. ниже) определяет, сколько сообщений об ошибке ICMP может быть послано в течение установленного временного интервала. Например, если установлен интервал 100 мс и размер сегмента - 10 сообщений, то в течение 1 секунды может пересылаться до 100 сообщений об ошибке ICMP.
- **ICMP Error Rate Limit Bucket Size (Размер сегмента сообщений об ошибке ICMP).** Устанавливает размер сегмента для сообщений об ошибке ICMPv6. Значение этого параметра и параметра интервала (см. выше) определяет, сколько сообщений об ошибке ICMP может быть послано в течение установленного временного интервала. Например, если установлен интервал 100 мс и размер сегмента - 10 сообщений, то в течение 1 секунды может пересылаться до 100 сообщений об ошибке ICMP. Значение по умолчанию - 100 сообщений об ошибке ICMP в секунду, что соответствует интервалу по умолчанию 100 мс, умноженному на размер сегмента по умолчанию, равный 10.
- **IPv6 Address (Адрес IPv6).** Указывает адрес IPv6, назначенный данному интерфейсу. Адрес должен быть достоверным адресом IPv6, записанным в 16-ричной системе, состоящий из 16-битных величин, разделенных двоеточием. Пример адреса IPv6: 2031:0:130F:0:0:9C0:876A:130D, а в сжатом виде - 2031::0:9C0:876A:130D. Для одного интерфейса может быть установлено до пяти адресов IPv6 (не включая адресов локальной связи), с общим ограничением до 128 адресов на систему.
- **Prefix (Префикс).** Указывает длину префикса адреса IPv6. Длина префикса представляет собой десятичное число, указывающее количество старших смежных битов адреса составляют префикс (сетевой сегмент адреса). Поле префикса применяется только для статических адресов IPv6, определенных как глобальные адреса IPv6.
- **IPv6 Address Type (Тип адреса IPv6).** Указывает способ присоединения IP-адреса к интерфейсу. Возможные значения:
  - **Link Local (Локальная связь).** Адрес локальной связи, который не маршрутизируется, а используется только для связи в пределах той же сети. Адрес локальной связи имеет префикс 'FE80'.
  - **Global Unicast (Глобальный адрес одноадресной передачи).** Указывает, что IP-адрес является глобальным уникальным адресом одноадресной пересылки системы IPv6; он является видимым и доступным из других подсетей.
  - **Global Anycast (Глобальный адрес произвольной адресации).** Указывает, что IP-адрес является глобальным уникальным адресом для произвольной адресации в системе IPv6; он является видимым и доступным из других подсетей**.**
  - **Multicast (Многоадресный).** Указывает, что данный IP-адрес является многоадресным.
- **IPv6 Address Origin Type (Тип происхождения адреса IPv6).** Определяет тип конфигурируемого статического IPv6-адреса интерфейса. Возможные значения:
  - **Dyanmic (Динамический).** Указывает, что адрес получен от системы автоматической конфигурации.
  - **Static (Статический).** Показывает, что конфигурация адреса произведена пользователем.
  - **System (система).** Показывает, что IP-адрес был генерирован системой.
- **DAD Status (состояние алгоритма DAD).** Отображает статус системы автоматического обнаружения дублирующихся адресов (DAD), которая

определяет уникальность введенных адресов IPv6. Этот параметр представляет собой параметр только для чтения, значения полей которого таковы:

- **Tentative (Временный).** Указывает, что система находится в процессе определения дублирующихся адресов IPv6.
- **Duplicate (Дублирование).** Указывает, что адрес IPv6 уже используется другим хостом сети. Дублирующийся адрес IPv6 блокируется и не используется в дальнейшем для пересылки и получения трафика.
- **Active (Работает).** Указывает, что IPv6 находится в рабочем состоянии.

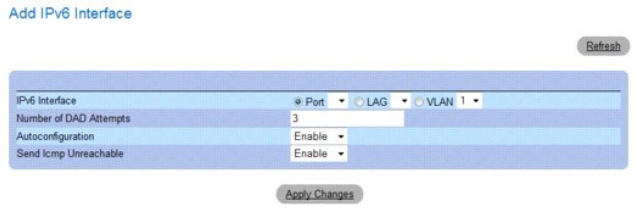
- **Remove (Удаление).** Если выбрана эта опция, происходит удаление адреса из таблицы.

Добавление интерфейса IPv6

1. Откройте страницу **IPv4 Interface Parameters** (Параметры интерфейса IPv4).
2. Выберите **Add IPv6 Interface** (Добавить интерфейс IPv6).

   Откроется страница **Add a Static IPv4 Interface** (Добавление статического интерфейса IPv6):

Рис. 6-28. Добавление интерфейса IPv6



3. Заполните поля на этой странице.

   IPv6 Interface (Интерфейс IPv6) указывает, является ли данный интерфейс портом, LAG или VLAN.

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

   Новый интерфейс будет добавлен, а устройство обновлено.

Добавление адреса IPv6 к текущему интерфейсу

1. Откройте страницу **IPv4 Interface Parameters** (Параметры интерфейса IPv4).
2. Выберите **Add IPv6 Address** (Добавить интерфейс IPv6).

   Откроется страница**Add IPv6 Address** (Добавление адреса IPv6):

Рис. 6-29. Добавление адреса IPv6

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

   Новый адрес будет добавлен и устройство обновлено.

Изменение параметров интерфейса IPv6

1. Откройте страницу **IPv4 Interface Parameters** (Параметры интерфейса IPv4).
2. Выберите интерфейс в раскрывающемся меню **Interface** (Интерфейс).
3. Измените необходимые поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Параметры будут изменены, а устройство обновлено.

Определение интерфейсов IPv6 с помощью команд консоли

В следующей таблице приведены команды консоли для настройки полей, отображаемых на странице **IPv4 Interface Parameters** (Параметры интерфейса IPv4).

Команда консоли	**Описание**
ipv6 enable [**нет автоконфигурации**]	Включает обработку IPv6 интерфейса.
ipv6 address autoconfig	Включает автоматическую конфигурацию адресов IPv6 с использованием автоконфигурации, не учитывающей состояние интерфейса.
ipv6 icmp error-interval *миллисекунды* [*bucketsize*]	Конфигурирует параметры предельного интервала и размера сегмента для протокола управляющих интернет-сообщений (ICMP) для сообщений об ошибках IPv6.
show ipv6 icmp error-interval	Отображает интервал подачи сообщений об ошибках ipv6 icmp error interval.
ipv6 address *ipv6-address/prefix-length* [**eui-64**] [**anycast**]	Конфигурирует адрес IPv6 интерфейса.
ipv6 address *ipv6-address* **link-local**	Конфигурирует адрес локальной связи IPv6 интерфейса.
ipv6 unreachables	Включает генерирование сообщений протокола ICMP для IPv6 (ICMPv6) о недоступном адресе для пакетов, поступающих на указанный интерфейс.
show ipv6 interface [ethernet *номер_интерфейса* | **vlan** *идентификатор_vlan* | **port-channel** *номер*]	Выводит состояние готовности настроенных интерфейсов IPv6.
ipv6 nd dad attempts *кол-во_попыток*	Устанавливает количество последовательных сообщений определения уникальности соседних адресов, которые были посланы на интерфейс при работе алгоритма обнаружения дублирующихся адресов (DAD) над адресами одноадресной передачи IPv6 данного интерфейса.
ipv6 host *name ipv6-address1 [ipv6-address2...ipv6-address4]*	Определяет соответствие статических имен хостов адресам в кэше имен хоста.
ipv6 set mtu {**ethernet** *interface* | **port-channel** *port-channel-number} { bytes* | ***default***}	Устанавливает максимальный размер пакета (МРП) для пакетов данных IPv6, пересылаемых на интерфейс.
ping {*ipv4-address* | *hostname*} [**size** *packet_size*] [**count** *packet_count*] [**timeout** *time_out*]	Пересылает пакеты эхо-запросов IPv4 ICMP на другой узел сети.
ping ipv6 {*ipv6-address* | *hostname*} [**size** *packet_size*] [**count** *packet_count*] [**timeout** *time_out*]	Пересылает пакеты эхо-запросов IPv6 ICMP на другой узел сети.

Далее приведен пример команд консоли.

```
console# show ipv6 interface vlan 1

Number of ND DAD attempts: 1

MTU size: 1500

Stateless Address Autoconfiguration state: enabled

ICMP unreachable message state: enabled

MLD version: 2


IP addresses            Type       DAD State

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

fe80::232:87ff:fe08:1700 linklayer Active

ff02::1                 linklayer N/A

ff02::1:ff08:1700       linklayer N/A
```

```
console(config)# ipv6 icmp

error-interval ICMP errors rate limiting

console(config)# ipv6 icmp error-interval

<0-2147483647> The time interval between tokens being placed in the bucket in milliseconds

console(config)# ipv6 icmp error-interval 100

<1-200>       The maximum number of tokens stored in the bucket
```

Определение шлюзов по умолчанию для адресов IPv6

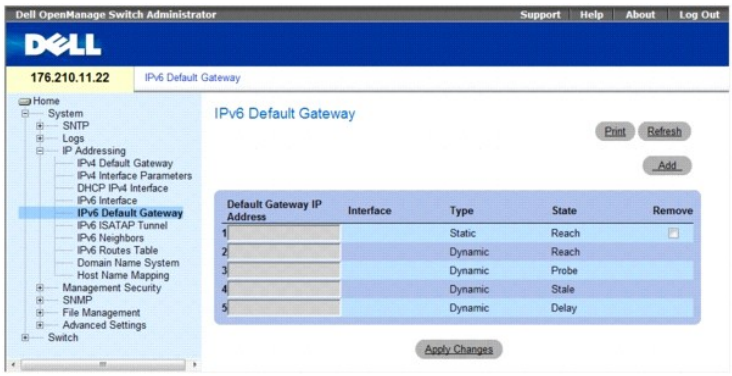
Страница **IPv6 Default Gateway** (Шлюзы IPv6 по умолчанию) позволяет произвести ручную настройку маршрутизатора для трафика по всем связям. Адрес шлюза по умолчанию - это интерфейс, который служит точкой доступа к другой сети. Для IPv6, конфигурация шлюза по умолчанию не является обязательной, поскольку хосты могут автоматически определять существование маршрутизатора локальной сети благодаря процедуре обнаружения маршрутизатора.

В отличие от системы IPv4, шлюз по умолчанию для системы IPv6 может иметь несколько адресов IPv6, которые могут включать один статический адрес, определяемый пользователем и несколько динамических адресов, определяемых при подаче сообщения определения маршрутизатора. Шлюз, определяемый пользователем, имеет более высокий приоритет над автоматически определяемым маршрутизатором.

- При удалении IP-интерфейса, все IP-адреса, определенные для него по умолчанию, также удаляются.
- Динамические IP-адреса удаляться не могут.
- Предупреждающее сообщение будет выводиться при попытке пользователя вставить более одного пользовательского адреса.
- При попытке вставить адрес другого типа, нежели адрес местной связи, будет выводится предупреждающее сообщение.

Чтобы открыть страницу **IPv6 Default Gateway** (Шлюз адреса IPv6 по умолчанию), выберите **System** (Система)→ **IP Addressing** (IP-адресация)→ **IPv6 Default Gateway** (Шлюз адреса IPv6 по умолчанию) на панели дерева.

Рис. 6-30. Шлюз адреса IPv6 по умолчанию



- **Default Gateway IP Address (IP-адрес шлюза по умолчанию).** Отображает IPv6 - адрес локальной связи для шлюза по умолчанию.
- **Interface (Интерфейс).** Указывает исходящий интерфейс, через который осуществляется доступ к шлюзу по умолчанию. К интерфейсу может относиться любой порт//LAG/VLAN и/или тоннель.
- **Type (Тип).** Указывает способ, которым конфигурируется шлюз по умолчанию. Возможные значения:
  - **Static (статический).** Показывает, что шлюз по умолчанию определяется пользователем.
  - **Dynamic (динамический).** Указывает, что шлюз был сконфигурирован динамически.
- **State (Статус).** Отображает статус шлюза по умолчанию. Возможные значения:
  - **Incomplete (Не закончено).** Указывает, что процесс определения адреса еще идет, и адрес канального уровня шлюза по умолчанию еще не был определен.
  - **Reachable (Доступен).** Указывает, что шлюз по умолчанию определен и доступен (по состоянию на несколько десятков секунд до настоящего момента).
  - **Stale (Устаревший).** Указывает, что шлюз по умолчанию больше не считается доступным, но, до тех пор, пока не будет пересылки трафика к шлюзу по умолчанию, не было предпринято попыток определить его доступность.
  - **Delay (Задержка).** Указывает, что шлюз по умолчанию более не рассматривается как доступный, и по шлюзу, установленному по умолчанию, был отправлен трафик. Имеется кратковременная задержка в отсылке тестовых импульсов для того, чтобы протоколы верхнего уровня смогли собрать информацию о доступности шлюза.
  - **Probe (Тестовый сигнал).** Указывает, что шлюз по умолчанию более не рассматривается в качестве доступного, и для проверки его доступности посылаются тестовые сигналы одноадресной передачи определения соседних адресов.
  - **Unreachable (Недоступен).** Указывает, что подтверждение доступности шлюза получено не было.

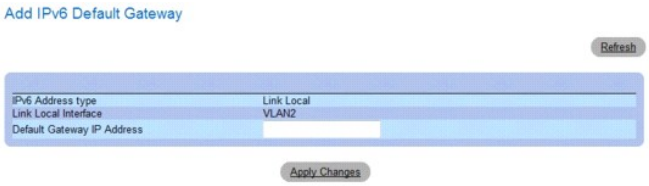
- **Remove (Удаление).** Если выбрана эта опция, происходит удаление адреса из списка.

Добавление шлюза по умолчанию для адресов IPv6

1. Откройте страницу **IPv6 Default Gateway** (Шлюз адреса IPv6 по умолчанию).
2. Нажмите кнопку **Add** (Добавить).

   Откроется страница **Add IPv6 Default Gateway** (Шлюз адреса IPv6 по умолчанию):

Рис. 6-31. Добавление шлюза адреса IPv6 по умолчанию



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

   Новый шлюз будет добавлен, а устройство обновлено.

Определение параметров шлюза IPv6 по умолчанию с помощью команд консоли

В следующей таблице приведены команды консоли для настройки полей, отображаемых на странице **IPv6 Default Gateway** (Шлюз адреса IPv6 по умолчанию).

Команда консоли	Описание
ipv6 default-gateway *ipv6-адрес*	Определяет шлюз IPv6 по умолчанию.

Определение туннелей IPv6 ISATAP

Страница **IPv6 ISATAP Tunnel** (Туннель IPv6 ISATAP) определяет процесс туннелирования устройства, которое формирует пакеты IPv6 и вставляет их в пакеты IPv4 для пересылки по сети IPv4.

Протокол внутрисайтовой автоматической туннельной адресации *(ISATAP)* представляет собой механизм переноса IPv6, который определяется как туннельный интерфейс IPv6 и предназначен для передачи пакетов IPv6 между двухстековыми узлами поверх сети IPv4.

При включении протокола ISATAP на туннельном интерфейсе, формируется конкретный IP-адрес, поскольку источник туннелирования или автоматический узел существует там, где IP-интерфейсу сопоставлен IPv4 - адрес с самым меньшим номером. Этот источник IPv4 используется для установки идентификатора туннельного интерфейса, в соответствии с правилами адресации протокола ISATAP. Если для протокола ISATAP включен туннельный интерфейс, для интерфейса необходимо указать источник тунелирования, чтобы этот интерфейс стал активным.

Адрес ISATAP представляется в следующем виде: [64-битный префикс]:0:5EFE:w.x.y.z, где 5EFE является идентификатором ISATAP, а w.x.y.z - публичные или частные адреса IPv4. Таким образом, адрес локальной связи Link Local может быть представлен в виде FE80::5EFE:w.x.y.z

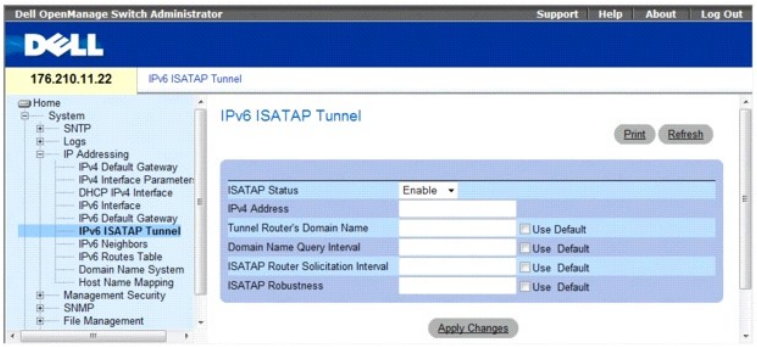
После удаления последнего IPv4-адреса с интерфейса, интерфейс ISATAP IP принимает негативное состояние и отображается как «отключенный», однако, при этом администрирование остается включенным.

При определении туннелирования, необходимо принимать во внимание следующее:

- Адрес локальной связи IPv6 назначается интерфейсу ISATAP. Первоначальный IP-адрес назначается этому интерфейсу, и интерфейс принимает активное состояние.
- Если интерфейс ISATAP является активным, IPv4 - адрес маршрутизатора ISATAP определяется системой DNS путем использования преобразования данных ISATAP - IPv4. Если запись ISATAP DNS не обнаружена, то начнется поиск преобразования данных ISATAP-имя хоста-адрес в кэше имен хоста.
- Если при процессе DNS адрес IPv4 маршрутизатора ISATAP не был определен, состояние интерфейса ISATAP IP остается *Активным*. Система не получит шлюз по умолчанию для трафика ISATAP до тех пор, пока процедура определения DNS не будет закончена.
- Для того, чтобы туннелирование по протоколу ISATAP работало правильно по сети IPv4 network, необходимо произвести установку маршрутизатора ISATAP.

Чтобы открыть страницу **IPv6 ISATAP Tunnel** (Туннелирование IPv6 ISATAP), выберите **System** (Система)→ **IP Addressing** (IP-адресация)→ **IPv6 ISATAP Tunnel** (Туннелирование IPv6 ISATAP) на панели дерева.

Рис. 6-32. Туннелирование IPv6 ISATAP



- **ISATAP Status (Состояние ISATAP).** Определяет состояние работы протокола ISATAP устройства. Возможные значения:
  - **Enable (Включено).** Работа протокола ISATAP на устройстве включена.
  - **Disable (Выключено).** Работа протокола ISATAP на устройстве выключена. Это значение по умолчанию.
- **IPv4 Address (адрес IPv4).** Указывает локальный адрес (источник) IPv4 туннельного интерфейса.
- **Tunnel Router's Domain Name (Имя домина туннельного маршрутизатора).** Указывает глобальное текстовое значение, которое представляет собой конкретное имя домина маршрутизатора автоматического туннелирования. По умолчанию установлено имя ISATAP.
  - **Use Default (Использовать стандартные установки).** Установка флажка на этой опии возвращает стандартные значения параметров установок.
- **Domain Name Query Interval (Интервал запроса доменного имени).** Определяет интервал между запросами системы DNS (перед определением IP-адреса маршрутизатора ISATAP), посылаемыми для автоматического определения доменного имени маршрутизатора автоматического туннелирования. Диапазон значений: 10 - 3600 секунд. Значение по умолчанию: 10 секунд.
  - **Use Default (Использовать стандартные установки).** Установка флажка на этой опии возвращает стандартные значения параметров установок.
- **ISATAP Router Solicitation Interval (Интервал запросов маршрутизатора ISATAP).** Указывает интервал между посылкой сообщений-запросов маршрутизатора, в случае отсутствия активного маршрутизатора. Диапазон значений: 10 - 3600 секунд. Значение по умолчанию:10.
  - **Use Default (Использовать стандартные установки).** Установка флажка на этой опии возвращает стандартные значения параметров установок.
- **ISATAP Robustness (Надежность ISATAP).** Указывает количество обновлении запросов DNS/ запросов маршрутизатора, которые пересылает устройство. Диапазон значений: 1 - 20 секунд. Значение по умолчанию: 3.
  - **Use Default (Использовать стандартные установки).** Установка флажка на этой опии возвращает стандартные значения параметров установок.

Определение параметров туннельного протокола с помощью команд консоли

В следующей таблице приведены команды консоли для настройки полей, отображаемых на странице **IPv6 ISATAP Tunnel** (Туннелирование IPv6 ISATAP).

Команда консоли	**Описание**
interface tunnel (туннель интерфейса) *number (номер)*	Вход в режим конфигурирования туннельного интерфейса.
tunnel mode ipv6ip {isatap}	Конфигурирует глобальный режим механизма переноса данных IPv6.
tunnel isatap router *router_name*	Конфигурирует глобальную строку, которая содержит доменное имя конкретного автоматического туннельного маршрутизатора.
tunnel source { **auto** | **ip-address** *ipv4-address* | *interface* }	Указывает локальный адрес (источник) IPv4 туннельного интерфейса.
tunnel isatap query-interval (интервал запросов туннеля ISATAP) *seconds (секунды)*	Определяет интервал между запросами системы DNS (перед определением IP-адреса маршрутизатора ISATAP), посылаемыми для автоматического определения доменного имени маршрутизатора автоматического туннелирования.
tunnel isatap solicitation-interval (интервал ответных сообщений на запросы туннеля ISATAP) *seconds (ctreyls)*	Указывает интервал между посылкой ответных сообщений на запросы маршрутизатора, в случае отсутствия активного маршрутизатора.
tunnel isatap robustness (надежность туннеля) *number (число)*	Указывает количество обновлении запросов DNS/ запросов маршрутизатора, которые пересылает устройство.
show ipv6 tunnel (показать туннель ipv6)	Выводит информацию о туннеле ISATAP.

Далее приведен пример команд консоли.

```
Console> show ipv6 tunnel

Router DNS name: ISATAP

Router IPv4 address: 172.16.1.1

DNS Query interval: 10 seconds

Min DNS Query interval: 0 seconds

Router Solicitation interval: 10 seconds

Min Router Solicitation interval: 0 seconds

Robustness: 3
```

Defining IPv6 Neighbors (Определение соседних узлов IPv6)

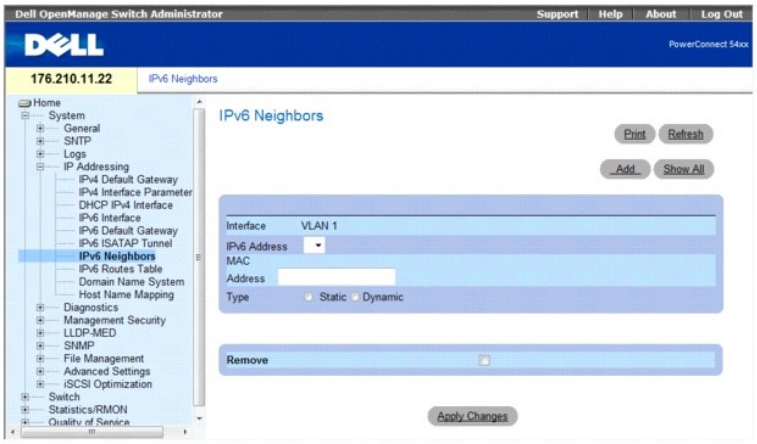
Страница **IPv6 Neighbors** (Соседние узлы IPv6) содержит информацию об определении соседних узлов IPv6, которая по своим функциональным свойствам аналогична странице *IPv4 Address Resolution Protocol (ARP) (Протокол определения адреса IPv4)*. Функция поиска соседних узлов IPv6 позволяет определить адреса локальных связей в пределах одной подсети и содержит базу данных для регистрации и поддержки информации о доступности путей к активным соседним узлам.

Устройство поддерживает до 256 соседних узлов, полученных статически или динамически.

При удалении интерфейса, все соседние узлы, определенные статически и динамически, будут также удалены.

Чтобы открыть страницу **IPv6 Neighbors** (Соседние узлы IPv6), выберите **System** (система)→ **IP Addressing** (IP-адресация)→ **IPv6 Neighbors** (Соседние узлы IPv6) на панели дерева.

Рис. 6-33. Соседние узлы IPv6



- **Interface (Интерфейс).** Отображает интерфейс, на котором определен интерфейс IPv6. В качестве интерфейсов могут использоваться порты, LAG или VLAN.
- **IPv6 Address (Адрес IPv6).** Определяет IPv6-адрес соседнего узла, который конфигурируется в данный момент.
- **MAC Address (MAC-адрес).** Отображает MAC-адрес, назначенный данному интерфейсу.
- **Type (Тип).** Отображает тип записи кэша при определении соседнего узла. Возможные значения:
  - **Static (Статический).** Показывает записи кэша статических соседних адресов. Если запись для конкретного IPv6-адреса уже существует в кэше данных по определению соседних узлов —это определяется в процессе поиска соседних узлов IPv6—вы можете преобразовать эту запись в статическую.
  - **Dynamic (динамический).** Показывает записи кэша динамических соседних адресов.
- **Remove (удаление).** Если выбрана эта опция, происходит удаление соседнего адреса из списка.

В таблице соседних узлов IPv6, также имеются следующие параметры:

State (Состояние). Отображает состояние соседнего узла IPv6. Возможные значения этого поля:

- **Incomplete (Не закончено).** Указывает, что процесс определения адреса еще идет, и адрес канального уровня соседнего узла по умолчанию еще не был определен.
- **Reachable (Доступен).** Указывает, что соседний узел определен и доступен (по состоянию на несколько десятков секунд до настоящего момента).
- **Stale (Состояние).** Указывает, что соседний больше не считается доступным, но, до тех пор, пока не было пересылки трафика к соседнему узлу, не было предпринято попыток определить его доступность.

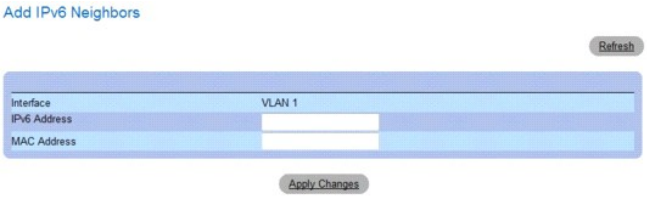
- **Delay (Задержка).** Указывает, что соседний узел более не рассматривается как доступный, и к соседнему узлу был послан трафик. Имеется кратковременная задержка в отсылке тестовых импульсов для того, чтобы протоколы верхнего уровня смогли собрать информацию о доступности соседнего узла.
- **Probe (Тестовый сигнал).** Указывает, что соседний узел более не рассматривается в качестве доступного, и для проверки его доступности посылаются тестовые сигналы-запросы одноадресной передачи определения соседних узлов.

Добавление соседнего узла IPv6

1. Откройте страницу **IPv6 Neighbors** (Соседние узлы IPv6).
2. Нажмите кнопку **Add** (Добавить).

   Откроется страница**Add IPv6 Neighbors** (добавить соседние узлы IPv6).

Рис. 6-34. Добавление соседних узлов IPv6



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

   Новый соседний узел будет добавлен, а устройство обновлено.

Изменение параметров соседнего узла

1. Откройте страницу **IPv6 Neighbors** (Соседние узлы IPv6).
2. Выберите IP-адрес в раскрывающемся списке **IPv6 Address** (Адрес IPv6).
3. Измените необходимые поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

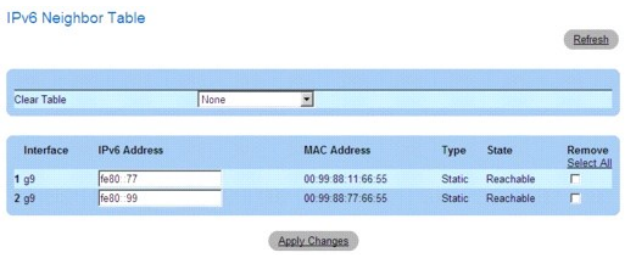
   Параметры будут изменены, а устройство обновлено.

Удаление соседних узлов

1. Откройте страницу **IPv6 Neighbors** (Соседние узлы IPv6).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **IPv6 Neighbors Table** (Таблица соседних узлов IPv6).

Рис. 6-35. Таблица соседних узлов IPv6



3. Поставьте флажок на опии **Remove** (Удалить) возле нужного узла. Другой способ - выберите нужное значение в поле **Clear Table** (Очистить таблицу). Возможные значения:
    - Static Only (Только статические). Удаляет записи для статических узлов таблицы соседних узлов IPv6.
    - Dynamic Only (Только динамические). Удаляет записи для динамических узлов таблицы соседних узлов IPv6
    - All Dynamic and Static (Динамические и статические). Удаляет все записи (статические и динамические) из таблицы соседних узлов IPv6.
    - None (Не удалять). Отмена удаления записей.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Выбранные соседние узлы будут удалены, а устройство обновлено.

Определение соседних узлов IPv6 с помощью команд консоли

В следующей таблице приведены команды консоли для настройки полей, отображаемых на странице **IPv6 Neighbors** (Соседние узлы IPv6).

Команда консоли	**Описание**
ipv6 neighbor *ipv6_addr hw_addr* {**ethernet** *interface-number* | **vlan** *vlan-id* | **port-channel** *number* }	Конфигурирует статистические записи кэша обнаружения соседних узлов IPv6.
show ipv6 neighbors {static | dynamic}[**ipv6-address** *ipv6-address*] [**mac-address** *mac-address*] [**ethernet** *interface-number* | **vlan** *vlan-id* | **port-channel** *number*]	Отображает информацию из кэша обнаружения соседних узлов IPv6.
clear ipv6 neighbors	Удаляет все записи из кэша обнаружения соседних узлов.

Далее приведен пример команд консоли.

```
Console# show ipv6 neighbors dynamic

Interface  IPv6 address              HW address        State

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

VLAN 1     2031:0:130F::010:B504:DBB4  00:10:B5:04:DB:4B  REACH

VLAN 1     2031:0:130F::050:2200:2AA4  00:50:22:00:2A:A4  REACH
```

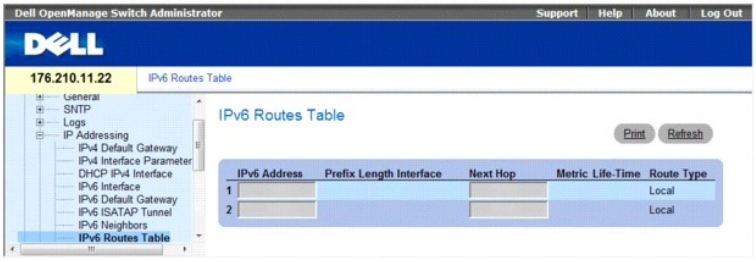
Просмотр таблицы маршрутов IPv6

Таблица маршрутов IPv6 **IPv6 Routes Table** хранит информацию о префиксах назначения адресов IPv6, и способе доступа к ним (прямом или косвенном). Таблица маршрутизации используется для определения адресов следующего скачка и интерфейса, используемого для переадресации.

Каждая динамическая запись имеет ассоциированное значение таймера недействительности (взятое из оповещения маршрутизатора), используемое для удаления записей, которые более не отображаются в оповещении.

Чтобы открыть страницу **IPv6 Routes Table** (Таблица маршрутов IPv6), выберите **System** (Система)→ **IP Addressing** (IP-адресация)→ **IPv6 Routes Table** (Таблица маршрутов IPv6) на панели дерева.

Рис. 6-36. Таблица маршрутов IPv6



- **IPv6 Address (Адрес IPv6).** Определяет IPv6-адрес назначения.
- **Prefix Length (Длина префикса).** Указывает длину префикса адреса IPv6. Поле префикса применяется только для статических адресов IPv6, определенных как глобальные адреса IPv6. Диапазон значений: 5 -128.
- **Interface (Интерфейс).** Отображает интерфейс, который используется для переадресации пакета. К интерфейсу может относиться любой

порт/LAG/VLAN.

- **Next Hop (Следующий скачок).** Определяет адрес, к которому переадресуется пакет, направленный по маршруту к адресу назначения (обычно это адрес соседнего маршрутизатора). В качестве этого адреса может использоваться адреса локальной связи или глобальные IPv6-адреса.
- **Metric (Метрика).** Указывает величину, используемую при сравнении этого маршрута с другими маршрутами с тем же местом назначения, находящимися в таблице маршрутизации IPv6. Это администрируемый параметр, с диапазоном изменения от 0 до 255. Значение по умолчанию - 1.
- **Life-Time (Срок службы).** Указывает срок службы маршрута.
- **Route Type (Тип маршрута).** Указывает, напрямую ли указано место назначения и способ определения этой записи. Возможны следующие значения::
  - **Local (Локальный).** Указывает прямую связь с записью маршрута.
  - **Static (Статический).** Указывает, что маршрут определен при работе процесса определения соседних узлов. Эта запись автоматически преобразуется в статическую запись.
  - **ICMP.** Указывает, что маршрут получен из сообщений ICMP.
  - **ND.** Указывает, что маршрут получен из сообщений алгоритма автоконфигурации.

Просмотр таблицы параметров маршрутизации IPv6 с помощью команд консоли

В следующей таблице приведены команды консоли для настройки полей, отображаемых на странице **IPv6 Routes Table** (Таблица маршрутов IPv6).

Команда консоли	**Описание**
traceroute {*ipv4-address* | *hostname*} [*size packet_size*] [*ttl max-ttl*] [**count** *packet_count*] [**timeout** *time_out*] [**source** *ip-address*] [**tos** *tos*]	Определяет маршруты, которые действительно принимают пакеты IPv4 при движении к месту назначения.
traceroute ipv6 {*ipv6-address* | *hostname*} [**size** *packet_size*] [**ttl** *max-ttl*] [**count** *packet_count*] [**timeout** *time_out*] [**source** *ip-address*] [**tos** *tos*]	Определяет маршруты, которые действительно принимают пакеты IPv6 при движении к месту назначения.
show ipv6 route	Отображает текущее состояние таблицы маршрутов IPv6.

Далее приведен пример команд консоли.

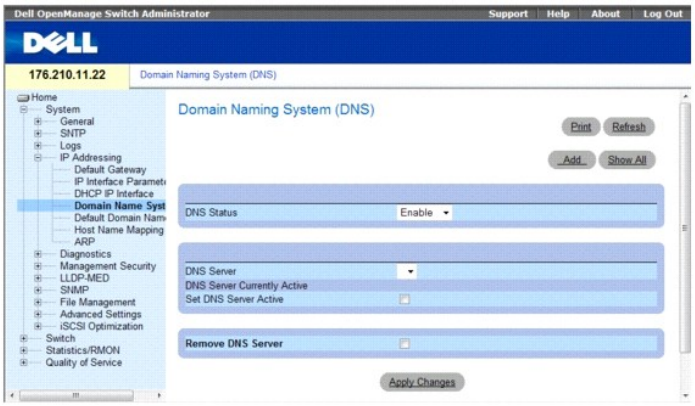
```
Console> show ipv6 route

Codes: L - Local, S - Static, I - ICMP, ND - Router Advertisment

The number in the brackets is the metric.

S ::/0 via fe80::77 [0] VLAN 1 Lifetime Infinite

ND ::/0 via fe80::200:cff:fe4a:dfa8 [0] VLAN 1 Lifetime 1784 sec

L 2001::/64 is directly connected, g2 Lifetime Infinite

L 2002:1:1:1::/64 is directly connected, VLAN 1 Lifetime 2147467 sec

L 3001::/64 is directly connected, VLAN 1 Lifetime Infinite

L 4004::/64 is directly connected, VLAN 1 Lifetime Infinite

L 6001::/64 is directly connected, g2 Lifetime Infinite
```

Настройка системы имен доменов

Система имен доменов (DNS) преобразует имена доменов, определенные пользователем, в IP-адреса. Каждый раз при назначении имени домина 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), на панели дерева выберите **System** (Система)→ **IP Addressing** (IP-адресация)→ **Domain Name System** (Система имен доменов).

Рис. 6-37. Система имен доменов



- **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.
- **Set DNS Server Active (Сделать сервер DNS активным).** активизирует сервер DNS, выбранный в поле **DNS Server** (Сервер DNS).
- **Remove DNS Server (Удалить сервер DNS).** когда выбран этот параметр, серверы DNS удаляются.

При определении нового сервера DNS, будут доступны следующие дополнительные параметры:

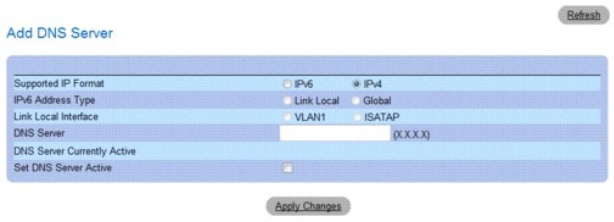
- **Supported IP Format (Поддерживаемый формат IP-адресов).** Отображает формат IP-адресов, поддерживаемый сервером. Возможные значения:
  - **IPv6.** поддержка IP версии 6
  - **IPv4.** поддержка IP версии 4.
- **IPv6 Address Type (Тип адреса IPv6).** В случае, если сервер поддерживает систему IPv6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

Добавление сервера DNS

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

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

Рис. 6-38. Добавление сервера DNS



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

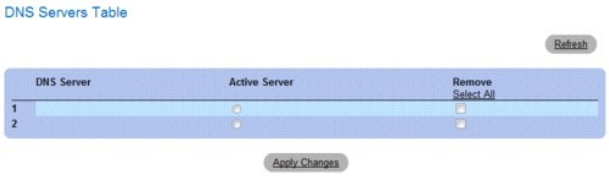
   Будет определен новый сервер DNS, а устройство обновлено.

Отображение таблицы серверов DNS

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

   Откроется страница **DNS Server Table** (Таблица серверов DNS).

Рис. 6-39. 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 системной информации устройства.

Команда консоли	**Описание**
ip name-server *адрес_сервера*	Задает доступные имена серверов. Можно определить до восьми имен серверов.
no ip name-server *адрес_сервера*	Удаляет имя сервера.
ip domain-name *имя*	Определяет имя домена по умолчанию, которое используется программой, если имена хостов указаны неправильно.
clear host {*имя* | *}	Удаляет записи из кэша имя хоста-адрес.
show hosts [*имя*]	Отображает имя домена по умолчанию, список хостов сервера имен, статические имена и адреса, а также список имен и адресов из кэша.

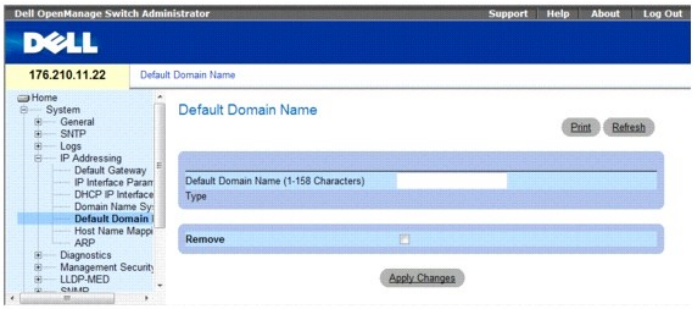
Далее приведен пример команд консоли.

```
console> enable

Console# configure

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), на панели дерева выберите **System** (Система)→ **IP Addressing** (IP-адресация)→ **Default Domain Name** (Имя домена по умолчанию).

Рис. 6-40. Имя домена по умолчанию



- **Default Domain Name (1-158 characters) (Имя домена по умолчанию (1-158 символов).** содержит имя сервера доменов DNS, определяемое пользователем. Когда выбран этот параметр, имя домена DNS является доменом по умолчанию.
- **Type (Тип).** тип домена, показывающий, как создан домен - статически или динамически.
- **Remove (Удалить).** когда этот флажок установлен, выбранный домен удаляется.

Определение имен доменов DNS с помощью команд консоли

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

Команда консоли	Описание
ip domain-name ***имя***	Определяет имя домена по умолчанию, которое используется программой, если имена хостов указаны неправильно.
no ip domain-name	Отключает использованием системы имен доменов (DNS).
show hosts [*имя*]	Отображает имя домена по умолчанию, список хостов сервера имен, статические имена и адреса, а также список имен и адресов из кэша.

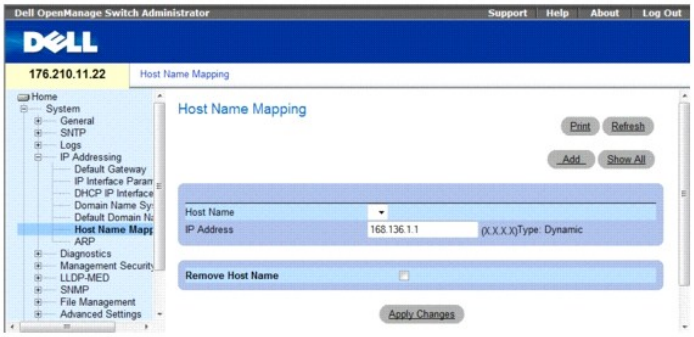
Далее приведен пример команд консоли.

```
console> enable

console# configure

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

Отображение хоста домина

Страница **Host Name Mapping** (Отображение имени хоста) содержит параметры для назначения статических IP-адресов для имен хостов. Страница **Host Name Mapping** (Отображение имени хоста) предоставляет до восьми IP-адресов 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. 6-41. Отображение имени хоста



- **Host Name (Имя хоста).** содержит список имен хостов. Имя хоста определяется на странице **Add Host Name Mapping** (Добавление отображения имени хоста). Каждый хост предоставляет до восьми IP-адресов. Возможны следующие значения поля Host Name (Имя хоста):
- **IP Address (X.X.X.X) (IP-адрес).** предоставляет до восьми IP-адресов, которые назначаются 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.

При определении нового имени хоста, будут доступны следующие дополнительные параметры:

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

Добавление имен домина 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. 6-42. Добавление отображения имени хоста

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

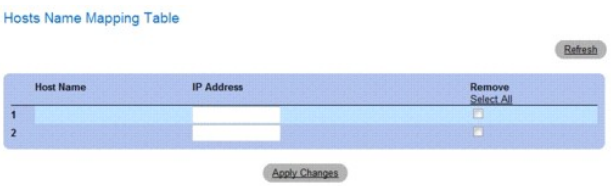
   IP-адрес будет сопоставлен с именем хоста, а устройство коммутатора обновлено.

Отображение таблицы отображения имен хостов

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

   Откроется страница **Hosts Name Mapping Table** (Таблица отображения имен хостов).

Рис. 6-43. Таблица отображения имен хостов



Удаление имени хоста из таблицы отображения IP-адресов

1. Откройте страницу **Host Name Mapping** (Отображение имени хоста).
2. Нажмите кнопку **Show All** (Показать все)
3. Откроется страница **Host Mapping Table** (Таблица отображения хостов).
4. Выберите запись **таблицы отображения хостов**.
5. Установите флажок **Remove** (Удалить).
6. Нажмите кнопку **Apply Changes** (Применить изменения).

   Запись **Host Mapping Table** (Таблица отображения хостов) будет удалена, а устройство коммутатора обновлено.

Сопоставление IP-адресов с именами хостов домина с помощью команд консоли

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

Команда консоли	**Описание**
ip host name address1 [address2 ... address8]	Определяет соответствие статических имен хостов адресам в кэше хоста для IPv4.
no ip host name	Улаляет связь имени и адреса для IPv4.
ipv6 host name ipv6-address1 [ipv6-address2 ... ipv6-address8]	Определяет соответствие статических имен хостов адресам в кэше хоста для IPv6.
no ipv6 host name	Улаляет связь имени и адреса для IPv6.
clear host {имя | *}	Удаляет записи из кэша имя хоста-адрес.
show hosts [name]	Отображает имя домина по умолчанию, список хостов сервера имен, статические имена и адреса, а также список имен и адресов из кэша.

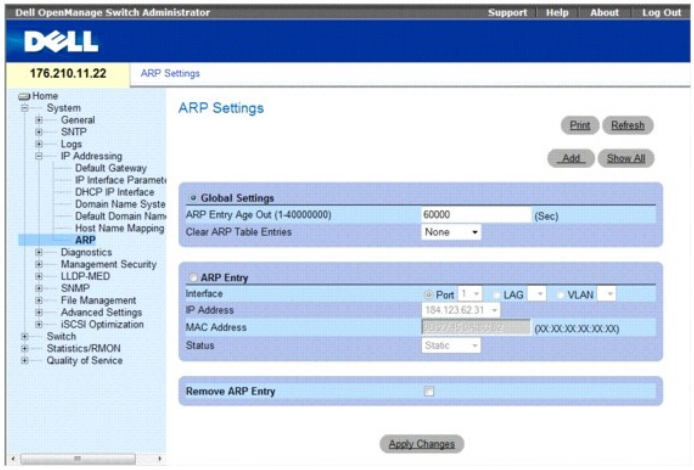
Далее приведен пример команд консоли.

```
console# enable

console# configure

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

Настройка протокола ARP

Протокол разрешения адресов Address Resolution Protocol (ARP). это протокол TCP/IP для преобразования IP-адресов в физические адреса. Статические записи можно определить в **ARP Table** (Таблице ARP). При определении статической записи в таблицу помещается постоянная запись, которую используется для перевода IP-адресов в MAC-адреса. Чтобы открыть страницу **ARP Settings** (Параметры ARP), на панели дерева выберите **System** (Система)→ **IP Addressing** (IP-адресация)→ **ARP**.

Рис. 6-44. Параметры ARP



- **Global Settings (Общие параметры).** выберите этот параметр, чтобы активизировать поля общих параметров ARP.
- **ARP Entry Age Out (1-40000000) (Срок хранения записи ARP).** время (в секундах) для всех устройств, которое проходит между запросами ARP по записям таблицы ARP. По истечении этого периода запись удаляется из таблицы. Диапазон значений: 0 - **4000000**, ноль указывает, что запись никогда не удаляется из кэша. Значение по умолчанию: 60000 секунд.
- **Clear ARP Table Entries (Удалить записи таблицы ARP).** тип записей ARP, которые удаляются на всех устройствах. Возможные значения:
  - **None (Нет).** записи ARP не удаляются.
  - **All (Все).** все записи ARP удаляются.
  - **Dynamic (Динамические).** удаляются только динамические записи ARP.
  - **Static (Статические).** удаляются только статические записи ARP.
- **ARP Entry (Запись ARP).** выберите этот параметр, чтобы активизировать поля параметров ARP для одного устройства.
- **Interface (Интерфейс).** номер интерфейса порта, группы LAG или VLAN, которые подключены к устройству.
- **IP Address (IP-адрес).** IP-адрес станции, который связан с MAC-адресом, указанным ниже.
- **MAC Address (MAC-адрес).** MAC-адрес станции, который связан с IP-адресом в таблице ARP.
- **Status (Состояние).** состояние записи таблицы ARP. Возможные значения этого поля:
  - **Dynamic (Динамическая).** запись ARP распознается динамически.
  - **Static (Статическая).** запись ARP - статическая.
- **Remove ARP Entry (Удалить запись ARP).** когда установлен этот флажок, запись ARP удаляется.

Добавление статической записи таблицы ARP:

1. Откройте страницу **ARP Settings** (Параметры ARP).
2. Нажмите кнопку **Add** (Добавить).

   Откроется страница **Add ARP Entry** (Добавление записи ARP).

Рис. 6-45. Добавление записи ARP

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

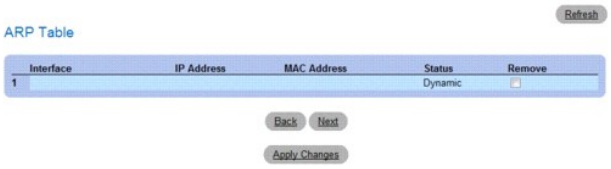
Запись **ARP Table** (Таблица ARP) будет добавлена, а устройство обновлено.

Отображение таблицы ARP

1. Откройте страницу **ARP Settings** (Параметры ARP).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **ARP Table** (Таблица ARP).

Рис. 6-46. Таблица ARP



Удаление записи таблицы ARP

1. Откройте страницу **ARP Settings**
2. (Параметры ARP)Нажмите кнопку **Show All** (Показать все).

   Откроется страница **ARP Table** (Таблица ARP).
3. Выберите запись таблицы.
4. Установите флажок **Remove** (Удалить).
5. Нажмите кнопку **Apply Changes** (Применить изменения).

   Выбранная запись таблицы **ARP Table** будет удалена, а устройство обновлено.

Настройка ARP с помощью команд консоли

В следующей таблице приведены команды консоли для настройки полей, отображаемых на странице **ARP Settings** (Параметры ARP).

Команда консоли	**Описание**
arp *ip_адрес hw_адрес* {**ethernet** *номер_интерфейса* | **vlan** *идентификатор_vlan*| **port-channel** *номер*}	Добавляет постоянную запись в кэш ARP.
arp timeout секунды	Настраивает срок хранения записи в кэше ARP.
clear arp-cache	Удаляет все динамические записи из кэша ARP
show arp	Выводит записи таблицы ARP.
no arp	Удаляет запись ARP из таблицы ARP Table.

Далее приведен пример команд консоли.

```
Console(config)# arp 198.133.219.232 00-00-0c-40-0f-bc

Console(config)# exit

Console# arp timeout 12000

Console# show arp

ARP timeout: 80000 Seconds
```

Interface	IP address	HW address	Status

| --- | --- | --- | --- |
| g1 | 10.7.1.102 | 00:10:B5:04:DB:4B | Dynamic |
| g2 | 10.7.1.135 | 00:50:22:00:2A:A4 | Static |

Запуск диагностики кабелей

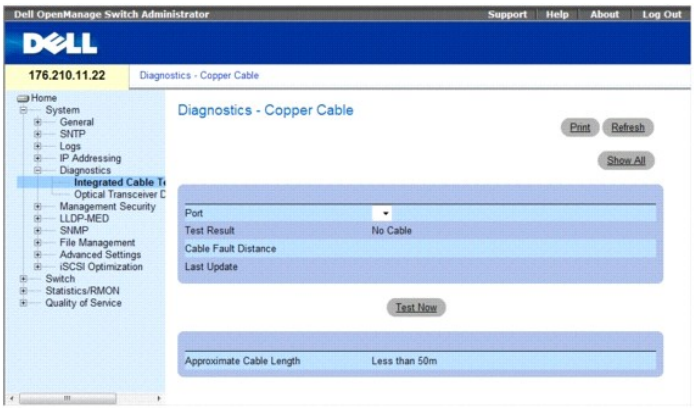
Страница **Diagnostics** (Диагностика) содержит ссылки на страницы, которые используются для виртуального тестирования медных и оптоволоконных кабелей. Чтобы открыть страницу **Diagnostics** (Диагностика), на панели дерева выберите **System** (Система)→ **Diagnostics** (Диагностика).

Просмотр диагностики медных кабелей

Страница **Integrated Cable Test for Copper Cables** (Интегрированное тестирование медных кабелей) содержит поля для выполнения тестирования медных кабелей. В ходе тестирования кабеля отображается информация о неисправностях кабеля, времени выполнения последнего теста кабеля и типе неисправности кабеля. В тестах используется технология TDR (Time Domain Reflectometry) для проверки качества и характеристик медного кабеля, подключенного к порту. Можно тестировать кабели длиной до 120 метров. Проверка кабелей выполняются при отключенных портах. Исключение составляет тест примерной длины кабеля (Approximated Cable Length). Длина кабеля, возвращаемая процедурой тестирования, усредняется до следующих величин: до 50 метров, от 50 до 80 метров, от 80 до 110 метров, от 110 до 120 метров или более 120 метров. Отклонение может составлять до 20 метров.

Чтобы открыть страницу **Integrated Cable Test for Copper Cables** (Интегрированное тестирование медных кабелей), на панели дерева выберите **System** (Система)→ **Diagnostics** (Диагностика)→ **Integrated Cable Test** (Интегрированное тестирование кабеля).

Рис. 6-47. Интегрированное тестирование медных кабелей



- **Port (Порт).** порт, к которому подключен кабель.
- **Test Result (Результат теста).** результаты теста кабеля. Возможные значения:
  - **No Cable (Нет кабеля).** кабель не подключен к порту.
  - **Open Cable (Оборванный кабель).** кабель подключен только с одной стороны.
  - **Short Cable (Короткозамкнутый кабель).** короткое замыкание в кабеле.
  - **OK.** кабель прошел тестирование.
  - **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 **Integrated Cable Test for Copper Cables** (Интегрированное тестирование медных кабелей).
3. Щелкните **Test Now** (Тестировать).

   Будет выполнен тест медного кабеля и результаты будут отображены на странице **Integrated Cable Test for Copper Cables** (Интегрированное тестирование медных кабелей).

Отображение таблицы результатов виртуального тестирования кабелей

1. Откройте страницу **Integrated Cable Test for Copper Cables** (Интегрированное тестирование медных кабелей).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **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.

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

Далее приведен пример команд консоли.

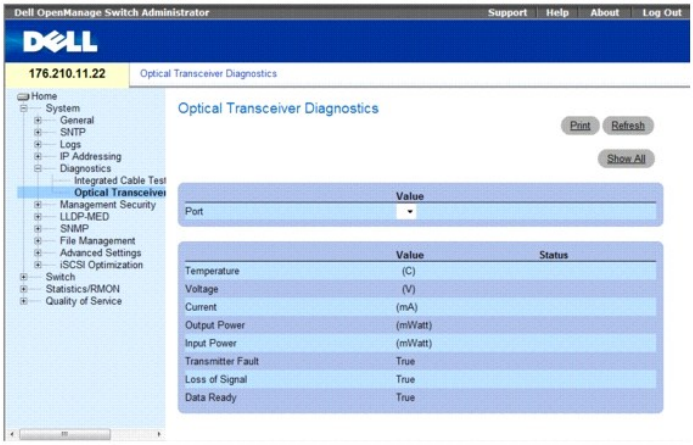
```
console> enable

Console# test copper-port tdr g3

Cable is open at 100 meters.

Console> show copper-ports tdr
```

Port	Result	Length [meters]	Date
----	------	----------	----
g1	OK		
g2	Short	50	13:32:00 15 January 2004
g3	Test has not been performed		
g4	Open	64	13:32:00 15 January 2004

Просмотр диагностики оптического трансивера

Страница **Optical Transceiver Diagnostics** (Диагностика оптического трансивера) содержит поля для выполнения тестов оптоволоконных кабелей. Диагностика оптического трансивера может быть выполнена только в том случае, если установлено соединение. Чтобы открыть страницу **Optical Transceiver Diagnostics** (Диагностика оптического трансивера), на панели дерева выберите **System** (Система)→ **Diagnostics** (Диагностика)→ **Optical Transceiver Diagnostics** (Диагностика оптического трансивера).

Рис. 6-48. Диагностика оптического трансивера



- **Port (Порт).** порт, к которому подключен оптоволоконный кабель.
- **Temperature (Температура).** рабочая температура кабеля (в градусах Цельсия).
- **Voltage (Напряжение).** рабочее напряжение кабеля.
- **Current (Ток).** рабочий ток кабеля.
- **Output Power (Выходная мощность).** значение выходной мощности.
- **Input Power (Входная мощность).** значение входной мощности.
- **Transmitter Fault (Сбой передатчика).** указывает, что произошла ошибка во время передачи.
- **Loss of Signal (Потеря сигнала).** указывает, возникла ли потеря сигнала.
- **Data Ready (Готовность к передаче данных).** на трансивер подается питание и он готов к передаче данных.

Отображение таблицы тестов диагностики оптического трансивера

1. Откройте страницу **Optical Transceiver Diagnostics** (Диагностика оптического трансивера).
2. Нажмите кнопку **Show All** (Показать все).

   Будет выполнена проверка и откроется страница **Virtual Cable Test Results Table** (Таблица результатов виртуального тестирования кабелей).

   Таблица **Optical Transceiver Diagnostics Table** (Таблица диагностики оптического трансивера) содержит следующие столбцы:

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

Трансиверы Finisar не поддерживают диагностический тест неисправности.

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

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

Выполнение тестирования оптоволоконных кабелей с помощью команд консоли

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

Команда консоли	**Описание**
show fiber-ports optical-transceiver [*интерфейс*][**detailed**]	Отображает данные диагностики оптического трансивера.

Далее приведен пример команды консоли:

```
console> enable

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

				Power			
Port	Temp (C)	Voltage (Volt)	Current (mA)	Output (mWatt)	Input (mWatt)	TX Fault	LOS
21	W	OK	OK	OK	OK	OK	OK
22	OK	OK	OK	OK	OK	E	OK
23	Copper						

```
Temp – Internally measured transceiver temperature.
```

```
Voltage - Internally measured supply voltage.

Current – Measured TX bias current.

Output Power – Measured TX output power.

Input Power – Measured RX received power.

Tx Fault – Transmitter fault

LOS – Loss of signal
```

Управление безопасностью устройств

Страница **Management Security** (Безопасность управления) предоставляет доступ на страницы, содержащие поля для настройки параметров безопасности для портов, методов управления устройством, пользователя и безопасности сервера. Чтобы открыть страницу **Management Security** (Безопасность управления), на панели дерева выберите **System** (Система)→ **Management Security** (Безопасность управления).

Defining Access Profiles (Определение профилей доступа)

Страница **Access Profiles** (Профили доступа) содержит поля для определения профилей и правил для доступа к устройству. Можно ограничить доступ к функциям управления группам пользователей, которые определены входящими интерфейсами и исходными IP-адресами или маской исходной подсети.

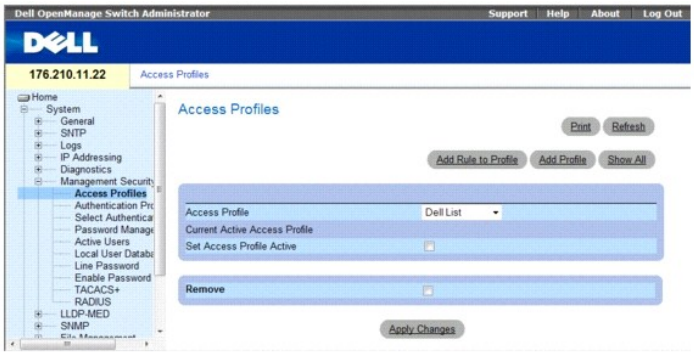
Доступ к управлению может быть отдельно определен для каждого метода доступа для управления, включая Web (HTTP), безопасный web (HTTPS), Telnet, безопасный Telnet и SNMP.

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) содержит поля для настройки списков управления и назначения их для определенных интерфейсов. Чтобы открыть страницу **Access Profiles** (Профили доступа), на панели дерева выберите **System** (Система)→ **Management Security** (Безопасность управления)→ **Access Profiles** (Профили доступа).

Рис. 6-49. Профили доступа



- **Access Profile (Профиль доступа).** список определенных пользователем профилей. Список **Access Profile** (Профиль доступа) содержит значения по умолчанию из **Console List** (Списка консоли), к которому добавляются профили, определенные пользователем. Если выбрать Console Only (Только консоль) в качестве имени **Access Profile** (Профиль 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 профиля доступа).

Активизация профиля

1. Откройте страницу **Access Profiles** (Профили доступа).
2. Выберите профиль доступа в поле **Access Profile** (Профиль доступа).

3. Установите флажок **Set Access Profile Active** (Активизировать профиль доступа).

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

   Профиль доступа будет активирован.

Добавление профиля доступа

Правила служат фильтрами для определения приоритетов правил, метода управления устройством, типа интерфейса, IP-адреса источника и сетевой маски, а также действия при доступе для управления устройством. Доступ пользователей для управления может быть разрешен или заблокирован. Приоритет правил задает порядок применения правил профиля.

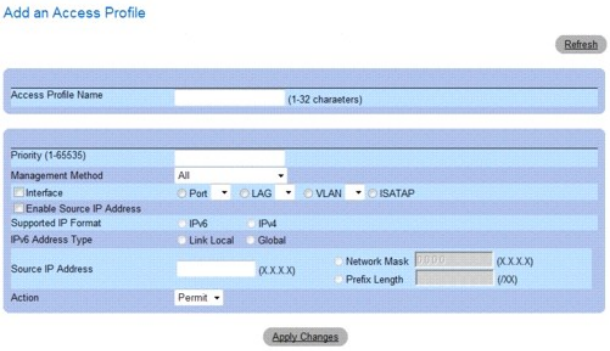
Определение правил для профиля доступа:

1. Откройте страницу **Access Profiles** (Профили доступа).

2. Щелкните **Add an Access Profile** (Добавить профиль доступа).

   Откроется страница **Add An Access Profile** (Добавление профиля доступа).

Рис. 6-50. Добавление профиля доступа



- **Access Profile Name (1-32 Characters) (Имя профиля доступа).** определенное пользователем имя профиля доступа.
- **Rule Priority (1-65535) (Приоритет правила).** 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. Это правило можно применять для выбранного порта, LAG или VLAN путем установки флажка и выбора соответствующей кнопки и интерфейса. Назначение профиля доступа интерфейсу закрывает доступ через другие интерфейсы. Если профиль доступа не назначен ни для одного интерфейса, устройство будет доступно для всех интерфейсов.
- **Enable Source IP Address (Включить IP-адрес источника).** Установите флажок на этом параметре для того, чтобы сузить условия, основанные на IP-адресе источника. Если флажок снят, IP-адрес источника не может быть введен в сконфигурированное правило.
- **Supported IP Format (Поддерживаемый формат IP-адресов).** Отображает формат IP-адресов. Возможные значения:
  - **IPv6.** поддержка IP версии 6.
  - **IPv4.** поддержка IP версии 4.
- **IPv6 Address Type (Тип адреса IPv6).** В случае, если сервер поддерживает систему IPv6 (см. предыдущий параметр), здесь указывается поддерживаемый тип статических адресов. Возможные значения:
  - **Link Local (Локальная связь).** Адрес локальной связи, который не маршрутизируется, а используется только для связи в пределах той же сети.
  - **Global (Глобальный).** Глобальный уникальный адрес IPv6 address; он является видимым и доступным для различных подсетей.
- **Source IP Address (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. Определите поле **Access Profile Name** (Имя профиля доступа).
4. Определите соответствующие поля.
5. Нажмите кнопку **Apply Changes** (Применить изменения).

   Новый профиль доступа будет добавлен, а устройство обновлено.

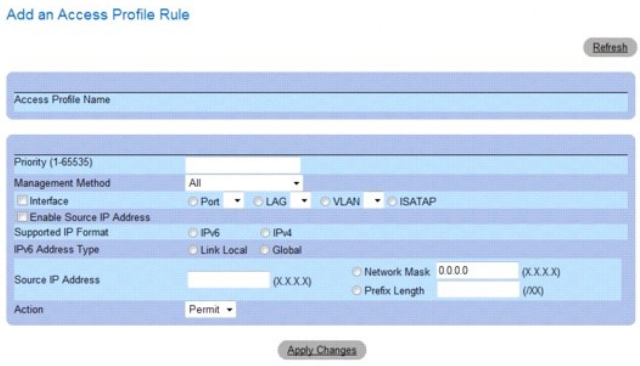
Добавление правил для профиля доступа

Первое правило необходимо определить для запуска соответствующего трафика на профили доступа.

1. Откройте страницу **Access Profiles** (Профили доступа).
2. Щелкните **Add Profile to Rule** (Добавить профиль для правила).

   Откроется страница **Add An Access Profile Rule**.

Рис. 6-51. Add An Access Profile Rule (Добавление правила профиля доступа)



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

   Правило будет добавлено в профиль доступа, а устройство обновлено.

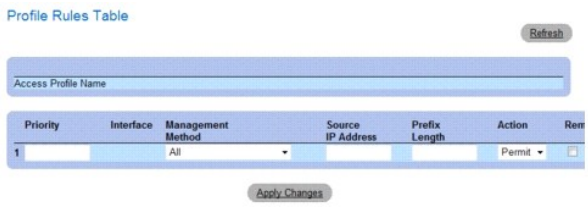
Просмотр таблицы правил профиля:

Порядок, в котором правила отображаются в таблице *Profile Rules Table* (Таблица правил профиля), имеет значение. Пакеты сравниваются с первым правилом, которое отвечает критериям правила.

1. Откройте страницу **Access Profiles** (Профили доступа).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **Profile Rules Table Page** (Таблица правил профиля).

Рис. 6-52. Profile Rules Table (Таблица правил профиля)



Удаление правила

1. Откройте страницу **Access Profiles** (Профили доступа).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **Profile Rules Table** (Таблица правил профиля).
3. Выберите правило.
4. Установите флажок **Remove** (Удалить).
5. Нажмите кнопку **Apply Changes** (Применить изменения).

   Выбранное правило будет удалено, а устройство обновлено.

Определение профилей доступа с помощью команд консоли

В следующей таблице приведены команды консоли для настройки полей, отображаемых на странице Access Profiles (Профили доступа).

Команда консоли	**Описание**
management access-list *имя*	Определяет список доступа для управления и вводит контекст списка доступа для конфигурации.
permit [**ethernet** *номер_интерфейса* | **vlan** *идентификатор_vlan* | **port-channel** *номер*] [**service** *служба*]	Задает разрешающие условия для списка доступа для управления для порта
permit ip-source {*ipv4-address* | *ipv6-address / prefix-length}* [**mask** *mask* | *prefix-length*] [**ethernet** *interface-number* | **vlan** *vlan-id* | **port-channel** *number*] [**service** *service*]	Задает для порта разрешающие условия списка доступа для управления и выбранный метод управления.
deny [**ethernet** *номер_интерфейса* | **vlan** *идентификатор_vlan* | **port-channel** *номер*] [**service** *служба*]	Задает для порта запрещающие условия списка доступа для управления и выбранный метод управления.
deny ip-source {*ipv4-address* | *ipv6-address / prefix-length}* [**mask** *mask* | *prefix-length*] [**ethernet** *interface-number* | **vlan** *vlan-id* | **port-channel** *number*] [**service** *service*]	Задает для порта запрещающие условия списка доступа для управления и выбранный метод управления.
management access-class {**console-only** | *имя*}	Определяет, какой список доступа используются в качестве активных соединений для управления.
show management access-list [*имя*]	Отображает активные списки доступа для управления.
show management access-class	Отображает информацию о классе доступа для управления.

Далее приведен пример команд консоли.

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

Console (config-macl)# permit ethernet g1

Console (config-macl)# permit ethernet g9

Console (config-macl)# deny ethernet g2

Console (config-macl)# deny ethernet g10

Console (config-macl)# exit

Console (config)# management access-class mlist

Console(config)# exit

Console# show management access-list

mlist

-----

permit ethernet g1

permit ethernet g9

! (Note: all other access implicitly denied)

Console> show management access-class

Management access-class is enabled, using access list mlist
```

Определение профилей проверки подлинности

Страница **Authentication Profiles** (Профили проверки подлинности) содержит поля для выбора метода проверки подлинности пользователя на устройстве. Идентификация пользователя происходит:

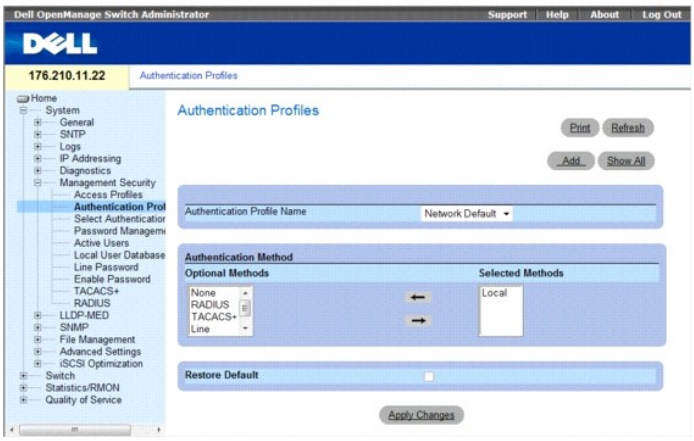
- Локально
- Через внешний сервер

Для идентификации пользователя также можно задать значение *None* (Нет).

Проверка подлинности пользователя происходит в том порядке, в каком выбраны методы. Например, если выделены и параметр *Local* (Локально), и параметр *RADIUS*, пользователи сначала идентифицируются локально. Если локальная пользовательская база данных пуста, то пользователь идентифицируется через сервер RADIUS.

Если при проверке подлинности происходит ошибка, используется следующий выбранный метод. Чтобы открыть страницу **Authentication Profiles** (Профили проверки подлинности), выберите **System** (Система)→ **Management Security** (Безопасность управления)→ **Authentication Profiles** (Профили проверки подлинности) на панели дерева.

Рис. 6-53. Authentication Profiles (Профили проверки подлинности)



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 см. в разделе **Configuring RADIUS Global Parameters** (Настройка общих параметров сервера RADIUS).
  - **Line (Канал).** для проверки подлинности пользователя используется пароль канала связи.
  - **Enable (Включение).** для проверки подлинности используется пароль включения.
  - **TACACS+.** проверка подлинности выполняется на сервере TACACS+.
- **Restore Default (Восстановить значения по умолчанию).** восстанавливает значения по умолчанию для метода проверки подлинности пользователя на устройстве.

Выбор профиля проверки подлинности:

1. Откройте страницу **Authentication Profiles** (Профили проверки подлинности).
2. Выберите профиль в поле **Authentication Profile Name** (Имя профиля проверки подлинности).
3. С помощью клавиш со стрелками выберите метод проверки подлинности.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

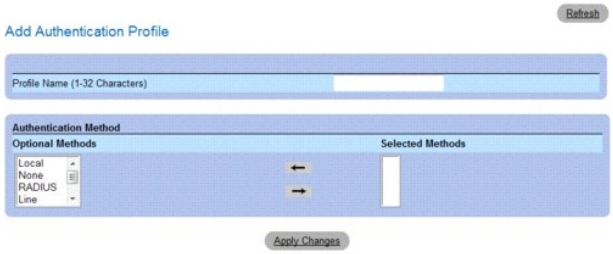
   Профиль проверки подлинности для этого устройства будет изменен.

Добавление профиля проверки подлинности:

1. Откройте страницу **Authentication Profiles** (Профили проверки подлинности).
2. Нажмите кнопку **Add** (Добавить).

   Откроется страница **Add Authentication Method Profile Name** (Добавить имя профиля проверки подлинности).

Рис. 6-54. Add Authentication Profile (Добавление профиля проверки подлинности)



3. Настройте профиль.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

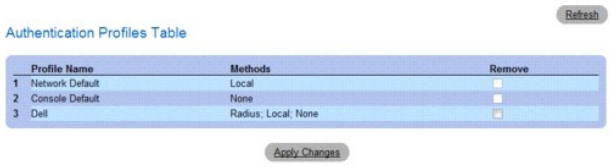
   Профиль проверки подлинности для этого устройства будет изменен.

Отображение страницы Show All Authentication Profiles (Отображение всех профилей проверки подлинности)

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

   Откроется страница **Authentication Profile** (Профиль проверки подлинности).

Рис. 6-55. Authentication Profiles (Профили проверки подлинности)



Удаление профиля проверки подлинности

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

   Откроется страница **Authentication Profile** (Профиль проверки подлинности).

3. Выберите профиль проверки подлинности.
4. Установите флажок **Remove** (Удалить).
5. Нажмите кнопку **Apply Changes** (Применить изменения).

   Выбранный профиль проверки подлинности будет удален.

Настройка профиля проверки подлинности с помощью команд консоли

В следующей таблице приведены команды консоли для настройки полей, отображаемых на странице **Authentication Profiles** (Профили проверки подлинности).

Команда консоли	Описание
aaa authentication login {**default** | *имя_списка*} *метод1* [*метод2*.]	Настраивает проверку подлинности при входе в систему.
no aaa authentication login {**default** | *имя_списка*}	Удаляет профиль проверки подлинности при входе в систему.

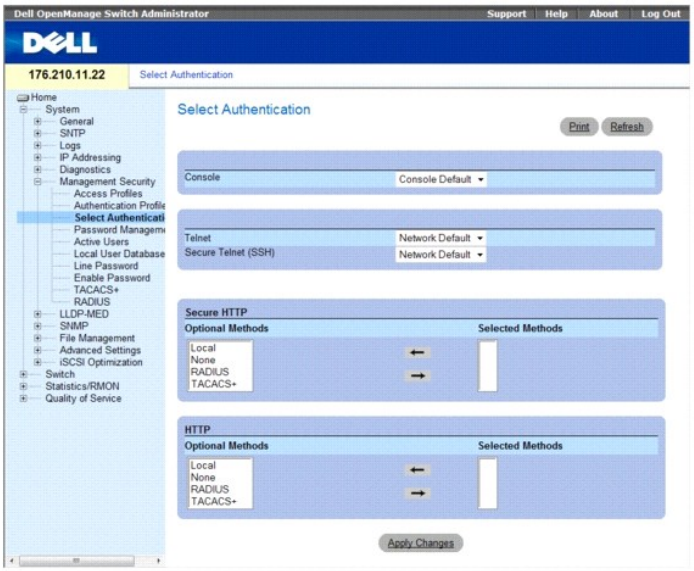
Далее приведен пример команд консоли.

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

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

Назначение профилей проверки подлинности

После того как профили проверки подлинности определены, их можно применить к методам доступа для управления. Например, проверка подлинности пользователей консоли может выполняться по списку методов проверки подлинности 1, а проверка подлинности пользователей Telnet - 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. 6-56. Select Authentication (Выбор проверки подлинности)



- **Console (Консоль).** профили проверки подлинности, используемые для проверки подлинности пользователей консоли.
- **Telnet.** профили проверки подлинности, используемые для проверки подлинности пользователей Telnet.
- **Secure Telnet (SSH).** профили проверки подлинности, используемые для проверки подлинности пользователей Secure Shell (SSH).Протокол SSH предоставляет клиентам безопасные и шифрованные удаленные соединения с устройством.
- **HTTP** и **Secure HTTP.** метод проверки подлинности, используемый для доступа к HTTP и Secure HTTP, соответственно. Возможные значения этого поля:
  - **None (Нет).** для доступа не используется никакой метод проверки подлинности пользователя.
  - **Local (Локально).** проверка подлинности выполняется локально.
  - **RADIUS.** проверка подлинности выполняется на сервере RADIUS.
  - **TACACS+.** проверка подлинности выполняется на сервере TACACS+.

Применение списка методов проверки подлинности к сеансам консоли

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

Сеансам консоли будет назначен список проверки подлинности.

Применение списка проверки подлинности к сеансам Telnet

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

   Сеансам Telnet будет назначен список проверки подлинности.

Применение профилей проверки подлинности к сеансам Secure Telnet (SSH)

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

   Сеансам Secure Telnet (SSH) будет назначен профиль проверки подлинности.

Назначение сеансам HTTP последовательности проверки подлинности

1. Откройте страницу **Select Authentication** (Выбор проверки подлинности).
2. Выберите последовательность проверки подлинности в поле **HTTP**.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

   Сеансам HTTP будет назначена последовательность проверки подлинности.

Назначение сеансам Secure HTTP последовательности проверки подлинности

1. Откройте страницу **Select Authentication** (Выбор проверки подлинности).
2. Выберите последовательность идентификации в поле **Secure HTTP**.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

   Сеансам Secure HTTP будет назначена последовательность проверки подлинности.

Назначение профилей или последовательностей проверки подлинности доступа с помощью команд консоли

В следующей таблице приведены команды консоли для настройки полей, отображаемых на странице **Select Authentication** (Выбор проверки подлинности).

Команда консоли	**Описание**
enable authentication [**default** | *имя_списка*]	Указывает список методов проверки подлинности при доступе на уровень с более высокими привилегиями в сеансе удаленного доступа Telnet или консоли.
login authentication [**default** | *имя_списка*]	Указывает список методов проверки подлинности для входа в систему с удаленного подключения Telnet или консоли.
ip http authentication *метод1* [*метод2*.]	Определяет методы проверки подлинности для серверов HTTP.
ip https authentication *метод1* [*метод2*.]	Определяет методы проверки подлинности для серверов HTTPS.
show authentication methods	Отображает информацию о методах проверки подлинности.

Далее приведен пример команд консоли.

```
      Console (config-line)# enable authentication default

      Console (config-line)# login authentication default

      Console (config-line)# exit

      Console (config)# ip http authentication radius local

      Console (config)# ip https authentication radius local

      Console(config)# exit

      Console# show authentication methods

Login Authentication Method Lists

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

Default: Radius, Local, Line

Console_Login: Line, None


Enable Authentication Method Lists

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

Default: Radius, Enable

Console_Enable: Enable, None




Line Login Method List Enable Method List

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

Console Console_Login Console_Enable

Telnet Default Default

SSH Default Default


HTTP: Radius, local

HTTPS: Radius, local

Dot1x: Radius
```

Управление паролями

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

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

Отсчет срока действия пароля начинается сразу после включения функции управления паролями. Сроки действия паролей определяются временем/датой, установленными пользователем. За десять дней до окончания действия пароля на устройстве отобразится соответствующее предупреждение.

После окончания срока действия пароля пользователь сможет войти в систему еще три раза. Во время трех последних входов в систему будут отображаться дополнительные сообщения, информирующие пользователя о необходимости немедленной смены пароля. Если пароль не будет изменен, вход пользователя в систему будет заблокирован. Пользователь сможет войти в систему только через консоль. Предупреждения относительно паролей записываются в файле *Syslog*.

При переопределении уровня привилегий необходимо также переопределить пользователя. Однако срок действия пароля истекает на основе начального определения пользователя.

Перед истечением срока действия пароля пользователь получает соответствующее предупреждение и запрос на смену пароля. Однако это предупреждение не отображается для веб-пользователей.

Для управления паролями поддерживается функция информационного центра.

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

Рис. 6-57. Password Management (Управление паролями)

Страница **Password Management** (Управление паролями) содержит следующие поля.

- **Password Minimum Length (8-64) (Минимальная длина пароля (8-64 символов)).** когда установлен этот флажок, указывает минимальную длину пароля. Например, администратор может определить, что минимальное количество символов для всех паролей канала - 10.
- **Consecutive Passwords Before Re-use (Последовательные пароли перед повторным использованием).** указывает количество изменений пароля перед тем, как использовать его повторно. Возможные значения этого поля: 1-10**.**
- **Enable Login Attempts (Включить контроль попыток ввода пароля).** включает блокировку входа пользователя устройства при использовании неверного пароля определенное количество раз. Например, если это поле отмечено, и определено, что число попыток ввода пароля равно пяти, когда пользователь неправильно введет пароль пять раз, при шестой попытке устройство заблокирует пользователя. Возможные значения этого поля: 1-5.

Определение параметров управления паролями

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

   Параметры управления паролями будут определены, а устройство обновлено.

Управление паролями с помощью команд консоли

В следующей таблице приведены эквивалентные команды интерфейса командной строки для настройки полей, отображаемых на странице **Password Management** (Управление паролями).

Команда консоли	**Описание**
минимальная длина *пароля*	Определение минимальной длины пароля.
история *пароля*	Определение количества изменений пароля перед тем, как его можно использовать повторно.
число попыток ввода *пароля*	Определение числа неправильных попыток ввода пароля до блокировки входа пользователя в систему.
отображение конфигурации пароля	Отображение информации об управлении паролями.

Далее приведен пример команд консоли.

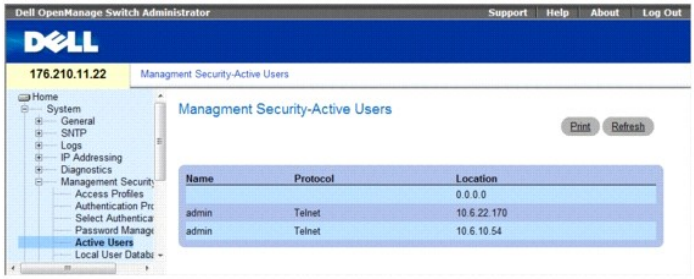
```
console # show passwords configuration

Minimal length: 0

History: Disabled

History hold time: no limit

Lockout control: disabled
```

Enable Passwords				
Level	Password Aging	Password Expiry date	Lockout	
-----	--------	----------	-------	
1	-	-	-	
15	-	-	-	
Line Passwords				
Line	Password Aging	Password Expiry date	Lockout	
-------	--------	----------	-------	
Telnet	-	-	-	
Страница SSH	-	-	-	
Console	-	-	-	
console # **show users accounts**				
Username	Privilege	Password Aging	Password Expiry Date	Lockout
--------	---------	--------	----------	-------
nim	15	39	18-Feb-2005	

Просмотр активных пользователей

Страница **Active Users** (Активные пользователи) содержит информацию о пользователях, находящихся в текущий момент в системе.

Рис. 6-58. Active Users (Активные пользователи)

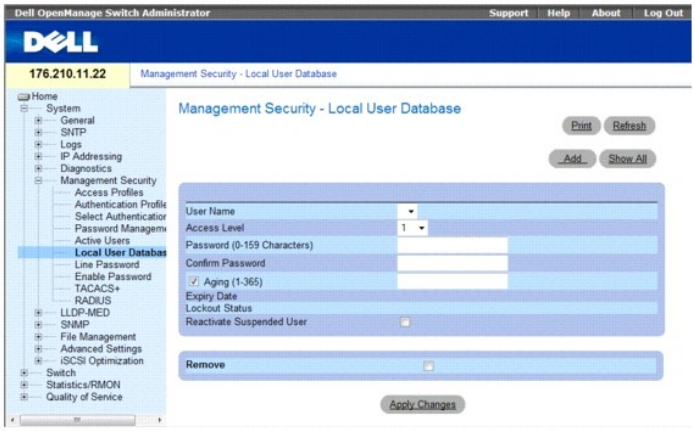


- **Name (Имя).** имя пользователя для входа в систему.
- **Protocol (Протокол).** протокол, используемый для доступа к устройству.
- **Location (Местоположение).** IP-адрес компьютера, используемого для доступа к устройству.

Определение локальных баз данных пользователей

Страница **Local User Database** (Локальная база данных пользователей) содержит поля, позволяющие определить пользователей, пароли и уровни доступа. Чтобы открыть страницу **Local User Database** (Локальная база данных пользователей), выберите **System** (Система)→ **Management Security** (Безопасность управления)→ **Local User Database** (Локальная база данных пользователей) на панели дерева.

Рис. 6-59. Local User Database (Локальная база данных пользователей)



Страница **Local User Database** (Локальная база данных пользователей) содержит следующие поля.

- **User Name (Имя пользователя).** список пользователей.
- **Access Level (Уровень доступа).** уровень доступа пользователя. Самый низкий уровень доступа пользователя - **1**, а самый высокий -**15**. Пользователи с уровнем доступа 15 являются привилегированными. Только эти пользователи имеют доступ к странице Dell OpenManage Switch Administrator.
- **Password (0-159 Characters) (Пароль (от 0 до 159 символов)).** задаваемый пользователем пароль.
- **Confirm Password (Подтверждение пароля).** подтверждение задаваемого пользователем пароля.
- **Aging (1-365) (Срок действия пароля (1-365)).** когда установлен этот флажок, указывает срок действия пароля в днях.
- **Expiry Date (Дата окончания действия).** указывает дату окончания действия определенного пользователем пароля.
- **Lockout Status (Состояние блокировки пароля).** Указывает, имеет ли пользователь в настоящее время доступ (статус *Usable (Доступ открыт)*), или пользователь лишен доступа вследствие большого числа неудачных попыток авторизации с момента последнего успешного входя в систему (статус *Locked (Доступ закрыт)*).
- **Reactivate Suspended User (Возобновление приостановленного пользователя).** если флажок установлен, восстанавливает права доступа конкретного пользователя. Права доступа могут быть приостановлены после неудачной попытки входа в систему.
- **Remove (Удалить).** когда установлен этот флажок, удаляется пользователь из списка **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).

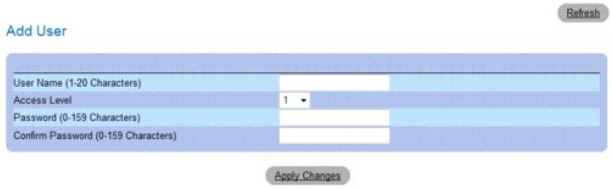
   Права доступа пользователя и пароли будут определены, а устройство обновлено.

Определение нового пользователя:

1. Откройте страницу **Local User Database** (Локальная база данных пользователей).
2. Нажмите кнопку **Add** (Добавить).

   Откроется страница **Add User** (Добавить пользователя).

Рис. 6-60. Добавление пользователя



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

   Новый пользователь будет определен, а устройство обновлено.

Отображение локальной пользовательской таблицы:

1. Откройте страницу **Local User Database** (Локальная база данных пользователей).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **Local User Table** (Таблица локальных пользователей).

Рис. 6-61. Local User Table (Таблица локальных пользователей)

Возобновление приостановленных прав пользователя:

1. Откройте страницу **Local User Database** (Локальная база данных пользователей).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **Local User Table** (Таблица локальных пользователей).
3. Выберите запись **User Name** (Имя пользователя).
4. Установите флажок **Reactivate Suspended User** (Возобновить приостановленные права пользователя).
5. Нажмите кнопку **Apply Changes** (Применить изменения).

   Права доступа пользователя будут восстановлены, а устройство обновлено.

Удаление пользователей:

1. Откройте страницу **Local User Database** (Локальная база данных пользователей).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **Local User Table** (Таблица локальных пользователей).
3. Выберите **User Name** (Имя пользователя).
4. Установите флажок **Remove** (Удалить).
5. Нажмите кнопку **Apply Changes** (Применить изменения).

   Выбранный пользователь будет удален, а устройство обновлено.

Назначение пользователей с помощью команд консоли

В следующей таблице приведены команды консоли для настройки полей, отображаемых на странице **Local User Database** (Локальная база данных пользователей).

Команда консоли	**Описание**
username *имя* [**password** *пароль*] [**level** *уровень*] [**encrypted**]	Устанавливает проверку подлинности по имени пользователя.
set username имя active	Восстановление прав доступа пользователя.

Далее приведен пример команд консоли.

```
console(config)# username bob password lee level 15

console# set username bob active
```

Defining Line Passwords

Страница **Line Password** (Пароль канала связи) содержит поля для определения паролей каналов для методов управления. Чтобы открыть страницу **Line Password** (Пароль канала), выберите **System** (Система)→ **Management Security** (Безопасность управления)→ **Line Passwords** (Пароли каналов) на панели дерева.

Рис. 6-62. 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 for Console / Telnet / Secure Telnet (Подтвердить пароль для консоли / Telnet / Secure Telnet).** подтверждает новый пароль канала. Пароль отображается в формате *****.
- **Line Aging (1-365) for Console / Telnet / Secure Telnet (Срок действия пароля канала (1-365) для консоли / Telnet / Secure Telnet).** когда установлен этот флажок, указывает срок действия пароля канала в днях.
- **Expiry Date for Console / Telnet / Secure Telnet (Дата окончания действия пароля для консоли / Telnet / Secure Telnet).** указывает дату окончания действия пароля канала.
- **Lockout Status for Console / Telnet / Secure Telnet (Состояние блокировки пароля для консоли / Telnet / Secure Telnet).** Указывает, имеет ли пользователь в настоящее время доступ (статус *Usable* (Доступ открыт)), или пользователь лишен доступа вследствие большого числа неудачных попыток авторизации с момента последнего успешного входя в систему (статус *Locked* (Доступ закрыт)).
- **Reactivate Locked Line for Console / Telnet / Secure Telnet (Восстановить пароль канала для консоли / Telnet / Secure Telnet).** когда флажок установлен, восстанавливает пароль канала для сеанса консоли/Telnet/Secure Telnet. Права доступа могут быть приостановлены после неудачной попытки входа в систему.

Определение паролей каналов связи для сеансов консоли

1. Откройте страницу **Line Password** (Пароль канала)
2. Введите значение в поле **Console Line Password** (Пароль канала для консоли).
3. Нажмите кнопку **Apply Changes** (Применить изменения).

   Пароль линии для сеансов консоли будет определен, а устройство обновлено.

Определение паролей каналов связи для сеансов Telnet

1. Откройте страницу **Line Password** (Пароль канала).
2. Введите значение в поле **Telnet Line Password** (Пароль канала для Telnet).
3. Нажмите кнопку **Apply Changes** (Применить изменения).

   Пароль линии для сеансов Telnet будет определен, а устройство обновлено.

Определение паролей каналов связи для сеансов безопасной связи Telnet

1. Откройте страницу **Line Password** (Пароль канала).
2. Введите значение в поле **Secure Telnet Line Password** (Пароль канала для Secure Telnet).
3. Нажмите кнопку **Apply Changes** (Применить изменения).

   Пароль канала для сеансов Secure Telnet будет определен, а устройство обновлено.

Назначение паролей каналов с помощью команд консоли

В следующей таблице приведены команды консоли для настройки полей, отображаемых на странице **Line Password** (Пароль канала).

Команда консоли	**Описание**
password *пароль* [**encrypted**]	Указывает пароль для канала.

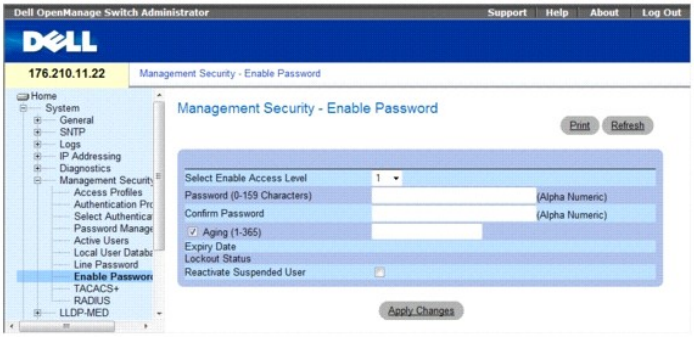
Далее приведен пример команд консоли.

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

Определение паролей включения

Страница **Enable Password** (Пароль включения) задает локальный пароль для управления доступом для конфигураций Normal (Обычная) и Privilege (С привилегиями). Чтобы открыть страницу **Enable Password** (Пароль включения), выберите **System** (Система)→ **Management Security** (Безопасность управления)→ **Enable Passwords** (Пароли включения) на панели дерева.

Рис. 6-63. Enable Password (Пароль включения)



Страница **Enable Password** (Пароль включения) содержит следующие поля.

- **Select Enable Access Level (Выбор уровня доступа для включения).** уровень доступа, связанный с паролем включения. Возможные значения этого поля: 1-15.
- **Password (0-159 characters) (Пароль (0-159 символов)).** текущий пароль включения.
- **Confirm Password (Подтвердить пароль).** подтверждение нового пароля включения. Пароль отображается в формате *****.
- **Aging (1-365) (Срок действия (1-365)).** когда этот флажок установлен, указывает срок действия пароля в днях.
- **Expiry Date (Дата окончания действия).** указывает дату окончания действия пароля включения.
- **Lockout Status (Состояние блокировки).** указывает число неправильных попыток ввода пароля с момента последнего успешного входа в систему, если установлен флажок Enable Login Attempts (Включить контроль попыток ввода пароля) на странице **Password Management** (Управление паролями). Если вход в систему для пользователя заблокирован, отображается состояние **LOCKOUT** (Блокировка).
- **Reactivate Suspended User (Возобновление приостановленного пользователя).** если флажок установлен, восстанавливает права доступа конкретного пользователя. Права доступа могут быть приостановлены после неудачной попытки входа в систему.

Определение нового пароля включения:

1. Откройте страницу **Enable Password** (Пароль включения).
2. Определите поля.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

   Новый пароль включения будет определен, а устройство обновлено.

Назначение паролей включения с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для настройки полей, отображаемых на странице **Enable Password** (Пароль включения).

Команда консоли	**Описание**
enable password [level *уровень*] *пароль* [**encrypted**]	Задает локальный пароль для управления доступом для уровней пользователей и привилегий.

Далее приведен пример команд консоли.

```
console(config)# enable password level 15 secret
```

Определение параметров TACACS+

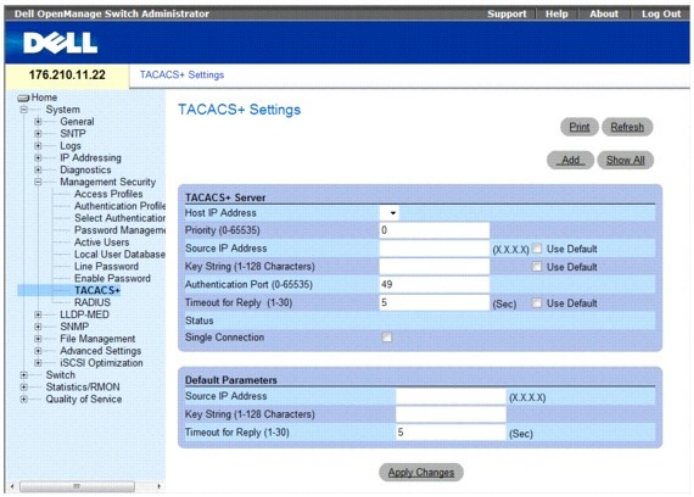
Устройство предоставляет поддержку для клиентов TACACS+ (Terminal Access Controller Access Control System). TACACS+ обеспечивает централизованную систему безопасности для проверки пользователей, получающих доступ к устройству.

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

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

Протокол TACACS+ обеспечивает целостность сети благодаря обмену шифрованными данными протокола между устройством и сервером TACACS+. Чтобы открыть страницу **TACACS+ Settings** (Параметры TACACS+), выберите **System** (Система)→ **Management Security** (Безопасность управления)→ **TACACS+** на панели дерева.

Рис. 6-64. TACACS+ Settings (Параметры TACACS+)



- **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) (Sec) (Время для ответа (1-30) сек).** время ожидания ответа при обмене данным между устройством и сервером TACACS+. Диапазон значений: 1-30 секунд.
- **Status (Состояние).** состояние соединения между устройством и сервером TACACS+. Возможные значения:
  - **Connected (Соединение установлено).** между устройством и сервером TACACS+ установлено соединение.
  - **Not Connected (Соединение не установлено).** отсутствует соединение между устройством и сервером TACACS+.
- **Single Connection (Одно соединение).** Если выбран этот параметр, поддерживается одно открытое соединение между устройством и сервером TACACS+.

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:

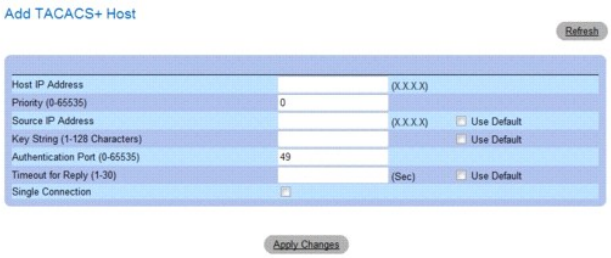
- **Source IP Address (IP-адрес источника).** IP-адрес устройства источника, используемый по умолчанию для сеанса TACACS+ между устройством и сервером TACACS+.
- **Key String (0-128 Characters) (Строка ключа (1-128 символов)).** используемые по умолчанию проверка подлинности и ключ шифрования обмена данными TACACS+ между устройством и сервером TACACS+.
- **Timeout for Reply (1-30) (Время для ответа (1-30)).** время ожидания ответа при обмене данным между устройством и сервером TACACS+.

Добавление сервера TACACS+

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

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

Рис. 6-65. Add TACACS+ Host (Добавление хоста TACACS+)



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

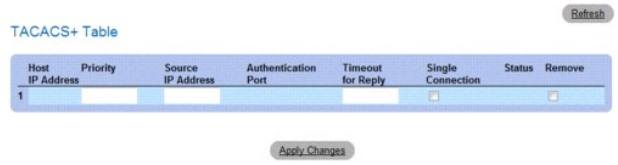
   Будет добавлен сервер TACACS+, а устройство будет обновлено.

Отображение таблицы TACACS+

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

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

Рис. 6-66. TACACS+ Table (Таблица TACACS+)



Удаление сервера TACACS+

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

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

   Будет удален сервер TACACS+, а устройство будет обновлено.

Определение параметров TACACS+ с помощью команд консоли

В следующей таблице приведены команды консоли для настройки полей, отображаемых на странице **TACACS+ Settings** (Параметры TACACS+).

Команда консоли	**Описание**
TACACS-server host (*ip-адрес* | *имя_хоста*) [**single-connection**] [**port** *номер_порта*] [**timeout** *тайм-аут*] [**key** *строка_ключа*] [**source** *источник*] [**priority** *приоритет*]	Определяет хост TACACS+.
no TACACS-server host (*ip-адрес* | *имя_хоста*)	Удаляет хост 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.)
tacacs-server timeout *время ожидания*	Указывает значение времени ожидания в секундах. (Диапазон: 1 - 30.)
tacacs-server source-ip *источник*	Определяет IP-адрес источника. (Диапазон: допустимый IP-адрес.)
show TACACS [*ip-адрес*]	Отображает настройку и статистику для сервера TACACS+.

Далее приведен пример команд консоли.

```
Console# show tacacs

Router Configuration

---------- --------- ---- ---------- --------- -------- --------
IP address Status    Port Single     TimeOut   Source   Priority
                          Connection           IP
---------- --------- ---- ---------- --------- -------- --------
12.1.1.2   Not       49   Yes        1         12.1.1.1 1
           Connected

Global values
-----------------
TimeOut : 5

Router Configuration
-----------------
Source IP : 0.0.0.0
console#
```

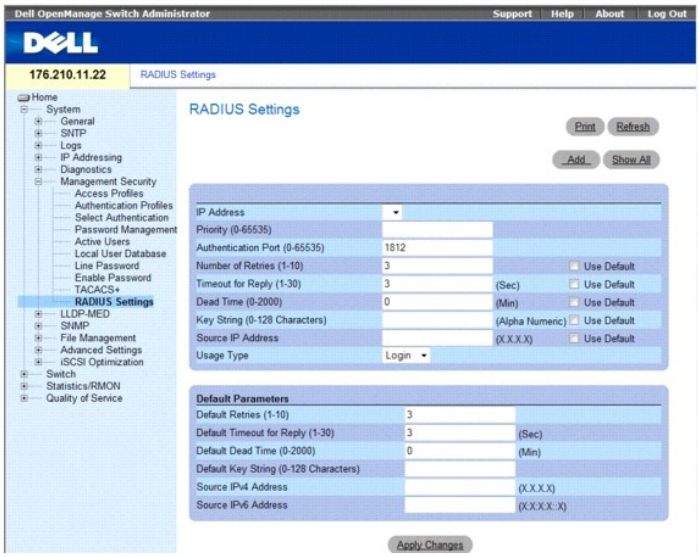
Настройка общих параметров RADIUS

Серверы RADIUS (RADIUS - Remote Authorization Dial-In User Service) обеспечивают дополнительную защиту сетей. Серверы RADIUS обеспечивают централизованный метод проверки подлинности:

- для доступа Telnet
- для доступа по Интернету
- для доступа к устройству с помощью консоли

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

Рис. 6-67. RADIUS Settings (Параметры RADIUS)



- **IP Address (IP-адрес).** список IP-адресов серверов для проверки подлинности.
- **Priority (1-65535) (Приоритет).** определяет приоритет сервера. Возможные значения: от 1 до 65535, где 1 - наибольшее значение. Используется для настройки порядка, в котором серверы выстраиваются в очередь.
- **Authentication Port (Порт проверки подлинности).** определяет порт проверки подлинности. Порт проверки подлинности используется для проверки подлинности сервера RADIUS.
- **Number of Retries (1-10) (Число повторных попыток).** число запросов, переданных серверу RADIUS, прежде чем произошла ошибка. Возможные значения: 1 - 10. Значение по умолчанию: 3.
- **Timeout for Reply (1-30) (Время для ответа).** определяет время в секундах, в течение которого устройство ожидает ответа от сервера RADIUS перед повторным запросом или переключением на следующий сервер. Возможные значения: 1 - 30. Значение по умолчанию: 3.
- **Dead Time (0-2000) (Время отключения).** время (в секундах), в течение которого сервер RADIUS не принимает запросы на обработку. Диапазон значений: 0-2000.
- **Key String (1-128 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 закодирован.
- **Source IP Address (IP-адрес источника).** определяет исходный IP-адрес, который используется для связи с серверами RADIUS.
- **Usage Type (Тип использования).** определяет тип использования сервера. Может быть задано одно из следующих значений: **login** (вход), **802.1x** или **all** (все). Если значение не указано, по умолчанию используется значение **all** (все).

Если не указаны значения времени ожидания, числа попыток или времени отключения для конкретного хоста, для каждого хоста используются общие значения (по умолчанию). Следующие поля задают значения по умолчанию для RADIUS:

- **Default Retries (1-10) (Число повторных попыток по умолчанию).** число запросов по умолчанию, передаваемых серверу RADIUS, прежде чем отображается ошибка.
- **Default Timeout for Reply (1-30) (Время для ответа по умолчанию).** время по умолчанию (в секундах), в течение которого устройство ожидает ответа от сервера RADIUS.
- **Default Dead time (0-2000) (Время отключения по умолчанию).** время по умолчанию (в секундах), в течение которого сервер RADIUS не принимает запросы на обработку. Диапазон значений: 0-2000.
- **Default Key String (1-128 Characters) (Строка ключа по умолчанию (1-128 символов)).** строка ключа по умолчанию, используемая для проверки подлинности и шифрования всех данных RADIUS, передаваемых между устройством и сервером RADIUS. Этот ключ закодирован.
- **Source IPv4 ddress (IPv4-адрес источника).** определяет исходный адрес IP версии 4, который используется для связи с серверами RADIUS.
- **Source IPv6 Address (IPv6-адрес источника).** определяет исходный адрес IP версии 6, который используется для связи с серверами RADIUS.

При определении нового сервера RADIUS server, будет доступен следующий дополнительный параметр:

- **Supported IP Format (Поддерживаемый формат IP-адресов).** Отображает формат IP-адресов, поддерживаемый сервером. Возможные значения:
  - **IPv6 Global (Глобальный адрес IPv6).** поддержка IP версии 6.
  - **IPv4.** поддержка IP версии 4.

Определение параметров RADIUS:

1. Откройте страницу **RADIUS Settings** (Параметры RADIUS).
2. Определите поля.

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

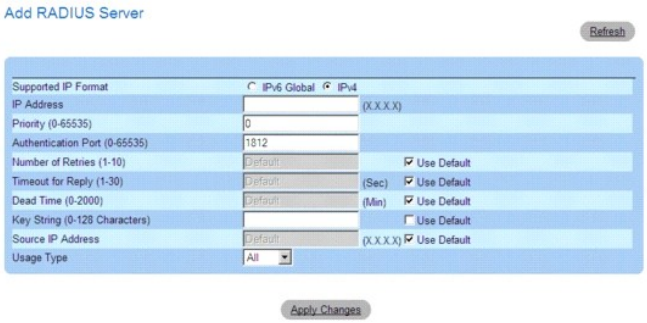
   Параметры RADIUS для данного устройства будут изменены.

Добавление сервера RADIUS:

1. Откройте страницу **RADIUS Settings** (Параметры RADIUS).
2. Нажмите кнопку **Add** (Добавить).

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

Рис. 6-68. Add RADIUS Server (Добавление сервера RADIUS)



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

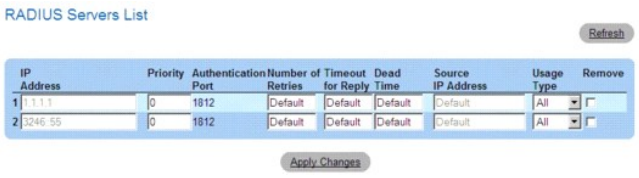
   Новый сервер RADIUS будет добавлен, а устройство обновлено.

Отображение списка серверов RADIUS:

1. Откройте страницу **RADIUS Settings** (Параметры RADIUS).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **Show all RADIUS Servers** (Показать все серверы RADIUS).

Рис. 6-69. Show all RADIUS Servers (Показать все серверы RADIUS)



Изменение параметров сервера RADIUS:

1. Откройте страницу **RADIUS Settings** (Параметры RADIUS).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **RADIUS Servers List** (Список серверов RADIUS).

3. Измените соответствующие поля.

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).

   Откроется страница **RADIUS Servers List** (Список серверов RADIUS).
3. Выберите сервер RADIUS в списке **RADIUS Servers List** (Список серверов RADIUS).
4. Установите флажок **Remove** (Удалить).
5. Нажмите кнопку **Apply Changes** (Применить изменения).

   Сервер RADIUS будет удален из **списка серверов RADIUS**.

Определение серверов RADIUS с помощью команд консоли

В следующей таблице приведены команды консоли для настройки полей, отображаемых на странице **RADIUS Settings** (Параметры RADIUS).

Команда консоли	**Описание**
radius-server timeout *тайм-аут*	Задает стандартный интервал для каждого устройства, ожидающего ответа сервера.
radius-server source-ip *источник*	Определяет IPv4-адрес источника, который будет использоваться для связи с сервером RADIUS по протоколу IPv4.
radius-server source-ipv6 *источник*	Определяет IPv6-адрес источника, который будет использоваться для связи с сервером RADIUS по протоколу IPv6.
radius-server retransmit *количество_попыток*	Определяет, сколько раз (по умолчанию) программа обращается к списку хостов сервера RADIUS.
radius-server deadtime *количество_секунд*	Настраивает пропуск недоступных серверов по умолчанию.
radius-server key [*строка_ключа*]	Задает стандартную проверку подлинности и ключ кодирования для всего обмена данными RADIUS между устройством и окружением RADIUS.
radius-server host {*ip-адрес* | *имя_хоста*} [**auth-port** *номер_порта_проверки_подлинности*] [**timeout** *количество_секунд*] [**retransmit** *количество_попыток*] [**deadtime** *количество_секунд*] [**key** *строка_ключа*] [**source** *источник*] [**priority** *приоритет*] [**usage** *тип*]	Указывает хост сервера RADIUS и параметры, не заданные по умолчанию.
show radius-servers	Отображает параметры сервера RADIUS.

Далее приведен пример команд консоли.

```
Console (config)# задержка сервера RADIUS 5

Console (config)# повторная передача сервера RADIUS 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 1645 timeout 20
```

```
Console# show radius-servers

                Port
IP address      Auth  Acct  TimeOut  Retransmit  Deadtime  Source IP  Priority  Usage
---------       ----  ----  -------  ----------  --------  ---------  --------  -----

33.1.1.1        1812  1813  6        4           10        0.0.0.0    0         All
```

172.16.1.2	1645	1646	11	8	Global	Global	2	All

```
Global values

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

TimeOut: 5

Retransmit: 5

Deadtime: 10

Source IP: 0.0.0.0
```

Настройка LLDP и LLDP-MED

Протокол LLDP позволяет сетевым администраторам выполнять поиск и устранение неисправностей и совершенствовать управление сетью путем выявления и сохранения топологии сети в средах, включающих оборудование самых разных поставщиков. С помощью протокола LLDP, используя стандартные методы, можно обнаружить сетевое окружение сетевых устройств, чтобы сообщить о них другим системам и сохранить обнаруженную информацию. Информация об устройствах включает следующее.

- Device Identification (Идентификатор устройства)
- Device Capabilities (Возможности устройства)
- Device Configuration (Конфигурация устройства)

Устройство рассылки запросов передает несколько наборов сообщений в одном пакете ЛВС. Для отправки нескольких наборов сообщений используется поле пакета Type Length Value (TLV) (Ввод значения длины). Устройства LLDP должны поддерживать сообщения о корпусе и идентификаторе порта, а также имя системы, идентификатор системы, описание системы и сообщения о возможностях системы.

В этом разделе рассмотрены следующие темы:

- Определение общих свойств LLDP
- Определение параметров порта для передачи пакетов LLDP
- Определение сетевой политики выявления конечной медиа-точки
- Определение параметров LLDP MED для порта
- Просмотр информации об окружении LLDP

Протокол LLDP Media Endpoint Discovery (LLDP-MED) повышает гибкость сети, обеспечивая различным системам IP возможность использовать один протокол LLDP.

Обеспечивает детальную информацию о топологии сети, включая сведения об устройствах сети и их местоположении.какой IP-телефон к какому порту подключен, какая программа работает на каком коммутаторе и какой порт к какому компьютеру подключен. Автоматически развертывает политики для сети для

- политик QoS;
- голосовых сетей VLAN

Обеспечивает службу экстренных вызовов (E-911), для которой используется информация о расположении IP-телефонов.

Предоставляет уведомления администраторам сети с информацией о поиске и устранении неисправностей при отправке данных по протоколу LLDP MED:

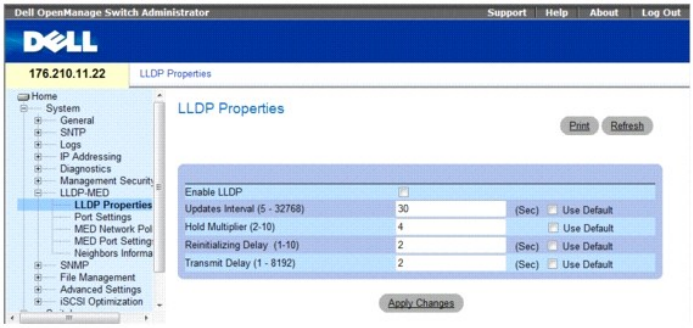
- Конфликты скорости порта и дуплексного режима
- Неправильная конфигурация политики QoS

Определение свойств LLDP

Страница **LLDP Properties** (Свойства LLDP) содержит поля для конфигурации LLDP.

Чтобы открыть страницу **LLDP Properties** (Свойства LLDP), выберите **System** (Система)→ **LLDP-MED**→ **LLDP Properties** (Свойства LLDP) на панели дерева**.**

Рис. 6-70. LLDP Properties (Свойства LLDP)



- **Enable LLDP (Включить LLDP).** указывает, включен ли LLDP на устройстве. Возможные значения:
  - **Отмечен**. LLDP включен на устройстве.
  - **Не отмечен**. LLDP отключен на устройстве. Это значение по умолчанию.
- **Updates Interval (5-32768) (Обновление интервала (5-32768)).** указывает частоту отправки обновлении объявлений через протокол LLDP. Возможные значения поля: 5 - 32768 секунд. Значение по умолчанию: 30 секунд.
- **Hold Multiplier (2-10) (Коэффициент хранения (2-10)).** Указывает кратность времени хранения пакетов LLDP до их удаления. Возможные значения поля: 2 - 10 раз. Значение по умолчанию: 4 кратное время.
- **Reinitializing Delay (1-10) (Задержка повторной инициализации (1-10)).** указывает период времени между отключением LLDP и началом повторной инициализации. Возможные значения поля: 1 - 10 секунд. Значение по умолчанию: 2 секунды.
- **Transmit Delay (1-8192) (Задержка передачи).** указывает период времени между последовательными передачами кадров LLDP в соответствии с изменениями в базе локальных систем LLDP MIB. Возможные значения поля: 1 - 8192 секунд. Значение по умолчанию: 2 секунды.

Конфигурация LLDP с помощью команд консоли

Таблица 6-39. Команды консоли для свойств LLDP

Команда консоли	Описание
lldp enable (global)	Включает протокол обнаружения каналов передачи данных.
lldp hold-multiplier число	Указывает время, в течение которого получающее устройство должно хранить пакет протокола обнаружения каналов передачи данных (LLDP) до его удаления.
lldp reinit-delay Секунды	Указывает минимальный период времени ожидания повторной инициализации для порта LLDP.
lldp tx-delay Секунды	Указывает время между последовательными передачами кадров LLDP.

Далее приведен пример команд консоли.

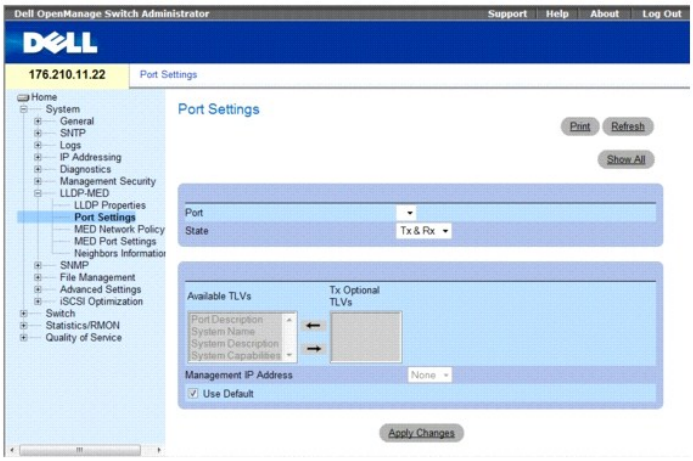
```
Console (config)# interface ethernet g5

Console(config-if)# lldp enable
```

Определение параметров порта для передачи пакетов LLDP

Страница LLDP **Port Settings** (Параметры порта для передачи пакетов LLDP) позволяет сетевым администраторам определять параметры порта для передачи пакетов LLDP, включая номер порта, номер порта для передачи пакетов LLDP и тип передаваемой через порт информации.

Страница **Port Settings** (Параметры порта) содержит поля для конфигурации LLDP. Чтобы открыть страницу **Port Settings** (Параметры порта), выберите **System** (Система)→ **LLDP-MED**→ **Port Settings** (Параметры порта) на панели дерева**.**

Рис. 6-71. Параметры порта



- **Port (Порт).** список портов, для которых включен протокол LLDP.
  - **State (Состояние).** тип порта, для которого включен протокол LLDP. Возможные значения:
  - **Tx Only (Только передача).** возможна только передача пакетов LLDP.
  - **Rx Only (Только прием).** возможен только прием пакетов LLDP.
  - **Tx & Rx (Передача и прием).** возможны передача и прием пакетов LLDP packets. Это значение по умолчанию.
  - **Disable (Отключить).** протокол LLDP отключен для порта.
- **Available TLVs (Доступные поля TLV).** список доступных полей TLV, которые могут использоваться портом для объявлений. Возможные значения:
  - **Port Description (Описание порта).** объявляет описание порта.
  - **System Name (Имя системы).** объявляет имя системы.
  - **System Description (Описание системы).** объявляет описание системы.
  - **System Capabilities (Возможности системы).** объявляет возможности системы.
- **Tx Optional TLVs (Дополнительные TLV для передачи).** список дополнительных TLV, объявленых портом. Полный список см. в поле **Available TLVs (Доступные TLV)**.
- **Management IP Address (IP-адрес управления).** указывает IP-адрес управления, объявленный с интерфейса.
- **Use Default (Использовать информацию по умолчанию).** указывает, что информация, включенная в TLV, является информацией по умолчанию для каждого устройства. Возможные значения:
  - **Checked (Отмечен).** включает отправку объявлений LLDP по умолчанию для устройства.
  - **Unchecked (Не отмечен).** указывает, что для устройства отключены параметры объявлений через протокол LLDP, они определяются пользователем. Это значение по умолчанию.

На странице **LLDP Port Table** (Таблица портов LLDP) отображается конфигурация порта для передачи пакетов LLDP. Чтобы открыть страницу **LLDP Port Table** (Таблица портов LLDP), выберите **Security→ LLDP→ Port Settings** (Параметры порта)→ S**how All** (Показать все) на панели дерева.

Рис. 6-72. Таблица портов LLDP

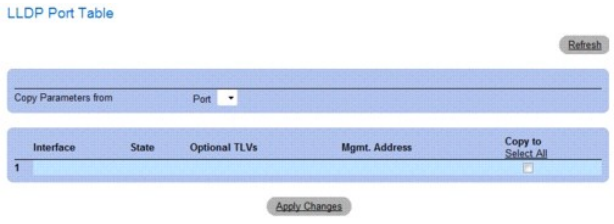


Таблица 6-40. Команды консоли для параметров портов LLDP

Команда консоли	**Описание**
`clear lldp rx` *interface*	Перезапускает устройство получения пакетов LLDP и выполняет очистку таблицы окружения
`lldp optional-tlv` *tlv1 [tlv2 ... tlv5]*	Указывает, передачу каких дополнительных TLV из базового набора необходимо выполнить.

`lldp enable [rx | tx | оба варианта]`	Включает протокол обнаружения каналов передачи данных (LLDP) для интерфейса.

Далее приведен пример команд консоли.

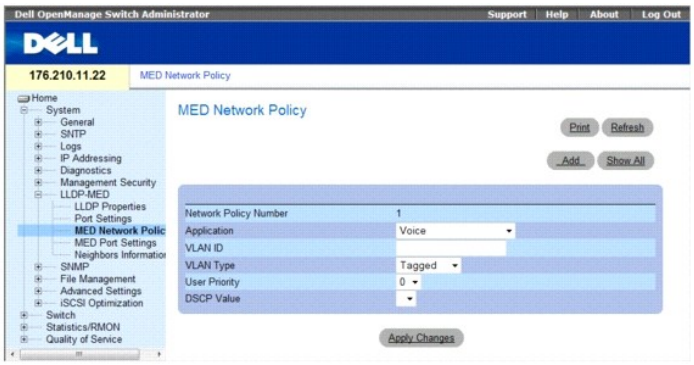
```
Console (config)# interface ethernet g5

Console(config-if)# lldp enable
```

Определение сетевой политики для протокола LLDP MED

Страница **MED Network Policy** (Сетевая политика MED) содержит поля для конфигурации LLDP.

Чтобы открыть страницу **MED Network Policy** (Сетевая политика MED), выберите**System** (Система)→ **LLDP-MED**→ **MED Network Policy** (Сетевая политика MED) на панели дерева**.**

Рис. 6-73. Сетевая политика MED



Страница ***MED Network Policy*** (Сетевая политика MED) **содержит следующие поля:**

- **Network Policy Number (Номер сетевой политики).** отображается номер сетевой политики.
- **Application (Приложение).** отображается приложение, для которого определяется сетевая политика. Возможные значения:
  - **Voice (Голос).** указывает, что сетевая политика определяется для голосового приложения.
  - **Voice Signaling (Голосовые сигналы).** указывает, что сетевая политика определяется для приложения голосовых сигналов.
  - **Guest Voice (Голос с подключенного устройства).** указывает, что сетевая политика определяется для приложения приема голоса с подключенного устройства.
  - **Guest Voice Signaling (Голосовые сигналы с подключенного устройства).** указывает, что сетевая политика определяется для приложения приема голосовых сигналов с подключенного устройства.
  - **Softphone Voice (Голос с программного телефона).** указывает, что сетевая политика определяется для приложения приема голоса с программного телефона.
  - **Video Conferencing (Видео конференции).** Указывает, что сетевая политика определяется для приложения видео конференций.
  - **Streaming Video (Потоковое видео).** указывает, что сетевая политика определяется для приложения потокового видео.
- **Video Signaling (Видеосигналы).** указывает, что сетевая политика определяется для приложения приема видеосигналов.
- **VLAN ID (ID VLAN).** отображает ID VLAN, для которой определяется сетевая политика.
- **VLAN Type (Тип VLAN).** отображает тип VLAN, для которой определяется сетевая политика. Возможные значения:
  - **Tagged (Отмечен).** указывает, что сетевая политика определена для отмеченных VLAN.
  - **Untagged (Не отмечен).** указывает, что сетевая политика определена для неотмеченных VLAN.
- **User Priority (Приоритет пользователя).** определяет приоритет, назначенный для сетевого приложения.
- **DSCP Value (Значение DSCP).** определяет значение DSCP, назначенное для сетевой политики. Возможные значения поля: 1-64.

Добавление сетевой политики MED:

1. Откройте страницу **MED Network Policy** (Сетевая политика MED).
2. Нажмите кнопку **Add** (Добавить).

   Отобразится страница **Add Network Policy** (Добавление сетевой политики).

Рис. 6-74. Добавление сетевой политики

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

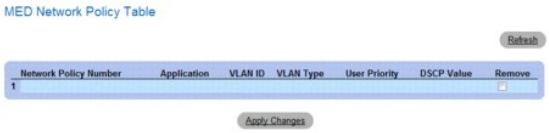
   Новая сетевая политика будет добавлена, а устройство обновлено.

Отображение таблицы сетевой политики MED:

1. Откройте страницу **MED Network Policy** (Сетевая политика MED).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **MED Network Policy Table** (Таблица сетевой политики MED) .

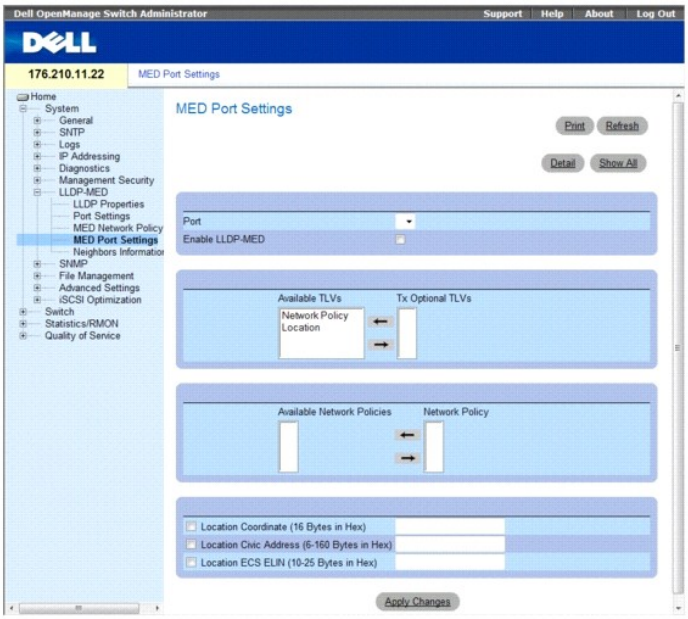
Рис. 6-75. MED Network Policy Table (Таблица сетевой политики MED)



Определение параметров LLDP MED для порта

Страница **MED Port Settings** (Параметры порта MED) содержит параметры для назначения сетевых политик LLDP определенным портам. Чтобы открыть страницу **MED Port Settings** (Параметры MED для порта), выберите **System** (Система)→ **LLDP-MED**→ **Port Settings** (Параметры MED для порта) на панели дерева.

Рис. 6-76. MED Port Settings (Параметры MED для порта)



На странице **MED Port Settings** (Параметры MED для порта) содержатся следующие поля:

- **Port (Порт).** отображает порт, для которого включен или выключен протокол LLDP-MED.
- **Enable LLDP-MED (Включить LLDP-MED).** обозначает, включен ли протокол LLDP-MED для выбранного порта. Возможные значения:

  Checked (Выбран). включает протокол LLDP-MED для порта.

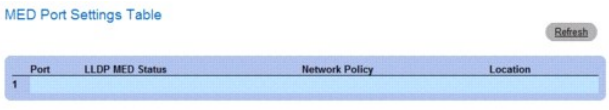
  Unchecked (Не выбран). выключает протокол LLDP-MED для порта. Это значение по умолчанию.
- **Tx Optional TLVs/Available TLVs (Дополнительные TLV для передачи/доступные поля TLV).** список доступных полей TLV, которые могут использоваться портом для объявлений. Возможные значения:
  - **Network Policy (Сетевая политика).** сетевая политика, связанная с портом.
  - **Location (Местоположение).** местоположение порта.
- **Network Policy/Available Network Policy (Сетевая политика/доступная сетевая политика).** содержит список сетевых политик, который можно назначить для порта.
- **Location Coordinate (Координата местоположения).** отображает координаты местоположения устройства.
- **Location Civic Address (6-160) (Адрес местоположения).** отображает город или название улицы для устройства, например 414 23rd Ave E. Возможное значение поля: 6 - 160 символов.
- **Location (10-25) (Местоположение ECS ELIN).** отображает местоположение ECS ELIN устройства. Диапазон значений поля: 10-25.

Отображение таблицы параметров MED для порта:

1. Откройте страницу **MED Port Settings** (Параметры MED для порта).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **MED Port Settings Table** (Таблица параметров MED для порта).

Рис. 6-77. MED Port Settings Table (Таблица параметров MED для порта)

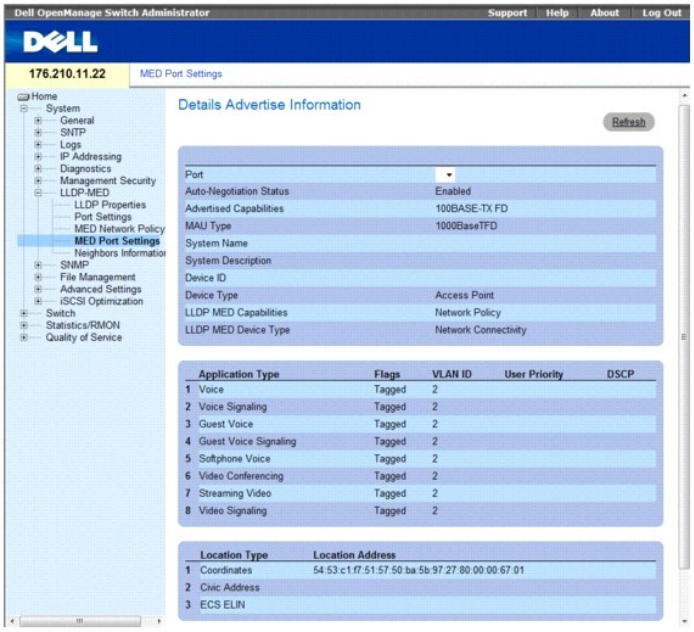


Отображение объявляемой информации:

1. Откройте страницу **MED Port Settings** (Параметры MED для порта).
2. Нажмите **Details** (Подробные сведения).

   Откроется страница **Details Advertise Information** (Объявляемая информация):

Рис. 6-78. Details Advertise Information Page (Объявляемая информация)



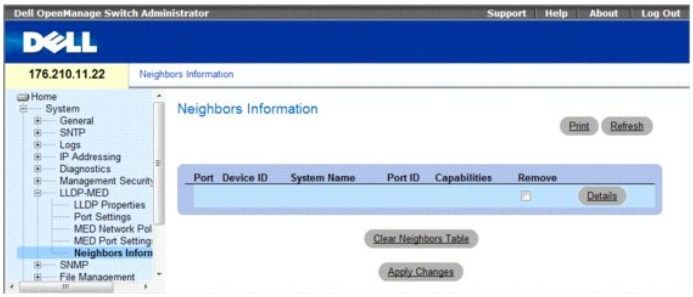
Страница **Details Advertise Information** (Объявляемая информация) содержит следующие поля:

- **Port (Порт).** порт, для которого отображается подробная информация.
- **Auto-Negotiation Status (Состояние автоматического согласования).** состояние автоматического согласования для порта. Возможные значения:
  - **Enabled (Включено).** автоматическое согласование включено для порта.
  - **Disabled (Выключено).** автоматическое согласование выключено для порта.
- **Advertised Capabilities (Характеристики объявления).** характеристики, объявляемые для порта.
- **MAU Type (Тип MAU).** обозначает тип устройства для подключения к линии связи. MAU выполняет функции на физическом уровне, включая преобразование цифровых данных при обнаружении коллизий интерфейсов Ethernet и подачу сигнала в битах в сеть.
- **System Name (Имя системы).** имя системы для порта.
- **System Description (Описание системы).** описание системы для порта.
- **Device ID (Код устройства).** код устройства порта.
- **Device Type (Тип устройства).** тип устройства.
- **LLDP MED Capabilities (Характеристики LLDP MED).** TLV, объявляемый портом.
- **LLDP MED Device Type (Тип устройства LLDP MED).** обозначает, является ли отправитель устройством с сетевым подключением или устройством, подключенным к конечной точке.
- **LLDP MED Network Policy (Сетевая политика LLDP MED).** сетевая политика LLDP порта для каждого из следующих типов применения:
  - Голос
  - Голосовые сигналы
  - Голос с подключенного устройства
  - Голосовые сигналы с подключенного устройства
  - Голос с программного телефона
  - Видео конференции
  - Потоковое видео
  - Видеосигналы
- **LLDP MED Location (Местоположение LLDP MED).** объявленное местоположение LLDP порта.
  - **Coordinates (Координаты).** отображает координаты местоположения устройства.
  - **Civic Address (Городской адрес).** отображает город или название улицы для устройства, например 414 23rd Ave E. Возможное значение поля: 6 - 160 символов.
  - **ECS ELIN.** отображает местоположение ECS ELIN устройства. Диапазон значений поля: 10 - 25.

Просмотр информации об окружении LLDP

Страница **Neighbors Information** (Информация об окружении) содержит сведения, полученные от близлежащих объявлений LLDP для устройства. Чтобы открыть страницу **Neighbor Information** (Информация об окружении), выберите **System** (Система)→ **LLDP-MED**→ **Neighbors Information** (Информация об окружении) на панели дерева**.**

Рис. 6-79. Neighbors Information (Информация об окружении)



- **Port (Порт).** отображает номер соседнего порта.
- **Device ID (Идентификатор устройства).** отображает идентификатор соседнего устройства.
- **System Name (Имя системы).** отображает время соседней системы.
- **Port ID (Идентификатор порта).** отображает идентификатор соседнего порта
- **Capabilities (Возможности).** отображает возможности соседнего устройства.
- Удаление порта в таблице.

1. Откройте страницу **Neighbors Information** (Информация об окружении).
2. Установите флажок **Remove** (Удалить) рядом с каждым портом, который требуется удалить.
3. Нажмите кнопку **Apply Changes** (Применить изменения). Порты будут удалены.

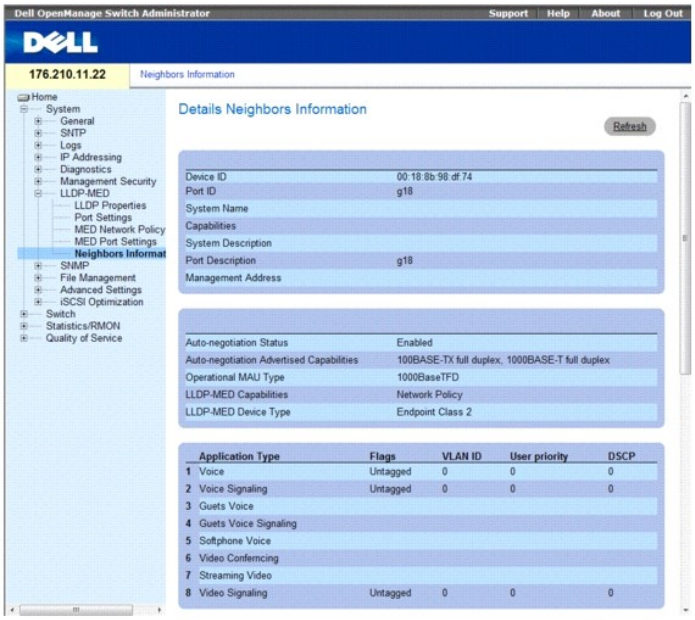
Очистка таблицы.

1. Откройте страницу **Neighbors Information** (Информация об окружении).
2. Выберите **Clear Neighbors Table** (Очистить таблицу соседей). Таблица будет очищена.

Просмотрите подробную информацию о LLDP MED, объявленную соседним устройством.

1. Откройте страницу **Neighbors Information** (Информация об окружении).
2. Нажмите кнопку **Details** (Подробности) рядом с нужной записью. Откроется страница Details Neighbor Information (Подробная информация об окружении).

Рис. 6-80. Details Neighbors Information (Подробная информация об окружении)



Для получения информации о полях см. страницу Details Advertise Information (Объявляемая информация) выше.

Таблица 6-41. Команды консоли для информации об окружении LLDP

Команда консоли	**Описание**
show lldp neighbors *interface*	Отображает информацию о соседних устройствах, обнаруженных с помощью протокола LLDP (Link Layer Discovery Protocol)

Далее приведен пример команд консоли.

Port	Идентификатор устройства	Идентификатор порта	Время задержки	Возможности	Имя системы
1	0060.704C.73FE	1	117	B	ts-7800-2
1	0060.704C.73FD	1	93	B	ts-7800-2
2	0060.704C.73FC	9	1	B, R	ts-7900-1
3	0060.704C.73FB	1	92	W	ts-7900-2

Switch# **show lldp neighbors**

Определение параметров SNMP

Протокол SNMP (Simple Network Management Protocol) обеспечивает способ управления устройствами в сети. На устройствах, поддерживающих SNMP, работает локальная программа (агент).

Агенты SNMP хранят список переменных, которые используются для управления устройством. Эти переменные задаются в базе данных Management Information Base (MIB). База данных MIB содержит переменные, которые контролируются агентом. Протокол SNMP задает формат спецификации MIB и формат для доступа к информации по сети.

Управление правами доступа к агенту SNMP осуществляется с помощью строк доступа. Для установки связи с коммутатором встроенный веб-сервер предлагает правильную строку сообщества для идентификации. Чтобы открыть страницу SNMP, выберите **System** (Система)→ **SNMP** на панели дерева.

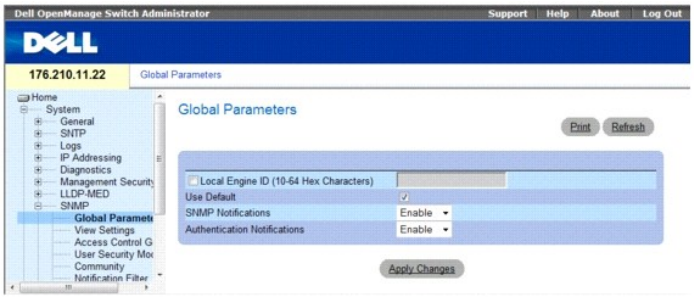
В этом разделе содержится информация по управлению настройкой SNMP.

Определение общих параметров SNMP

На странице **SNMP Global Parameters** (Общие параметры SNMP) можно включить уведомления о SNMP и о проверке подлинности. Чтобы открыть страницу **SNMP Global Parameters** (Общие параметры SNMP), выберите **System** (Система)→ **SNMP**→ **Global Parameters** (Общие параметры) на панели

дерева.

Рис. 6-81. Global Parameters (Общие параметры)



- **Local Engine ID (10 - 64 Hex Characters) (Идентификатор механизма на локальном устройстве (10 - 64 шестнадцатеричных символов)).** указывает идентификатор механизма на локальном устройстве. Значение этого поля является шестнадцатеричным. Каждый байт в строке шестнадцатеричного символа - это две шестнадцатеричных цифры. Каждый байт должен быть разделен точкой или двоеточием. Идентификатор механизма должен быть определен перед включением протокола SNMP версии 3. Для автономных устройств выберите идентификатор механизма по умолчанию, который состоит из номера предприятия и MAC-адреса по умолчанию.
- **Use Default (Использовать значения по умолчанию).** использует идентификатор механизма, созданный устройством. Идентификатор механизма по умолчанию состоит из MAC-адреса устройства и определяется стандартом:
  - **Первые 4 октета.** первый бит = 1, остальные - номер предприятия IANA = 674.
  - **Пятый октет.** задайте значение 3, чтобы указать последующий MAC-адрес.
  - **Последние 6 октетов.** MAC-адрес устройства.
- **SNMP Notifications (Уведомления SNMP).** включает или отключает отправку маршрутизатором уведомлений SNMP.
- **Authentication Notifications (Уведомления о проверке подлинности).** включает или отключает отправку маршрутизатором системных прерываний SNMP при ошибке проверки подлинности.

Включение уведомлений SNMP

1. Откройте страницу **SNMP Global Parameters** (Общие параметры SNMP).
2. Выберите Enable (Включить) в поле SNMP Notifications (Уведомления SNMP).
3. Нажмите кнопку **Apply Changes** (Применить изменения).

   Уведомления SNMP будут включены, а устройство обновлено.

Включение уведомлений о проверке подлинности

1. Откройте страницу **SNMP Global Parameters** (Общие параметры SNMP).
2. Выберите Enable (Включить) в поле SNMP Notifications (Уведомления SNMP).
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Включение уведомлений SNMP с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для просмотра полей на странице **SNMP Global Parameters** (Общие параметры SNMP).

Команда консоли	Описание
snmp-server enable traps	Разрешает маршрутизатору отправлять системные прерывания SNMP (Simple Network Management Protocol).
snmp-server trap authentication	Разрешает маршрутизатору отправлять системные прерывания SNMP (Simple Network Management Protocol) при ошибке проверки подлинности.
show snmp	Выполняет проверку состояния соединений по протоколу SNMP.

snmp-server engine ID local {*строка-идентификатора-механизма* | **default**}	Указывает идентификатор механизма на локальном устройстве. Значение этого поля является шестнадцатеричным. Каждый байт в строке шестнадцатеричного символа - это две шестнадцатеричных цифры. Каждый байт должен быть разделен точкой или двоеточием. Идентификатор механизма должен быть определен перед включением протокола SNMP версии 3.

Далее приведен пример команд консоли.

```
Console (config)# snmp-server enable traps

Console (config)# snmp-server trap authentication

Console# show snmp

Community-String        Community-Access        View name       IP address
----------------        ----------------        ---------       ----------
public                  read only               view-1          All

Community-String        Group name              IP address      Type
----------------        ----------              ----------      ----

Traps are enabled.
Authentication-failure trap is enabled.

Version 1,2 notifications
Target Address  Type  Community  Version  Udp Port  Filter name  To Sec  Retries
-------         ----  ---------  -------  ----      ------       ---     -------

Version 3 notifications
Target Address  Type  Username   Security Level  Udp Port  Filter name  To Sec  Retries
--------        ----  ---------  --------        ----      ------       ---     -------

System Contact: Robert
System Location: Marketing
```

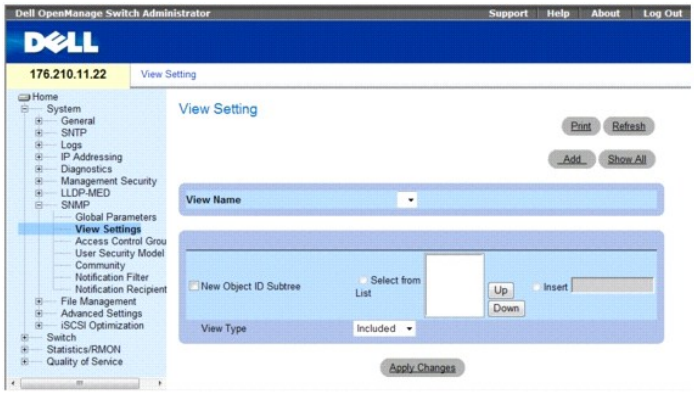
Определение параметров представления SNMP

Представления SNMP обеспечивают или блокируют доступ к функциям устройства или аспектам функций. Например, можно определить представление, которое устанавливает, что SNMP-группа A имеет доступ к группам многоадресной передачи только для чтения, тогда как SNMP-группа B имеет доступ к группам многоадресной передачи с возможностью чтения и записи. Доступ к функциям предоставляется с помощью имени MIB или идентификатора объекта MIB.

С помощью стрелок вверх и вниз можно выполнять навигацию в MIB-дереве и переходить между ветвями MIB-дерева.

Чтобы открыть страницу **SNMPv3 View Settings** (Параметры представления SNMP версии 3), выберите **System** (Система)→ **SNMP**→ **View Settings** (Параметры представлений SNMP) на панели дерева.

Рис. 6-82. Параметры представления SNMP версии 3



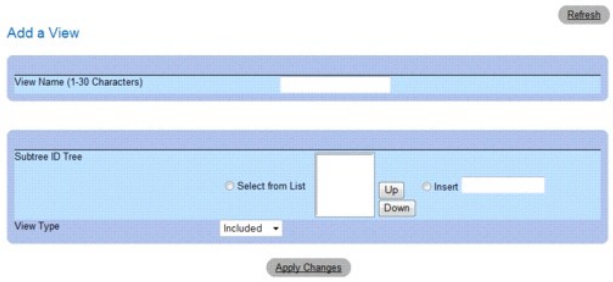
- **View Name (Имя представления).** содержит список видов, определенных пользователем. Имя представления может содержать не более 30 буквенно-цифровых символов. Возможные значения:
  - **Default (По умолчанию).** отображает представление по умолчанию, определенное пользователем.
  - **DefaultSuper (Супер по умолчанию).** отображает суперпредставление по умолчанию, определенное пользователем.
- **New Object ID Subtree (Новая ветвь идентификатора объекта).** указывает наличие или отсутствие идентификатора объекта функции устройства в представлении SNMP.
- **Selected from List (Выбранный в списке).** с помощью кнопок со стрелками вверх и вниз выберите идентификатор объекта устройства, прокрутив список всех идентификаторов объекта устройства (OID).
- **Вставить.** укажите идентификатор объекта устройства.
- **View Type (Тип представления).** указывает, будет ли включен идентификатор ветви объекта в выбранное представление **SNMP**.

Добавление представления

1. Откройте страницу **SNMPv3 View Settings** (Параметры представления SNMP версии 3).
2. Нажмите кнопку **Add** (Добавить).

Откроется страница **Add a View** (Добавление представление).

Рис. 6-83. Add A View (Добавление представления)



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

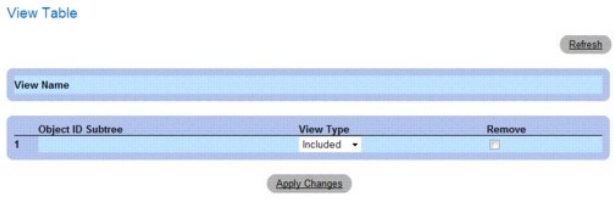
   Будет добавлено представление **SNMP**, а устройство обновлено.

Отображение таблицы представлений

1. Откройте страницу **SNMPv3 View Settings** (Параметры представления SNMP версии 3).
2. Нажмите кнопку **Show All** (Показать все).

Откроется страница **View Table** (Таблица представлений).

Рис. 6-84. Таблица представлений



Определение представлений SNMP с помощью команд консоли

В следующей таблице приведены команды консоли для определения полей, отображаемых на странице **SNMPv3 View Settings** (Параметры представления SNMP версии 3).

Команда консоли	Описание
snmp-server view *имя-представления дерево-идентификаторов-объектов* {**included** | **excluded**}	Создает иди обновляет запись представления.
show snmp views [*имя_представления*]	Отображает конфигурацию представлений.

Далее приведен пример команд консоли:

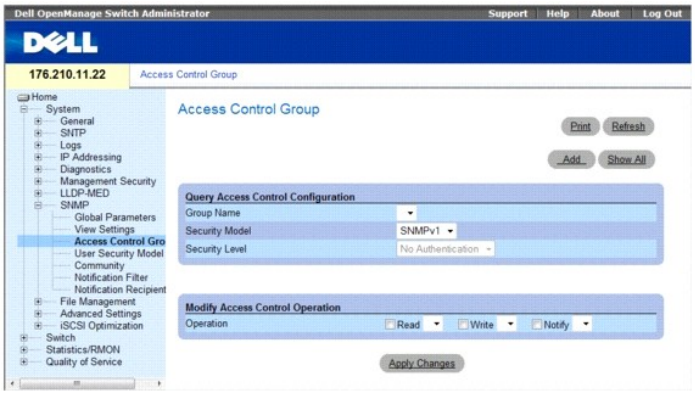
```
Console (config)# snmp-server view user1 1 included

Console (config)# end

Console # show snmp views
```

Name	OID Tree	Type
----------	----------	----------
user1	iso	included
Значение по умолчанию	iso	included
Значение по умолчанию	snmpVacmMIB	excluded
Значение по умолчанию	usmUser	excluded
Значение по умолчанию	rndCommunityTable	excluded
DefaultSuper	iso	included

Определение контроля доступа по протоколу SNMP

На странице **Access Control Add Group** (Группа добавления контроля доступа) представлена информация для создания групп SNMP и назначения привилегий доступа к группам SNMP. Выделив группы, администраторы сети могут назначать права доступа к отдельным функциям устройства или аспектам функций. Чтобы открыть страницу **Access Control Group** (Группа контроля доступа), выберите **System** (Система)→ **SNMP**→ **Access Control** (Контроль доступа) на панели дерева.

Рис. 6-86. Access Control Group (Группа контроля доступа)



- **Group Name (Имя группы).** группа, определенная пользователем, к которой применяются правила контроля доступа. Диапазон значений поля: до 30 символов.
- **Security Model (Модель безопасности).** определяет версию SNMP, используемую для группы. Возможные значения:
  - **SNMPv1 (SNMP версии 1).** для группы определен протокол SNMP версии 1.
  - **SNMPv2 (SNMP версия 2).** для группы определен протокол SNMP версии 2.
  - **SNMPv3 (SNMP версии 3).** для группы определен протокол SNMP версии 3.
  - **Security Level (Уровень безопасности).** уровень безопасности, применяемый к группе. Уровни безопасности применяются только для SNMP версии 3. Возможные значения:
  - **No Authentication (Нет проверки подлинности).** для группы не назначаются ни проверка подлинности, ни уровни безопасности для обеспечения конфиденциальности данных.
  - **Authentication (Проверка подлинности).** выполняет проверку подлинности сообщений SNMP и обеспечивает проверку подлинности источника сообщений SNMP.
  - **Privacy (Конфиденциальность).** выполняет шифрование сообщений SNMP.
- **Operation (Работа).** определяет права доступа группы. Возможные значения:

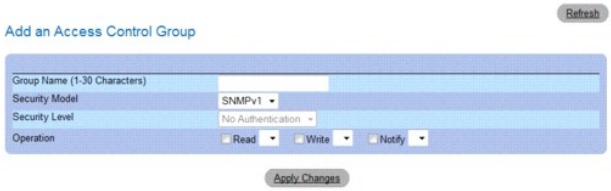
- **Read (Чтение).** доступ к управлению ограничивается доступом только для чтения, изменения назначенного представления SNMP невозможны.
- **Write (Запись).** доступ к управлению характеризуется доступом для чтения и записи, возможны изменения назначенного представления SNMP.
- **Notify (Уведомление).** отправляет прерывания для назначенного представления SNMP.

Определение групп SNMP

1. Откройте страницу **Access Control Group** (Группа контроля доступа).
2. Нажмите кнопку **Add** (Добавить).

Откроется страница **Add** an **Access Control Group** (Добавление группы контроля доступа).

Рис. 6-87. Add an Access Control Group (Добавление группы контроля доступа)



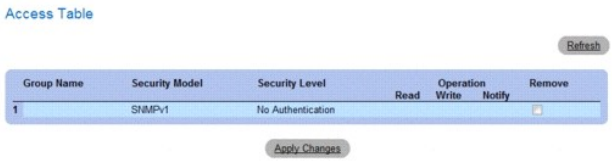
3. Определите поля на странице **Add an Access Control Group** (Добавление группы контроля доступа).
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Группа будет добавлена, а устройство обновлено.

Отображение таблицы доступа

1. Откройте страницу **Access Control Group** (Группа контроля доступа).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница Access Table (Таблица доступа).



Удаление групп SNMP

1. Откройте страницу **Access Control Group** (Группа контроля доступа).
2. Нажмите кнопку **Show All** (Показать все). Откроется страница Access Table (Таблица доступа).
3. Выберите **SNMP group** (Группа SNMP).
4. Установите флажок **Remove** (Удалить).
5. Нажмите кнопку **Apply Changes** (Применить изменения). Группа SNMP будет удалена, а устройство обновлено.

Определение контроля доступа SNMP с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для определения полей, отображаемых на странице **Access Control Group** (Группа контроля доступа).

Команда консоли	Описание
snmp-server group *имя группы* {**v1 | v2 | v3** {**noauth | auth | priv**}} [**read** *чтение*] [**write** *запись*] [**notify** *уведомление*]	Определяет конфигурацию группы SNMP (Simple Network Management Protocol) или таблицы, в которой устанавливается соответствие между пользователями SNMP и представлениями SNMP.
no snmp-server group *имя группы* [**v1 | v2 | v3** [**noauth | auth | priv**]] [**context** name]	Удаление указанной группы SNMP.

Далее приведен пример команд консоли.

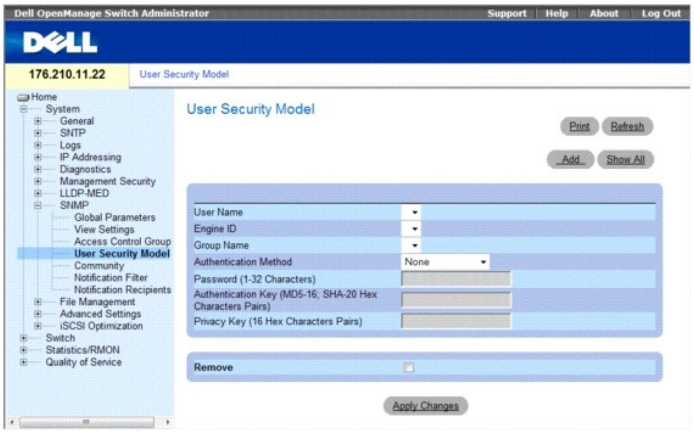
```
console (config)# snmp-server group user-group v3 priv read user-view
```

Назначение уровня безопасности SNMP пользователя

С помощью страницы **User Security Model** (USM) (Модель USM) можно назначать группам **SNMP** пользователей системы и определять метод проверки подлинности пользователей.

Чтобы открыть страницу U**ser Security Model** (Модель USM), click **System** (Система)→ **SNMP** (Система SNMP)→ U**ser Security Model** (Модель USM) на панели дерева.

Рис. 6-89. User Security Model (Модель USM)



- **User Name (Имя пользователя).** содержит список имен пользователя, определенных пользователем. Диапазон значений поля: до 30 буквенно-цифровых символов.
- **Engine ID (Идентификатор механизма).** определяет локальный или удаленный объект SNMP, к которому подключен пользователь. При изменении или удалении локального идентификатора механизма SNMP будет удалена база данных пользователей SNMP версии 3.
- **Group Name (Имя группы).** содержит список групп SNMP, определенных пользователем. Группы SNMP определяются на странице **Access Control Group (Группа контроля доступа).**
- **Authentication Method (Метод проверки подлинности).** метод проверки подлинности, используемый для определения подлинности пользователей. Возможные значения:
  - **MD5 Key (Ключ MD5).** проверка подлинности пользователей осуществляется с использованием алгоритма HMAC-MD5-96.
  - **SHA Key (Ключ SHA).** проверка подлинности пользователей осуществляется с использованием уровня HMAC-SHA-96.
  - **MD5 Password (Пароль MD5).** указывает, что для проверки подлинности используется пароль HMAC-MD5-96. Пользователь должен ввести пароль.
  - **SHA Password (Пароль SHA).** проверка пользователей осуществляется с использованием уровня проверки подлинности HMAC-SHA -96. Пользователь должен ввести пароль.
  - **None (Нет).** проверка подлинности пользователей не используется.
- **Password (0-32 Characters) (Пароль (0-32 символа)).** изменяет определенный пользователем пароль для группы. Пароли могут содержать не более 32 буквенно-цифровых символов.
- **Authentication Key (MD5-16; SHA-20 hexa chars) (Ключ проверки подлинности (MD5-16; SHA-20 шестнадцатеричных символов)).** определяет уровень проверки подлинности HMAC-MD5-96 or HMAC-SHA-96. Ключи проверки подлинности и конфиденциальности вводятся для определения ключа проверки подлинности. Если требуется только проверка подлинности, для MD5 определяются только 16 байт. Если требуется проверки и конфиденциальности, и подлинности, для MD5 определяются 32 байта. Каждый байт в строке шестнадцатеричного символа - это две

шестнадцатеричных цифры. Каждый байт должен быть разделен точкой или двоеточием.

- **Privacy Key (16 hexa characters) (Ключ конфиденциальности (16 шестнадцатеричных символов)).** если требуется только проверка подлинности, определяются только 20 байт. Если требуется проверка и конфиденциальности, и подлинности, определяются 16 байт. Каждый байт в строке шестнадцатеричного символа - это две шестнадцатеричных цифры. Каждый байт должен быть разделен точкой или двоеточием.
- **Remove (Удалить).** когда установлен этот флажок, удаляются пользователи из указанной группы.

Добавление пользователей в группу

1. Откройте страницу **User Security Model** (Модель USM).
2. Нажмите кнопку **Add** (Добавить).

Откроется страница **Add User Name** (Добавление имени пользователя).

Рис. 6-90. Add SNMPv3 User Name (Добавление имени пользователя SNMP версии 3)

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

   Пользователь будет добавлен к группе, а устройство обновлено.

Отображение таблицы USM (User Security Model)

1. Откройте страницу **User Security Model** (Модель USM).
2. Нажмите кнопку **Show All** (Показать все).

Откроется страница **User Security Model Table** (Таблица USM (User Security Model)).

Рис. 6-91. Таблица USM (User Security Model)

Удаление записи в таблице USM (User Security Model)

1. Откройте страницу **SNMPv3 User Security Model (USM)** (Модель USM протокола SNMP версии 3).
2. Нажмите кнопку Show All (Показать все). Откроется страница **User Security Model Table** (Таблица USM (User Security Model)).
3. Выберите запись **User Security Model Table** (Таблица USM (User Security Model)).
4. Установите флажок **Remove** (Удалить).
5. Нажмите кнопку **Apply Changes** (Применить изменения). Запись User Security Model Table (Таблица USM (User Security Model)) будет удалена, а

устройство обновлено.

Определение пользователей SNMP с помощью команд консоли

В следующей таблице приведены команды консоли для определения полей, отображаемых на странице **User Security Model** (Модель USM).

Команда консоли	Описание
snmp-server user *имя_пользователя имя_группы* [**remote** *строка-идентификатора-механизма*][**auth-md5** *пароль* | **auth-sha** *пароль* | **auth-md5-key** *md5-des-ключ* | **auth-sha-key** *sha-des-ключ*]	Определяет конфигурацию нового пользователя SNMP версии 3.
show snmp users [*имя_пользователя*]	Отображает конфигурацию пользователей.

Далее приведен пример команд консоли.

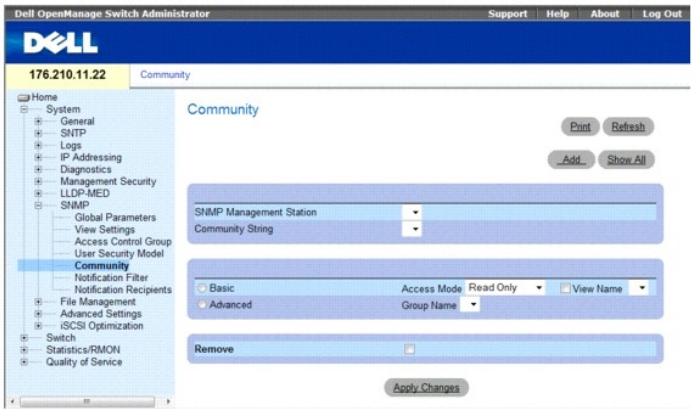
```
console (config)# snmp-server user John user-group auth-md5 1234

console(config)# end

console (config)# show snmp users
```

Name	Group Name	Auth Method	Remote
-------	----------	----------	------
John	user-group	md5	

Определение сообщества

Управление правами доступа осуществляется путем определения сообществ в таблице **Community Table** (Таблица сообществ). При изменении имен сообществ изменяются также и права доступа. Чтобы открыть страницу **SNMP Community** (Сообщество SNMP), выберите **System** (Система)→ **SNMP**→ **Community** (Сообщества) на панели дерева.

Рис. 6-92. SNMP Community (Сообщество SNMP)



- **SNMP Management Station (Станция управления SNMP).** список IP-адресов станций управления.
- **Community String (Строка сообщества).** работает в качестве пароля и используется для идентификации выбранной станции управления для устройства.
- **Basic Access Mode (Основной режим доступа).** определяет права доступа к сообществу. Возможные значения:
  - **Read Only (Только чтение).** доступ управления предоставляется только для чтения. Это справедливо для всех MIB, кроме таблицы сообществ, доступ к которой не предоставляется.
  - **Read Write (Чтение и запись).** доступ управления предоставляется с возможностью чтения и записи. Это справедливо для всех баз MIB, кроме таблицы сообществ, доступ к которой не предоставляется.
  - **SNMP Admin (Администратор SNMP).** доступ управления предоставляется с возможностью чтения и записи. Это справедливо для всех баз MIB, включая таблицу сообществ.

Установите флажок **Представление**, чтобы создать новое представление или выбрать имя существующего представления. Представление

определяет, какие объекты сообщества будут видимы.

- **Advanced (Расширенный).** выбирает расширенное представление SNMP.
- **Group Name (Имя группы).** имена ранее определенных групп. Группа определяет, какие объекты сообщества будут видимы.
- **Remove (Удалить).** когда установлен этот флажок, сообщество удаляется.

При определении нового сервера SNMP, будет доступен следующий дополнительный параметр:

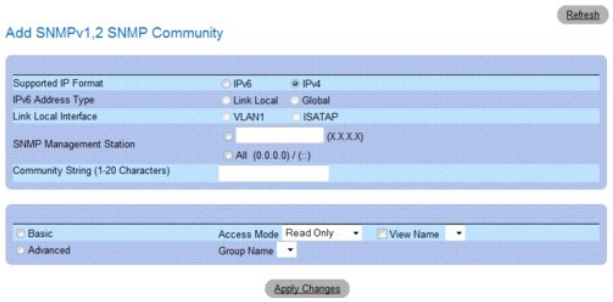
- **Supported IP Format (Поддерживаемый формат IP-адресов).** Отображает формат IP-адресов, поддерживаемый сообществом. Возможные значения:
  - **IPv6.** поддержка IP версии 6.
  - **IPv4.** поддержка IP версии 4.
- **IPv6 Address Type (Тип адреса IPv6).** В случае, если сообщество поддерживает систему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

Определение нового сообщества

1. Откройте страницу **SNMP Community** (Сообщество SNMP).
2. Нажмите кнопку **Add** (Добавить).

   Откроется страница **Add SNMP Community** (Добавление сообщества SNMP):

Рис. 6-93. Add SNMP Community (Добавление сообщества SNMP)



3. Выберите одно из следующих значений:
   - **SNMP Management Station (Станция управления SNMP).** определяет сообщество SNMP для отдельной станции управления. (Значение 0.0.0.0 означает выбор всех станций управления.)
   - **All (Все).** определяет сообщество SNMP для всех станций управления.
4. Определите оставшиеся поля.
5. Нажмите кнопку **Apply Changes** (Применить изменения).

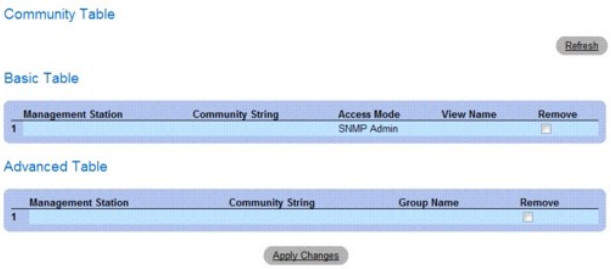
   Новое сообщество будет сохранено, а устройство обновлено.

Отображение всех сообществ:

1. Откройте страницу **SNMP Community** (Сообщество SNMP).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **Community Table** (Таблица сообществ).

Рис. 6-94. Community Table (Таблица сообществ)



Удаление сообществ

1. Откройте страницу **Community Table** (Таблица сообществ).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **Community Table** (Таблица сообществ).
3. Выберите сообщество в таблице **Community Table** (Таблица сообществ).
4. Установите флажок **Remove** (Удалить).
5. Нажмите кнопку **Apply Changes** (Применить изменения).

   Выбранная запись сообщества будет удалена, а устройство обновлено.

Настройка сообществ с помощью команд консоли

В следующей таблице приведены команды консоли для настройки полей, отображаемых на странице **Community Table** (Таблица сообществ).

Команда консоли	**Описание**
snmp-server community *community* [**ro** | **rw** | **su**] [*ipv4-address* | *ipv6-address*] [**view** *view-name*] [**type router** | **oob**]	Задает строку доступа к сообществу для разрешения доступа по протоколу SNMP.
snmp-server host {*ipv4-address* | *ipv6-address* | *hostname*} *community-string* [**traps** | **informs**] [**1** | **2**] [**udp-port** *port*] [**filter** *filtername*] [**timeout** *seconds*] [**retries** *retries*]	Определяет тип системных прерываний, отправляемых выбранному получателю.
snmp-server v3-host { *ipv4-address* | *ipv6-address* | *hostname*} *username* [**traps** | **informs**] {**noauth** | **auth** | **priv**} [**udp-port** *port*] [**filter** *filtername*] [**timeout** *seconds*] [**retries** *retries*]	Указывает получателя сообщения о работе SNMP версии 3.
show snmp	Выполняет проверку состояния сообществ SNMP.

Далее приведен пример команд консоли.

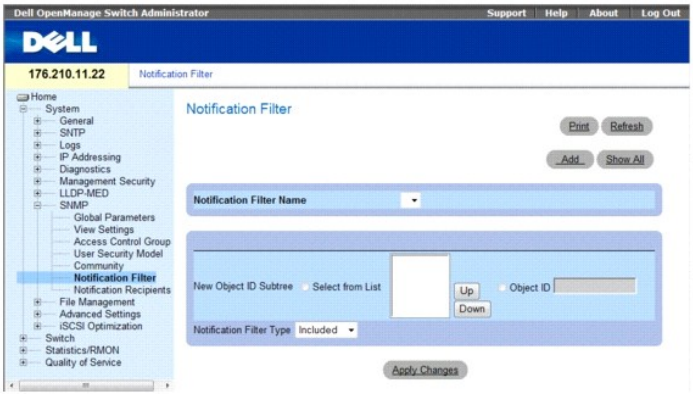
```
console(config)# snmp-server community public_1 su 1.1.1.1
console(config)# snmp-server community public_2 rw 2.2.2.2
console(config)# snmp-server community public_3 ro 3.3.3.3
console(config)# snmp-server host 1.1.1.1 public_1 1
console(config)# snmp-server host 2.2.2.2 public_2 2
console(config)#

console# show snmp

Community-String                Community-Access        IP address
---------------------------------
public_1                        super                   1.1.1.1
public_2                        readwrite               2.2.2.2
public_3                        readonly                3.3.3.3

Traps are enabled.
```

Authentication-failure trap is enabled.		
Trap-Rec-Address	Trap-Rec-Community	Version
System Contact: 345 6789		
System Location: 1234 5678		
console#		

Определение фильтров уведомлений

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 Filter** (Фильтры уведомлений) на панели дерева.

Рис. 6-95. Notification Filters (Фильтры уведомлений)



- **Notification Filter Name (Имя фильтра уведомлений).** фильтры уведомлений, определенных пользователем.
- **New Object ID Subtree (Новая ветвь идентификатора объекта).** идентификатор объекта, указывающий, какие из уведомлений отправлены или заблокированы. Если к идентификатору объекта (OID) применяется фильтр, системные прерывания или сообщения генерируются и отправляются получателям системных прерываний. Идентификаторы объектов либо выбираются в окне Select from List (Выбор из списка), либо в списке Object ID (Идентификатор объекта).
- **Notification Filter 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. 6-96. Add Filter (Добавление фильтра)

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

   Новый фильтр будет добавлен, а устройство обновлено.

Отображение таблицы фильтров

1. Откройте страницу **Notification Filter** (Фильтр уведомлений).
2. Нажмите кнопку **Show All** (Показать все).

Откроется страница Filter Table (Таблица фильтров).

Рис. 6-97. Filter Table (Таблица фильтров)

Удаление фильтра

1. Откройте страницу **Notification Filter** (Фильтр уведомлений).
2. Нажмите кнопку **Show All** (Показать все). Откроется страница **Filter Table** (Таблица фильтров).
3. Выберите запись в таблице **Filter Table** (Таблица фильтров).
4. Установите флажок **Remove** (Удалить). Запись фильтра будет удалена, а устройство обновлено.

Настройка фильтров уведомлений с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для определения полей, отображенных на странице **Notification Filters** (Фильтры уведомлений).

Команда консоли	**Описание**
snmp-server filter *имя_фильтра oid-tree* {**included** | **excluded**}	Создает или обновляет фильтр уведомлений SNMP.
show snmp filters [*имя_фильтра*]	Отображает конфигурацию фильтров уведомлений SNMP.

Далее приведен пример команд консоли:

```
Console (config)# snmp-server filter user1 iso included
Console (config)# end
Console # show snmp filters

Name        OID Tree      Type
----------  ------------  --------
user1       iso           Included
```

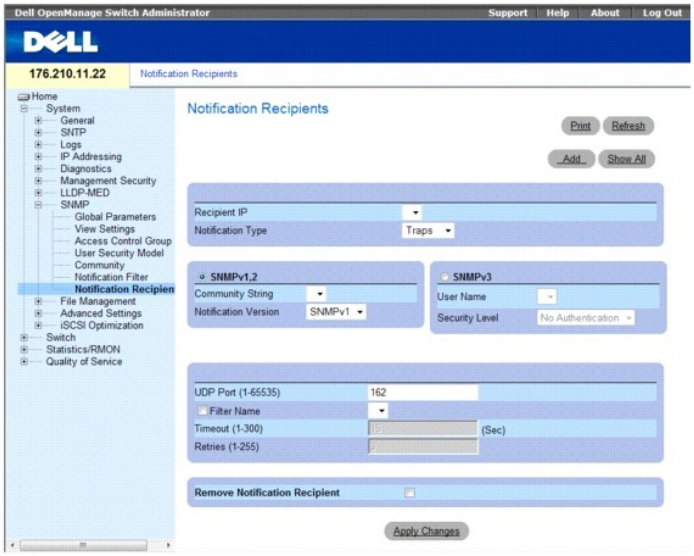
Определение получателей уведомлений SNMP

На странице **Notification Recipients** (Получатели уведомлений) представлена информация по настройке фильтров, которые указывают, отправляются ли системные прерывания определенным пользователям, а также тип системных прерываний. Фильтры уведомлений SNMP выполняют следующие функции.

- Определение объектов системных прерываний управления
- Фильтрация системных прерываний
- Выбор параметров генерации системных прерываний
- Обеспечение проверок контроля доступа

Чтобы открыть страницу **Notification Recipients** (Получатели уведомлений), выберите **System** (Система)→ **SNMP**→ **Notification Recipient** (Получатель уведомлений) на панели дерева.

Рис. 6-98. Notification Recipients (Получатели уведомлений)



- **Recipient IP (IP-адрес получателя).** IP-адрес, по которому отправляются системные прерывания.
  - **Notification Type (Тип уведомлений).** отправленное уведомление. Возможные значения:
  - **Traps (Прерывания).** отправленные прерывания.
  - **Informs (Сообщения).** отправленные сообщения.
- **SNMPv1,2 (SNMP версия 1, 2).** для выбранного получателя включен протокол SNMP версий 1 и 2. Заполните следующие поля для SNMPv1 и SNMPv2:
- **Community String (1-20 Characters) (Строка сообщества (1-20 символов)).** строка сообщества менеджера системных прерываний.
  - **Notification Version (Версия уведомления).** определяет версию уведомления. Возможные значения:
  - **SNMPv1.** отправляются системные прерывания SNMP версии 1.
  - **SNMPv2.** отправляются системные прерывания SNMP версии 1.
- **SNMPv3.** SNMPv3 используется для отправки и получения прерываний. Заполните следующие поля для SNMPv3:
- **User Name (Имя пользователя).** пользователь, которому отправляются уведомления SNMP.
- **Security Level (Уровень безопасности 1).** определяет средства, с помощью которых проверяется подлинность пакета. Возможные значения:
  - **No Authentication (Нет проверки подлинности).** не производится ни проверка подлинности, ни шифрование пакета.
  - **Authentication (Проверка подлинности).** производится проверка подлинности пакета.
  - **Privacy (Конфиденциальность).** производится и проверка подлинности, и шифрование пакета.
- **UDP Port (1-65535) (Порт UDP).** порт UDP, используемый для отправки уведомлений. Значение по умолчанию: 162.
- **Filter Name (Имя фильтра).** включает или исключает фильтры SNMP.
- **Timeout (1-300) (Тайм-аут).** время ожидания устройства (в секундах) перед повторной отправкой сообщений. Значение по умолчанию: 15 секунд.
- **Retries (1-255) (Повторные попытки).** число повторных попыток отправки устройством запросов. Значение по умолчанию: 3.
- **Remove Notification Recipient (Удаление получателя уведомлений).** когда установлен этот флажок, удаляет выбранных получателей уведомлений.

При добавлении получателя уведомления, будут доступны следующие дополнительные параметры:

- **Supported IP Format (Поддерживаемый формат IP-адресов).** Отображает формат IP-адресов, поддерживаемый получателем. Возможные

значения:

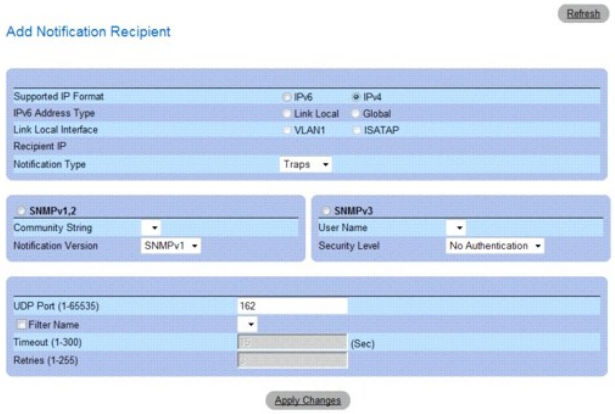
- **IPv6.** поддержка IP версии 6.
- **IPv4.** поддержка IP версии 4.

- **IPv6 Address Type (Тип адреса IPv6).** Если получатель поддерживает систему IPv6 (см. предыдущий параметр), здесь указывается поддерживаемый тип статических адресов. Возможные значения:
  - **Link Local (Локальная связь).** Адрес локальной связи, который не маршрутизируется, а используется только для связи в пределах той же сети.
  - **Global (Глобальный).** Глобальный уникальный адрес IPv6 address; он является видимым и доступным для различных подсетей.
- **Link Local Interface (Интерфейс локальной связи).** Если сервер поддерживает систему адресов локальной связи IPv6 (см. предыдущий параметр), здесь указывается интерфейс локальной связи. Возможные значения:
  - **VLAN1.** Интерфейс IPv6 конфигурируется по сети VLAN1.
  - **ISATAP.** Интерфейс IPv6 конфигурируется по туннелю ISATAP.

Добавление новых получателей системных прерываний

1. Откройте страницу **Notification Recipients** (Получатели уведомлений).
2. Нажмите кнопку **Add** (Добавить).

Откроется страница **Add Notification Recipients** (Добавление получателей уведомлений).



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

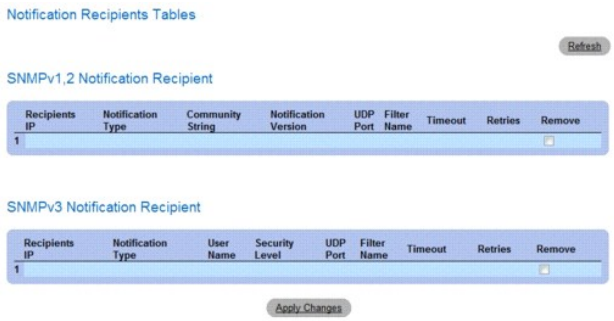
   Получатель уведомлений будет добавлен, а устройство обновлено.

Отображение таблиц получателей уведомлений

1. Откройте страницу **Notification Recipients** (Получатели уведомлений).
2. Нажмите кнопку **Show All** (Показать все).

Откроется страница **Notification Recipients Tables** (Таблицы получателей уведомлений).

Рис. 6-99. Таблицы получателей уведомлений



Удаление получателей уведомлений

1. Откройте страницу **Notification Recipients** (Получатели уведомлений).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **Notification Recipients Tables** (Таблицы получателей уведомлений).
3. Выберите получателя уведомлений в таблице **SNMPV1,2 Notification Recipient** (Получатель уведомлений SNMP версии 1, 2) или S**NMPv3 Notification Recipient** (Получатель уведомлений SNMP версии 3).
4. Установите флажок **Remove** (Удалить).
5. Нажмите кнопку **Apply Changes** (Применить изменения). Получатель будет удален, а устройство обновлено.

Настройка получателей уведомлений SNMP с помощью команд консоли

В следующих таблицах приведены команды консоли для определения полей, отображаемых на странице **Notification Recipients** (Получатели уведомлений).

Команда консоли	**Описание**
snmp-server host {*ip-адрес* | *имя_хоста*} *community-string* [**traps** | **informs**] [**1** | **2**] [**udp-port** *номер_порта*] [**filter** *имя_фильтра*] [**timeout** *секунды*] [**retries** *число_попыток*]	Создает или обновляет получателя уведомлений SNMP версий 1 или 2.
snmp-server v3-host {ip-*адрес* | *имя_хоста*} *имя_пользователя* [**traps** | **informs**] {**noauth** | **auth** | **priv**} [**udp-port** *номер_порта*] [**filter** *имя_фильтра*] [**timeout** *секунды*] [**retries** *число_попыток*]	Создает или обновляет получателя уведомлений SNMP версии 3.
show snmp	Показывает текущую конфигурацию SNMP.

Далее приведен пример команд консоли.

```
console (config)# snmp-server host 172.16.1.1 private

console# show snmp
```

Community-String	Community-Access	View name	IP address
---	---	---	---
public	read only	просмотр пользователя	All
private	read write	по умолчанию	172.16.1.1
private	su	DefaultSuper	172.17.1.1

Управление файлами

Страница **File Management** (Управление файлами) содержит поля для управления программным обеспечением устройства, файлами образов, а также файлами настройки. Файлы можно загрузить с сервера TFTP.

Обзор управления файлами

Структура файлов настройки состоит из следующих файлов настройки:

- **Startup Configuration File (Файл настройки для запуска).** содержит команды, необходимые для восстановления тех же параметров настройки устройства при отключении или перезагрузке устройства. Файл для запуска создается путем копирования команд настройки из файла рабочей настройки или файла образа.
- **Running Configuration File (Файл рабочей настройки).** содержит все команды файла для запуска, а также все команды, введенные во время последнего сеанса. После отключения или перезагрузки устройства все команды, сохраненные в файле рабочей настройки, теряются. В ходе запуска все команды файла для запуска копируются в файл рабочей настройки и применяются для устройства. 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.
- **Image files (Файлы образа).** системные образы сохраняются в двух файлах Flash, называемых образами (Image 1 и Image 2). Активный образ включает активную копию, остальные - вторую копию. Устройство загружается и запускается из активного образа. Если активный образ поврежден, система автоматически загружается из неактивного образа. Эта функция защиты от сбоев, возникающих в процессе обновления программного обеспечения.

Чтобы открыть страницу **File Management** (Управление файлами), выберите **System** (Система)→ **File Management** (Управление файлами) на панели дерева. Страница **File Management** (Управление файлами) содержит следующие ссылки:

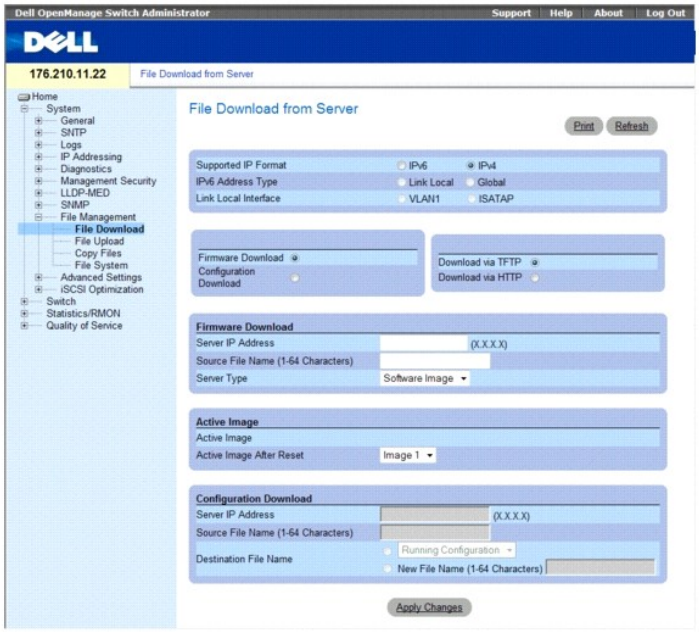
- File Download from Server (Загрузка файла с сервера)
- File Upload to Server (Выгрузка файла на сервер)
- Copy Files

  (Копирование файлов)
- File on File System (Файл в файловой системе)

Загрузка файлов

Страница **File Download From Server** (Загрузка файлов с сервера) содержит поля для загрузки системного образа и файлов настройки с сервера TFTP или HTTP-клиента на устройство. Чтобы открыть страницу **File Download From Server** (Загрузка файлов с сервера), выберите **System** (Система)→ **File Management** (Управление файлами)→ **File Download** (Загрузка файла) на панели дерева.

Рис. 6-100. File Download from Server (Загрузка файлов с сервера)



- **Supported IP Format (Поддерживаемый формат IP-адресов).** Отображает формат IP-адресов, поддерживаемый сервером. Возможные значения:
  - **IPv6.** поддержка IP версии 6.
  - **IPv4.** поддержка IP версии 4.
- **IPv6 Address Type (Тип адреса IPv6).** В случае, если сервер поддерживает систему IPv6 (см. предыдущий параметр), здесь указывается поддерживаемый тип статических адресов. Возможные значения:
  - **Link Local (Локальная связь).** Адрес локальной связи, который не маршрутизируется, а используется только для связи в пределах той же

сети.

- **Global (Глобальный).** Глобальный уникальный адрес IPv6 address; он является видимым и доступным для различных подсетей.

- **Link Local Interface (Интерфейс локальной связи).** Если сервер поддерживает систему адресов локальной связи IPv6 (см. предыдущий параметр), здесь указывается интерфейс локальной связи. Возможные значения:
  - **VLAN1.** Интерфейс IPv6 конфигурируется по сети VLAN1.
  - **ISATAP.** Интерфейс IPv6 конфигурируется по туннелю ISATAP.
- **Firmware Download (Загрузка микропрограммы).** загружается файл микропрограммы. Если поле **Firmware Download** (Загрузка встроенных программ) выделено, то поля **Configuration Download** (Загрузка конфигурации) недоступны.
- **Configuration Download (Загрузка настройки).** загружается файл настройки. Если выбран параметр **Configuration Download** (Загрузка настройки), поля **Firmware Download** (Загрузка микропрограммы) недоступны.
- **Download via TFTP (Загрузить через TFTP).** загружает образ через сервер TFTP.
- **Download via HTTP (Загрузить через HTTP).** загружает образ через сервер HTTP.

Firmware Download (Загрузка микропрограммы)

- **Server IP Address (IP-адрес сервера).** IP-адрес сервера, с которого загружаются файлы микропрограммы.
- **Source File Name (1-64 Characters) (Имя исходного файла (1-64 символа)).** обозначает файл для загрузки.

Active Image (Активный образ)

- **Active Image (Активный образ).** текущий активный файл образа.
- **Active Image After Reset (Активный образ после перезагрузки).** файл образа, который станет активным после перезагрузки устройства.

Configuration Download (Загрузка конфигурации)

- **Server IP Address (IP-адрес сервера).** IP-адрес сервера, с которого загружаются файлы конфигурации.
-
- **Source File Name (1-64 Characters) (Имя исходного файла (1-64 символа)).** обозначает файлы конфигурации для загрузки.
- **Destination (Файл назначения).** файл, в который будет загружен файл настройки.

Возможные значения:

- **Running Configuration (Рабочая настройка).** команды загружаются в файл рабочей настройки.
- **Startup Configuration (Настройка для запуска).** загружается и переписывается файл настройки для запуска.
- **<filename>.** Загружает команды в резервный конфигурационный файл. Имя файла определяется пользователем при загрузке.

Образ из файла заменяет неактивный образ. Рекомендуется определить неактивный образ, который станет активным после сброса, а затем выполнить сброс устройства после загрузки. Во время загрузки файла образа откроется диалоговое окно, в котором отобразится состояние процесса выполнения. Окно закроется автоматически по завершении загрузки.

Каждый знак «!» свидетельствует об успешной передаче десяти пакетов.

Загрузка файлов

1. Откройте страницу **File Download from Server** (Загрузка файлов с сервера).
2. Определите тип файла для загрузки.
3. Определите поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Программное обеспечение будет загружено на устройство.

Загрузка файлов с сервера с помощью команд консоли

В следующей таблице приведены команды консоли для настройки полей, отображаемых на странице **File Download From Server** (Загрузка файлов с сервера).

Команда консоли	Описание
copy *url_источника url_приемника* [**snmp**]	Копирует файл из исходного местоположения в место назначения.

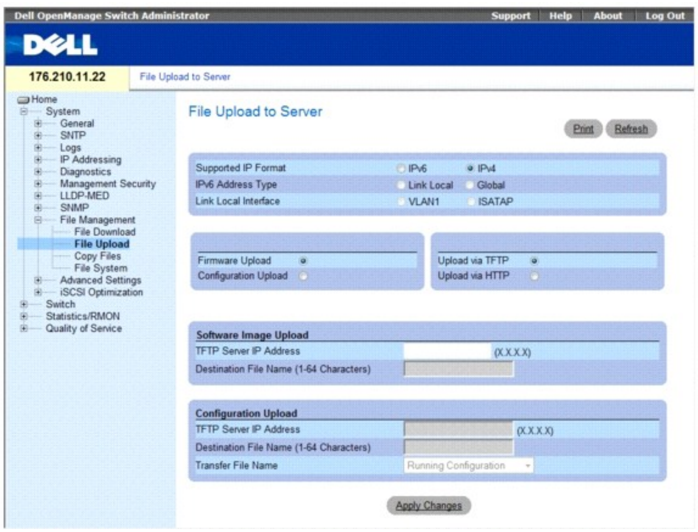
Далее приведен пример команд консоли.

```
console# copy running-config tftp://11.1.1.2/pp.txt

Accessing file 'file1' on 172.16.101.101.

Loading file1 from 172.16.101.101: !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !!!!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !!!!!!!!!!!!!!!!!!!!!!!
[OK]

Copy took 0:01:11 [hh:mm:ss]
```

Передача файлов на сервер

На странице **File Upload to Server** (Загрузка файла на сервер) содержатся поля для загрузки программного обеспечения с сервера TFTP на устройство. Чтобы открыть страницу **File Upload to Server** (Передача файлов на сервер), выберите **System** (Система)→ **File Management** (Управление файлами)→ **File Upload** (Передача файла) на панели дерева.

Рис. 6-101. File Upload to Server (Передача файлов на сервер)



- **Supported IP Format (Поддерживаемый формат IP-адресов).** Отображает формат IP-адресов, поддерживаемый сервером SNTP. Возможные значения:
  - **IPv6.** поддержка IP версии 6.
  - **IPv4.** поддержка IP версии 4.
- **IPv6 Address Type.** В случае, если сервер поддерживает систему IPv6 (см. предыдущий параметр), здесь указывается поддерживаемый тип статических адресов. Возможные значения:
  - **Link Local (Локальная связь).** Адрес локальной связи, который не маршрутизируется, а используется только для связи в пределах той же сети.
  - **Global (Глобальный).** Глобальный уникальный адрес IPv6 address; он является видимым и доступным для различных подсетей.
- **Link Local Interface (Интерфейс локальной связи).** Если сервер поддерживает систему адресов локальной связи IPv6 (см. предыдущий параметр), здесь указывается интерфейс локальной связи. Возможные значения:
  - **VLAN1.** Интерфейс IPv6 конфигурируется по сети VLAN1.
  - **ISATAP.** Интерфейс IPv6 конфигурируется по туннелю ISATAP.
- **Firmware Upload (Передача микропрограммы).** передается файл микропрограммы. Если выбран параметр **Firmware Upload** (Передача микропрограммы), поля **Configuration Upload** (Передача настройки) недоступны.
- **Configuration Upload (Передача файла настройки).** передаются файлы настройки. Если выбран параметр **Configuration Upload** (Передача настройки), поля **Firmware Upload** (Передача микропрограммы) недоступны.
- **Upload via TFTP (Передача через TFTP).** передает образ через сервер TFTP.
- **Upload via HTTP (Передача через HTTP).** передает образ через сервер FTP.

Software Image Upload (Передача образа программы)

- **TFTP Server IP Address (IP-адрес сервера TFTP).** IP-адрес сервера TFTP, на который передается файл образа.
- **Destination File Name (1-64 Characters)** (Имя файла назначения (1-64 символа)). путь к файлу образа, куда передается файл.

Configuration Upload (Передача файла настройки)

- **TFTP Server IP Address (IP-адрес сервера TFTP).** IP-адрес сервера TFTP, на который передается файл настройки.
- **Destination File Name (1-64 Characters) (Имя файла назначения (1-64 символа)).** путь к файлу настройки, куда передается файл.
- **Transfer File Name (Имя передаваемого файла).** программный файл, в который выполняется передача файла настройки. Этот определенный пользователем список файлов настройки отображается, если пользователь создал резервные файлы настройки. Например, если пользователь скопировал файлы рабочей настройки в определенный пользователем файл настройки BACKUP-SITE-1, этот список отобразится на странице File Upload to Server (Передача файла на сервер) и файл настройки BACKUP-SITE-1 отобразится в списке. Возможные значения полей:
  - **Running Configuration (Рабочая настройка).** передает текущий файл настройки.
  - **Startup Configuration (Настройка для запуска).** передает файл настройки для запуска.
  - **<filename>.** Загружает указанный конфигурационный файл. Имя файла определяется пользователем при загрузке.

Передача файлов на сервер

1. Откройте страницу **File Upload to Server** (Передача файлов на сервер).
2. Определите тип файла для загрузки.
3. Определите поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Программное обеспечение будет передано с устройства.

Передача файлов на сервер с помощью команд консоли

В следующей таблице приведены команды консоли для настройки полей, отображаемых на странице **File Upload to Server** (Загрузка файлов на сервер).

Команда консоли	**Описание**
copy *url_источника url_приемника* [**snmp**]	Копирует файл из исходного местоположения в место назначения.

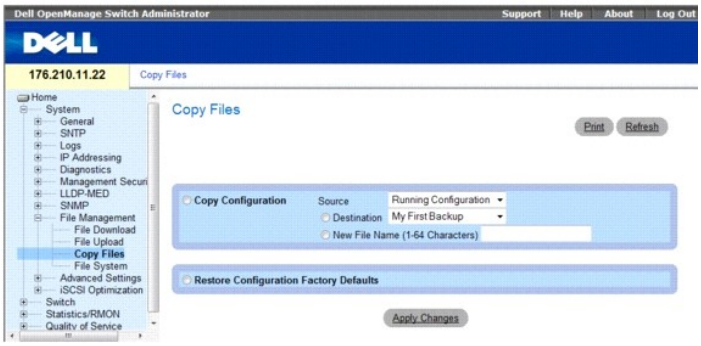
Далее приведен пример команд консоли.

```
console# copy image tftp://10.6.6.64/uploaded.ros

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

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

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

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

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

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

Copy (Копировать): 4234656 bytes copied in 00:00:33 [hh:mm:ss]

01-Jan-2000 07:30:42 %COPY-W-TRAP: The copy operation was
completed successfully
```

Копирование файлов

Файлы можно копировать и удалять со страницы **Copy Files** (Копирование файлов). Чтобы открыть страницу **Copy Files** (Копирование файлов), выберите **System** (Система)→ **File Management** (Управление файлами)→ **Copy Files** (Копирование файлов) на панели дерева.

Рис. 6-102. Copy Files (Копирование файлов)



- **Copy Configuration (Копировать настройку).** когда установлен этот флажок, выполняется копирование файлов настройки в указанный файл назначения.
  - **Source (Исходный).** указывает тип файла, который необходимо скопировать в файл назначения. Выберите файл рабочей настройки или файл настройки запуска.
  - **Destination (Целевой).** указывает целевой файл настройки, в который копируется исходный файл. Выберите резервный файл, файл рабочей настройки или файл настройки запуска.
  - **New File Name (Новое имя файла).** указывает имя созданного резервного файла настройки.
- **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.

Копирование файлов

1. Откройте страницу **Copy Files** (Копирование файлов).
2. Заполните поля **Copy Configuration** (Копирование настройки).
3. Нажмите кнопку **Apply Changes** (Применить изменения).

   Файл будет скопирован, а устройство обновлено.

Восстановление заводских настроек по умолчанию

1. Откройте страницу **Copy Files** (Копирование файлов).
2. Выберите **Restore Company Factory Defaults** (Восстановить заводские файлы настройки).
3. Нажмите кнопку **Apply Changes** (Применить изменения).

   Заводские настройки по умолчанию будут восстановлены, а устройство обновлено.

Копирование и удаление файлов с помощью команд консоли

В следующей таблице приведены команды консоли для настройки полей, отображаемых на странице **Copy Files** (Копирование файлов).

Команда консоли	**Описание**
copy *url_источника url_приемник***а [snmp]**	Копирует файл из исходного местоположения в место назначения.
delete startup-config	Удаляет файл конфигурации для запуска.

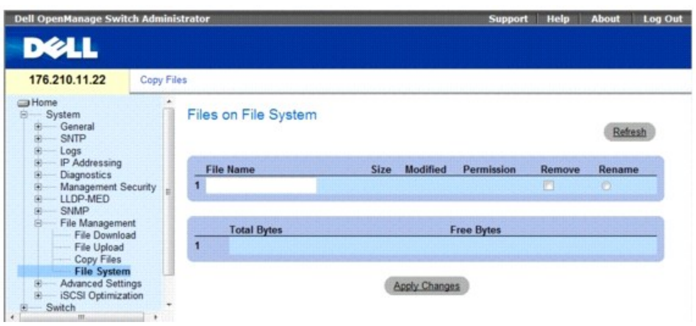
Далее приведен пример команд консоли.

```
Console # copy tftp://172.16.101.101/file1 image

Accessing file 'file1' on 172.16.101.101.

Loading file1 from
172.16.101.101: !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK]

Copy took 0:01:11 [hh:mm:ss]

Console# delete startup-config



Console# copy running-config startup-config

01-Jan-2000 01:55:03 %COPY-W-TRAP: The copy operation was completed successfully

Copy succeeded
```

Управление файлами устройства

На странице **Files on File System** (Файлы в файловой системе) представлена информация о файлах, хранящихся в системе, включая имена файлов, размеры файлов, изменения файлов и разрешения файлов. Файловая система позволяет выполнять управление до пяти файлов с общим размером до 3 МБ. Чтобы открыть страницу **Files on File System** (Файлы в файловой системе), выберите **System** (Система)→ **File Management** (Управление файлами)→ **File System** (Файловая система) на панели дерева.

Рис. 6-103. Файлы в файловой системе



На странице **Files on File System** (Файлы в файловой системе) содержатся следующие поля:

- **File Name (Имя файла).** обозначает файл, хранящийся в системе управления файлами.
- **Size (Размер).** означает размер файла.
- **Modified (Изменен).** обозначает дату изменения файла.
- **Permission (Разрешение).** указывает тип разрешения, назначенный файлу. Возможные значения:
  - **Read Only (Только чтение).** обозначает файл, предназначенный только для чтения.
  - **Read Write (Чтение и запись).** обозначает файл, предназначенный для чтения и записи.
- **Remove (Удалить).** удаляет файл при выборе.
- **Rename (Переименовать).** изменяет имя файла. Имя файла изменяется в поле **File Name** (Имя файла).
- **Total Bytes (Всего байт).** обозначает общее количество занятого в данный момент места.
- **Free Bytes (Свободные байты).** обозначает количество оставшегося на данный момент свободного места.

Управление файлами с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для управления файлами системы

Команда консоли	Описание
dir	Отображение списка файлов в файловой системе флэш-памяти

Далее приведен пример команд консоли.

console# **dir**				
Папка флэш-памяти:				
Имя файла	Разрешение	Объем флэш-памяти	Размер данных	Изменено
----------	------	------	------	----------
3.txt	rw	524288	523776	22-Feb-2005 18:49:27
setup	rw	524288	95	22-Feb-2005 15:58:19
setup2	rw	524288	95	22-Feb-2005 15:58:35
image-1	rw	4325376	4325376	06-Feb-2005 17:55:32
image-2	rw	4325376	4325376	06-Feb-2005 17:55:31
test.txt	rw	524288	95	22-Feb-2005 12:16:44
aaafile.prv	--	131072	--	06-Feb-2005 19:09:02
syslog1.sys	r-	262144	--	22-Feb-2005 18:49:27
syslog2.sys	r-	262144	--	22-Feb-2005 18:49:27
directory.prv	--	262144	--	06-Feb-2005 17:55:31
startup-config	rw	524288	347	22-Feb-2005 11:56:03
Общий объем флэш-памяти: 16646144 байт				
Свободное место на флэш-памяти: 4456448 байт				

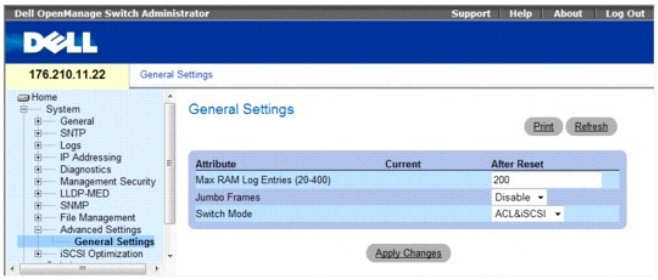
Определение расширенных параметров

Страница **Advanced Settings** (Расширенные параметры) содержит ссылки для настройки общих параметров. Расширенные параметры используются для настройки прочих глобальных атрибутов устройства. Изменения для этих атрибутов применяются только после сброса устройства. Чтобы открыть страницу **Advanced Settings** (Расширенные параметры), выберите **System** (Система)→ **Advanced Settings** (Расширенные параметры) на панели дерева.

Общие параметры точной настройки устройства

Страница **General Settings** (Общие параметры) сдержит информацию, позволяющую определить общие параметры устройства. Чтобы открыть страницу **General Settings** (Общие параметры), выберите **System** (Система)→ **Advanced Settings** (Расширенные параметры)→ **General** (Общие) на панели дерева.

Рис. 6-104. General Settings (Общие параметры)



- **Attribute (Атрибут).** общий атрибут параметра.
- **Current (Текущее).** текущее настроенное значение.
- **After Reset (После перезагрузки).** будущее значение (после перезагрузки). При вводе значения в столбце After Reset (После сброса) выделяется память для поля таблицы.

- **Max RAM Log Entries (20-400) (Максимальное число записей журнала ОЗУ).** максимальное число записей журнала ОЗУ. Когда журнал заполнен, он очищается, и файл журнала перезагружается.
- **Jumbo Frames (Большие кадры).** включает или отключает поддержку больших кадров. Большие кадры позволяют передавать данные меньшим числом пакетов. Это уменьшает объем служебной информации, время обработки и перерывы.
- **Switch Mode (Режим коммутации).** Указывает рабочий режим устройства. Новый режим вступает в силу после перезагрузки устройства. Возможные значения:
  - **ACL & iSCSI.** Устройство использует списки управления доступом и iSCSI. Динамическое назначение VLAN не используется. Для получения более подробной информации, см. разделы ACL Overview (Обзор ACL) и Optimizing iSCSI (Оптимизация iSCSI).
  - **DVA & iSCSI.** Устройство использует динамическое назначение VLAN и iSCSI. Списки управления доступом не используются. Для получения более подробной информации, см. раздел Configuring Advanced Port Based Authentication (Настройка расширенной проверки подлинности на базе портов) и Optimizing iSCSI (Оптимизация iSCSI).

Просмотр счетчика записей журнала ОЗУ с помощью команд консоли

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

Команда консоли	Описание
logging buffered size *число*	Задает число системных сообщений, хранящихся во внутреннем буфере (ОЗУ).
port jumbo-frame	Включает поддержку больших кадров для устройства.
show port jumbo-frame	Показывает информацию о больших кадрах для данного устройства.

Далее приведен пример команд консоли.

```
Console (config)# logging buffered size 300
```

Оптимизация iSCSI

iSCSI - протокол связи, используемый для обмена данными между файловыми серверами и носителями. Файловые серверы называются *инициаторами*, а диски - *конечными устройствами*. Можно оптимизировать поток iSCSI, установив параметры приоритета кадров с помощью функции Quality of Service (Качество обслуживания) на устройстве. Устройство может также перехватывать кадры iSCSI и предоставлять информацию о связи iSCSI (называемой сеансами).

Настройка общих параметров iSCSI

На странице **iSCSI Optimization Global Parameters** (Общие параметры оптимизации iSCSI) отображаются параметры, которые влияют на способ обработки устройством кадров iSCSI.

iSCSI можно настроить для QoS. На странице **iSCSI Optimization Global Parameters** (Общие параметры оптимизации iSCSI), необходимо включить iSCSI, установить классификацию для CoS или DSCP. Также имеется возможность включить подачу соообщения, предназначенного для изменения поля приоритета DSCP или Cos для данного пакета. На страницах QoS можно затем установить очередь для *строгого приоритета* или *WRR*, затем соотнести CoS или DSCP с соответствующей очередью. Очередь необходимо задать на странице **Qos Queue Settings** (Параметры очереди QoS) и выполнить привязку к очереди на странице **QoS CoS to Queue** (Привязка QoS CoS к очереди) или **DSCP to Queue** (DSCP к очереди).

Соблюдайте осторожность при задании параметров QoS. Например, если для очереди задать значение WRR и указать небольшой размер, трафик iSCSI будет снижен при перегрузке.

Чтобы открыть страницу **iSCSI Optimization Global Parameters** (Общие параметры оптимизации iSCSI), выберите **System** (Система)→ **iSCSI Optimization** (Оптимизация iSCSI)→ **Global Parameters** (Общие параметры) на панели дерева.

Рис. 6-105. Global Parameters (Общие параметры)

- **iSCSI Status (Состояние iSCSI).** при включении или отключении оптимизации iSCSI на устройстве. Значением по умолчанию является **включено**.
- **Classification (Классификация).** определение приоритета пакетов iSCSI с помощью CoS или DSCP. Выберите классификацию, затем необходимо значение.
- **Remark (Повторно пометить).** включение повторных пометок iSCSI на устройстве.
- **iSCSI Aging Time (Время хранения iSCSI).** время ожидания устройства после последнего полученного кадра сеанса iSCSI до удаления сеанса из списка.

Настройка общих параметров iSCSI:

1. Откройте страницу iSCSI Optimization **Global Parameters** (Общие параметры оптимизации iSCSI).
2. Измените соответствующие поля.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Определение общих параметров iSCSI с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для определения полей, отображаемых на странице **iSCSI Global Parameters** (Общие параметры iSCSI).

Команда консоли	**Описание**
iscsi enable no iscsi enable	Для глобального включения осведомленности iSCSI используйте команду включения iscsi в режиме общей настройки. Чтобы отключить осведомленность iSCSI, используйте форму no этой команды.
iscsi cos {**up** *vpt* | **dscp** *dscp*} [**remark**] [**bandwidth** *flow-bandwidth*] [**burstsize** *flow-burstsize*] no iscsi cos	Чтобы задать профиль качества обслуживания, который будет применен к потокам iSCSI, используйте команду iscsi cos. Чтобы восстановить значение по умолчанию, используйте форму no этой команды.
iscsi aging time *time* no iscsi aging time	Чтобы задать время хранения сеансов iSCSI, используйте команду iscsi aging time в режиме Global Configuration. Чтобы отменить хранение, используйте форму no этой команды.
show iscsi	Чтобы отобразить параметры iSCSI, используйте команду show iscsi в режиме Privileged EXEC.

Figure 6-107. Ниже приводится пример команд консоли.

```
Console# show iscsi

Target: iqn.1993-11.com.disk-vendor:diskarrays.sn.45678

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

Session 1:

---------

Initiator: iqn.1992-04.com.os-vendor.plan9:cdrom.12.

storage:sys1.xyz
```

```
Time started: 23-Jul-2002 10:04:50

Time for aging out: 10 min

ISID: 11


Initiator Initiator Target Target

IP address TCP port IP address IP port

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

172.16.1.3 49154 172.16.1.20 30001

172.16.1.4 49155 172.16.1.21 30001

172.16.1.5 49156 172.16.1.22 30001


Session 2:

---------

Initiator: iqn.1995-05.com.os-vendor.plan9:cdrom.10

Time started: 23-Jul-2002 21:04:50

Time for aging out: 2 min

ISID: 22


Initiator Initiator Target Target

IP address TCP port IP address IP port

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

172.16.1.30 49200 172.16.1.20 30001

172.16.1.40 49201 172.16.1.21 30001
```

Управление конечными устройствами iSCSI

Таблица **iSCSI Targets Table** (Таблица конечных устройств iSCSI) содержит информацию о конечных устройствах iSCSI в сети.

Чтобы открыть страницу **iSCSI Targets Table** (Таблица конечных устройств iSCSI), выберите **System** (Система)→ **iSCSI Optimization** (Оптимизация iSCSI)→ **iSCSI Targets** (Конечные устройства iSCSI) на панели дерева.

Рис. 6-108. iSCSI Targets Table (Таблица конечных устройств iSCSI)

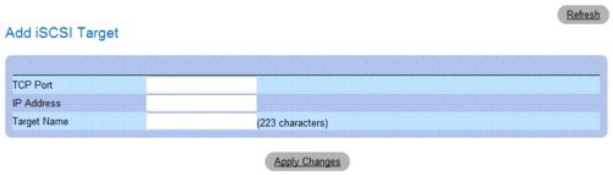
- **TCP Port (Порт TCP).** порт TCP используется конечным устройством для связи iSCSI.
- **IP Address (IP-адрес).** IP-адрес конечного устройства. IP-адрес 0.0.0.0 является *любым* IP -адресом.
- **Target Name (Имя конечного устройства).** имя конечного устройства.
- **Remove (Удалить).** используется для удаления конечных устройств в таблице.

Adding Targets (Добавление конечных устройств)

1. Откройте таблицу **iSCSI Targets Table** (Таблица конечных устройств iSCSI).
2. Нажмите кнопку **Add** (Добавить).

   Откроется страница **Add iSCSI Target** (Добавление конечного устройства iSCSI).

Рис. 6-109. Add iSCSI Target (Добавление конечного устройства iSCSI)



3. Укажите параметры.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Удаление конечных устройств

1. Откройте таблицу **iSCSI Targets Table** (Таблица конечных устройств iSCSI).
2. Установите флажок **Remove** (Удалить) рядом с каждым конечным устройством, которое необходимо удалить.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Определение конечных устройств iSCSI с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для определения полей, отображаемых на странице **iSCSI Targets Table** (Таблица конечных устройств iSCSI).

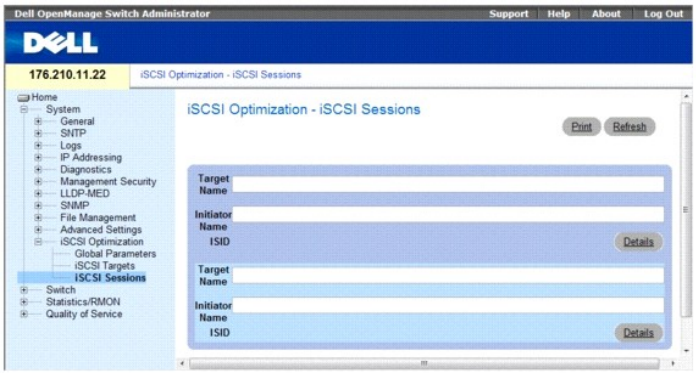
Команда консоли	**Описание**
iscsi target port *tcp-порт-1* [*tcp-порт-2... tcp-порт-8*] [**address** *ip-адрес*] [**name** *имя_конечного_устройства*]	Чтобы определить конфигурацию портов iSCSI, адрес и имя конечного устройства, используйте команду iscsi target port в режиме Global Configuration. Для удаления портов и целевого устройства iSCSI используйте форму no этой команды.
no iscsi target port *tcp-порт-1* [*tcp-порт-2... tcp-порт-8*] [**address** *ip-адрес*]	Для удаления портов и целевого устройства iSCSI используйте форму no этой команды.
show iscsi sessions	Отображает текущие сеансы iSCSI.

Мониторинг сеансов iSCSI

На странице **iSCSI Sessions** (Сеансы iSCSI) содержится информация о связи iSCSI в устройстве.

Чтобы открыть страницу iSCSI Sessions (Сеансы iSCSI), выберите **System** (Система)→ **iSCSI Optimization** (Оптимизация iSCSI)→ **iSCSI Sessions** (Сеансы iSCSI) на панели дерева.

Рис. 6-111. iSCSI Sessions (Сеансы iSCSI)



Для каждого сеанса отображается следующая информация:

- **Target Name (Имя конечного устройства).** имя конечного устройства.
- **Initiator Name (Имя инициатора).** имя инициатора.
- **ISID.** идентификатор сеанса iSCSI.

При нажатии кнопки **Details** (Подробно) для сеанса отображается дополнительная информация:

- **Session Life Time (Продолжительность сеанса).** время, прошедшее с начала первого кадра сеанса.
- **Aging Time (Срок хранения).** время, оставшееся до истечения срока хранения сеанса и его удаления.
- **Initiators/Targets IP Address/TCP Port (Инициаторы/IP-адрес конечных устройств/порт TCP).** IP-адрес и порт TCP, используемые каждым инициатором и конечным устройством во время сеанса.

Определение сеансов iSCSI с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для определения полей, отображаемых на странице **iSCSI Sessions** (Сеансы iSCSI).

Команда консоли	**Описание**
`show iscsi sessions [`*`подробно`*`]`	Чтобы отобразить сеансы iSCSI, используйте команду show iscsi sessions в режиме Privileged EXEC.

Далее приведен пример команд консоли.

```
Console# show iscsi sessions


iSCSI enabled

iSCSI vpt: 5, remark

Session aging time: 60 min

Maximum number of sessions: 256


iSCSI targets and TCP ports:

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


TCP Target IP Name

Port Address

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

860

3260

5000
```

```
30001 172.16.1.1 iqn.1993-11.com.disk-vendor:diskarrays.sn.45678.tape:sys1.xyz

30033 172.16.1.10

30033 172.16.1.25
```

Назад на страницу содержания

Назад на страницу содержания

Руководство пользователя систем Dell™ PowerConnect™ 54xx

ПРИМЕЧАНИЕ. ПРИМЕЧАНИЕ указывает важную информацию, которая необходима для содействия пользователю при работе с компьютером.

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

ОСТОРОЖНЫ. Сообщение БУДЬТЕ ОСТОРОЖНЫ указывает на возможность материального ущерба, травмы или летального исхода.

Декабрь, 2008 Ред. A01

Назад на страницу содержания

Назад на страницу содержания

Использование Dell OpenManage Switch Administrator

Руководство пользователя систем Dell™ PowerConnect™ 54xx

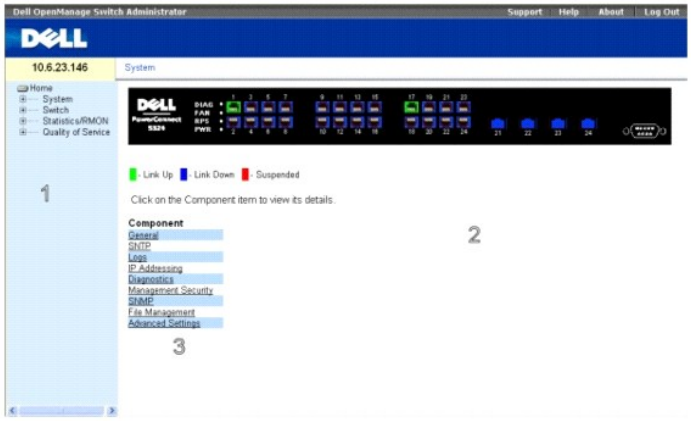
В этом разделе представлено описание интерфейса пользователя.

Элементы интерфейса

Домашняя страница содержит следующие панели:

- **Панель дерева.** Расположена в левой части домашней страницы и представляет собой развертываемое дерево параметров и их компонентов.
- **Панель устройства.** Расположена с правой стороны домашней страницы и отображает вид устройства, информационную или табличную область и инструкции по настройке.

Рис. 5-1. Компоненты программы Switch Administrator



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

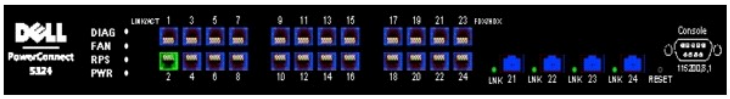
Табл. 5-1. Компоненты интерфейса

Компонент	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 прокрутки вправо.
2	На панели устройства приведены сведения о портах устройства, текущей настройке и состоянии устройства, табличная информация и компоненты параметров. В зависимости от выбранного параметра, в нижней области панели устройства отображается прочая информация об устройстве и диалоговые окна для настройки параметров.
3	В списке компонентов приведен список компонентов параметров. Компоненты также можно просмотреть, раскрыв параметр на панели дерева.
4	Информационные кнопки предоставляют доступ к сведениям об устройстве, а также доступ на веб-узел поддержки Dell. Дополнительную информацию см. в разделе Информационные кнопки.

Представление устройства

Домашняя страница PowerConnect содержит рисунок передней панели устройства.

Рис. 5-2. Индикаторы портов



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

Таблица 5-2. Индикаторы

Компонент	Название
Индикаторы портов	
Зеленый	Порт включен.
Красный	Произошла ошибка порта.
Синий	Порт отключен.

ПРИМЕЧАНИЕ. На странице программы PowerConnect OpenManage Switch Administrator не отображаются индикаторы портов, имеющиеся на передней панели коммутатора PowerConnect. Состояние индикаторов можно выяснить, только посмотрев на реальное устройство. Более подробную информацию об индикаторах см. в разделе Описания индикаторов.

Использование кнопок программы Switch Administrator

В этом разделе описаны кнопки, которые находятся в интерфейсе OpenManage Switch Administrator.

Информационные кнопки

Информационные кнопки предоставляют доступ к интерактивной поддержке и интерактивной справку, а также к информации об интерфейсах OpenManage Switch Administrator.

Таблица 5-3. 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 устройством. Страницы интерактивной справки напрямую связаны со страницами открытыми в настоящий момент. 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

Кнопки управления устройством обеспечивают простой способ настройки сведений об устройстве. К ним относятся следующие кнопки:

Таблица 5-4. Кнопки управления устройством

Кнопка	Описание
Apply Changes (Применить изменения)	Применяет заданные изменения для устройства.
Add (Добавить)	Добавляет информацию в таблицы или диалоговые окна.
Telnet	Запускает сеанс Telnet.
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 Neighbors 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.

Запуск приложения

1. Откройте веб-браузер.
2. Введите в строке адреса IP-адрес устройства (как определено в консоли) и нажмите клавишу <Enter>.

   Для получения сведений о назначении IP-адреса для устройства см. раздел «Статический IP-адрес и маска подсети».
3. Когда появится окно **Enter Network Password** (Ввод сетевого пароля), введите имя пользователя и пароль.

   ПРИМЕЧАНИЕ. Для коммутатора не настроен пароль по умолчанию, поэтому можно настроить коммутатор без ввода пароля. 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 **OK**.

   Откроется домашняя страница **Dell PowerConnect OpenManage™ Switch Administrator**.

Доступ к устройству с помощью команд консоли

Устройством можно управлять через прямое соединение с портом консоли или через соединение Telnet. 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.

Более подробную информацию о настройке начального IP-адреса см. в разделе «Статический IP-адрес и маска подсети».

ПРИМЕЧАНИЕ. Перед использованием консоли убедитесь, что клиент загружен.

Подключение консоли

1. Включите питание устройства и дождитесь завершения запуска.
2. Когда появится приглашение консоли Console>, введите команду enable и нажмите <Enter>.
3. Настройте устройство и введите необходимые команды для выполнения нужных задач.
4. 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.

Устройство поддерживает одновременно до четырех сеансов Telnet. Во время сеанса Telnet можно использовать все команды консоли.

Чтобы запустить сеанс Telnet:

1. Щелкните **Пуск > Выполнить**.

   Открывает диалоговое окно **Запуск программы**.
2. В окне **Запуск** программы введите Telnet <*IP-адрес*> в поле **Открыть**.

3. Нажмите кнопку **OK**, чтобы начать сеанс Telnet.

Использование консоли

В этом разделе содержится информация по использованию режима командной строки.

Обзор режима командной строки

Режим командной строки подразделяется на несколько командных режимов. Каждый из них имеет свой собственный набор команд. 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 в формате *****. 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 (config) и символ решетки #.

```
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.

Режим VLAN Database

Режим VLAN содержит команды для создания и настройки сети VLAN в целом, например для создания сети VLAN и применения IP-адреса к сети VLAN. Далее приведен пример приглашения режима VLAN:

```
Console # vlan database

Console (config-vlan)#
```

Режим Port Channel

Режим Port Channel содержит команды для настройки групп LAG (Link Aggregation Groups). Далее приведен пример приглашения режима Port Channel:

```
Console (config)# interface port-channel 1

Console (config-if)#
```

Режим Interface

Режим Interface содержит команды, которые используются для настройки интерфейса. В режиме Global Configuration, команда interface ethernet используется для перехода в режим настройки интерфейса. Далее приведен пример приглашения режима Interface:

```
console> enable

console# configure

console(config)# interface ethernet g18

console(config-if)#
```

Режим Management Access List

Режим Management Access List содержит команды для управления списками доступа. В режиме Global Configuration, команда management access-list используется для перехода в режим настройки списков управления доступом.

В следующем примере показан способ создания списка доступа «mlist», настройки двух интерфейсов управления (ethernet g1 и ethernet g9), а также активации списка доступа:

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

Console (config-macl)# permit ethernet g1

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

```
Console (config-macl)# exit

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

Открытый ключ SSH

Режим открытого ключа SSH содержит команду для ручного указания открытых ключей SSH других устройств.

В режиме Global Configuration команда `crypto key pubkey-chain ssh` используется для входа в режим настройки по цепочке открытого ключа SSH.

В следующем примере показан вход в режим настройки по цепочке открытого ключа SSH:

```
Console(config)# crypto key pubkey-chain ssh

Console(config-pubkey-chain)#
```

Примеры команд консоли

Команды консоли предоставляются как примеры настройки. Для получения полного описания команд консоли с примерами см. «Справочник по командам консоли» на компакт-диске с документацией.

Назад на страницу содержания

Назад на страницу Содержание

Просмотр статистики

Руководство пользователя систем Dell™ PowerConnect™ 54xx

На страницах **Statistic** (Статистика) приведены ссылки на информацию для интерфейса, GVRP, Etherlike, RMON и использования устройства. Команды CLI доступны не для всех страниц статистики.

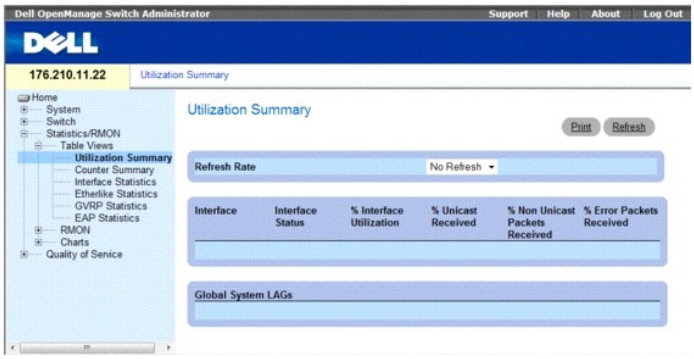
Просмотр таблиц

Страница **Table Views** (Просмотр в виде таблиц) содержит ссылки для отображения статистики в графическом виде. Чтобы открыть страницу, щелкните **Statistics** (Статистика)→ **Table** (Таблица) на панели дерева.

Просмотр общих сведений по использованию

Страница **Utilization Summary** (Общие сведения по использованию) содержит статистику по использованию интерфейса. Чтобы открыть страницу, щелкните **Statistics** (Статистика)→ **Table Views** (Просмотр в виде таблиц)→ **Utilization Summary** (Общие сведения по использованию) на панели дерева.

Рис. 8-1. Utilization Summary (Общие сведения по использованию)

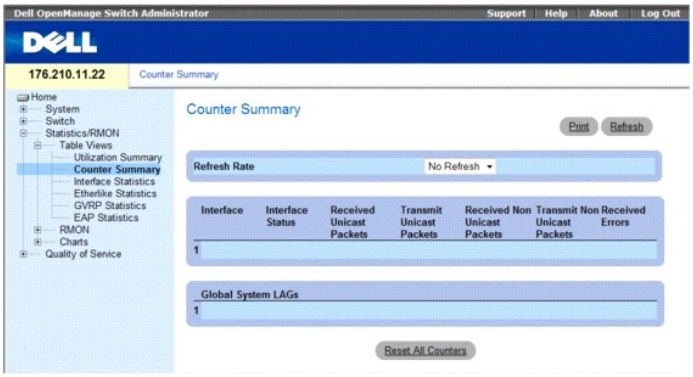


- **Refresh Rate** (Частота обновления). Период времени между обновлениями статистики интерфейса.
- **Interface** (Интерфейс). Номер интерфейса.
- **Interface Status** (Состояние интерфейса). Состояние интерфейса.
- **% Interface Utilization** (% использования интерфейса). Процент использования сетевого 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.
- **Global System LAG** (Общее состояние системы LAG). Текущая производительность группы LAG/trunk.

Просмотр сводки по счетчикам

Страница **Counter Summary** (Сводка по счетчикам) содержит статистику по использованию порта в числовых суммах, а не в процентах. Чтобы открыть страницу **Counter Summary** (Сводка по счетчикам) нажмите **Statistics/RMON** (Статистика/RMON)→ **Table Views** (Просмотр в виде таблиц)→ **Counter Summary** (Сводка по счетчикам) на панели дерева.

Рис. 8-2. Counter Summary (Сводка по счетчикам)

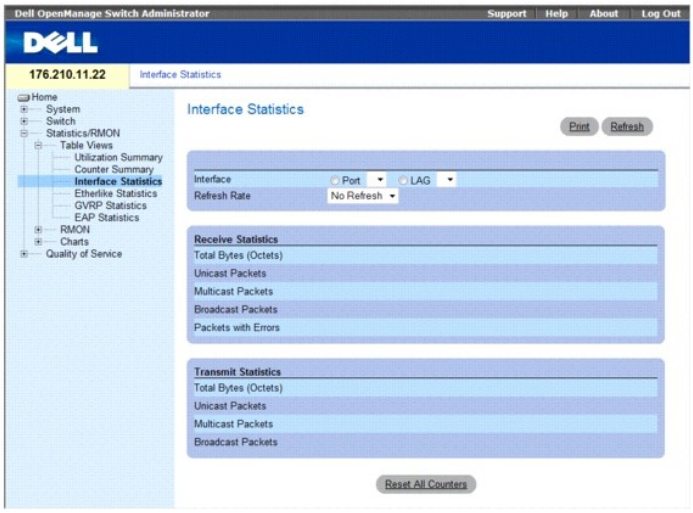


- **Refresh Rate** (Частота обновления). Период времени между обновлениями статистики интерфейса.
- **Interface** (Интерфейс). Номер интерфейса.
- **Interface Status** (Состояние интерфейса). Состояние интерфейса.
- **Received Unicast Packets** (Получено одноадресных пакетов). Число полученных на интерфейс одноадресных пакетов.
- **Received Non Unicast Packets** (Получено многоадресных пакетов). Число полученных на интерфейс многоадресных пакетов.
- **Transmit Unicast Packets** (Передано одноадресных пакетов). Число переданных одноадресных пакетов из интерфейса.
- **Transmit Non Unicast Packets** (Передано многоадресных пакетов). Число переданных многоадресных пакетов из интерфейса.
- **Received Errors** (Получено пакетов с ошибками). Число пакетов с ошибками, полученных на интерфейс.
- **Global System LAG** (Общее состояние системы LAG). Текущая производительность группы LAG/trunk.

Просмотр статистики интерфейса

Страница **Interface Statistics** (Статистика интерфейса) содержит статистику по принятым и переданным пакетам. Поля для полученных и переданных пакетов идентичны. Чтобы открыть страницу **Interface Statistics** (Статистика интерфейса), щелкните **Statistics/RMON** (Статистика/RMON)→ **Table Views** (Просмотр в виде таблиц)→ **Interface Statistics** (Статистика интерфейса) на панели дерева.

Рис. 8-3. Interface Statistics (Статистика интерфейса)



- **Interface** (Интерфейс). Указывает, отображается статистика для порта или LAG.
- **Refresh Rate** (Частота обновления). Период времени между обновлениями статистики интерфейса.

Статистика приема

- **Total Bytes (Octets)** (Всего байт (октетов)). Число октетов, принятых на выбранный интерфейс.
- **Unicast Packets** (Одноадресные пакеты). Число одноадресных пакетов, полученных на выбранный интерфейс.

- **Multicast Packets** (Многоадресные пакеты). Число многоадресных пакетов, полученных на выбранный интерфейс.
- **Broadcast Packets** (Пакеты широковещательной рассылки). Число пакетов широковещательной рассылки, полученных на выбранный интерфейс.
- **Packets with Errors** (Получено пакетов с ошибками). Число пакетов с ошибками, полученных на интерфейс.

Статистика передачи

- **Total Bytes (Octets)** (Всего байт (октетов)). Число октетов, переданных 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 пакетов с ошибками, переданных с выбранного интерфейса.

Отображение статистики интерфейса

1. Откройте страницу **Interface Statistics** (Статистика интерфейса).
2. Выберите интерфейс в поле **Interface** (Интерфейс).

   Отобразится статистика интерфейса.

Сброс счетчиков статистики интерфейса

1. Откройте страницу **Interface Statistics** (Статистика интерфейса).
2. Щелкните **Reset All Counters** (Сбросить все счетчики).

   Произойдет сброс счетчиков статистики интерфейса

Просмотр статистики интерфейса с помощью команд консоли

В следующей таблице приведены команды консоли для просмотра статистики интерфейса.

Таблица 8-1. Команды консоли для статистики интерфейса

Команда консоли	**Описание**
show interfaces counters [**ethernet** *интерфейс* | **port-channel** *номер_канала_порта*]	Отображает трафик, видимый физическим интерфейсом.

Далее приведен пример команд консоли.

```
Console> enable


Console# show interfaces counters

Port    InOctets    InUcastPkts    InMcastPkts    InBcastPkts
------- ----------- -------------- -------------- -----------
g1      183892      1289           987            8
g2      0           0              0              0
g3      123899      1788           373            19

Port    OutOctets   OutUcastPkts   OutMcastPkts   OutBcastPkts
------- ----------- -------------- -------------- -----------
g4      9188        9              8              0
g5      0           0              0              0
```

g6	8789	27	8	0
Ch	InOctets	InUcastPkts	InMcastPkts	InBcastPkts
-------	------------	----------------	----------------	------------
1	27889	928	0	78
Ch	OutOctets	OutUcastPkts	OutMcastPkts	OutBcastPkts
-------	------------	----------------	----------------	------------
1	23739	882	0	122

Просмотр статистики Etherlike

Страница **Etherlike Statistics** (Статистика Etherlike) содержит статистику интерфейса. Чтобы открыть страницу **Etherlike Statistics** (Статистика интерфейса), щелкните **Statistics/RMON** (Статистика/RMON)→ **Table Views** (Просмотр в виде таблиц)→ **Etherlike Statistics** (Статистика интерфейса) на панели дерева.

Рис. 8-4. Etherlike Statistics (Статистика Etherlike)

- **Interface** (Интерфейс). Указывает, отображается статистика для порта или LAG.
- **Refresh Rate** (Частота обновления). Период времени между обновлениями статистики интерфейса.
- **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.
- **Late Collisions** (Последние коллизии). Число последних коллизий, полученных на выбранный интерфейс.
- **Excessive Collisions** (Чрезмерные коллизии). Число чрезмерных коллизий, полученных на выбранный интерфейс.
- **Oversize Packets** (Превышение размера пакетов). Число ошибок слишком больших 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 приостановленных кадров, переданных с выбранного интерфейса.

Отображение статистики Etherlike для интерфейса

1. Откройте страницу **Etherlike Statistics** (Статистика Etherlike).
2. Выберите интерфейс в поле **Interface** (Интерфейс).

   Отобразится статистика Etherlike интерфейса.

Сброс статистики Etherlike

1. Откройте страницу **Etherlike Statistics** (Статистика Etherlike).
2. Щелкните **Reset All Counters** (Сбросить все счетчики).

   Статистика Ethernetlike будет сброшена.

Просмотр статистики Etherlike с помощью команд консоли

В следующей таблице приведены команды консоли для просмотра статистики интерфейса etherlike.

Таблица 8-2. Команды консоли статистики Etherlike

Команда консоли	**Описание**
show interfaces counters [ethernet интерфейс | **port-channel** *номер_канала_порта*]	Отображает трафик, видимый физическим интерфейсом.

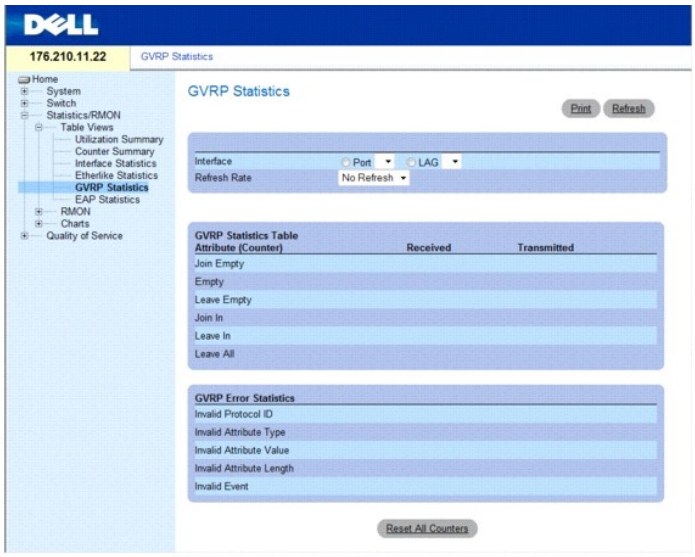
Далее приведен пример команд консоли.

```
Console> enable

Console# show interfaces counters ethernet g1

Port    InOctets    InUcastPkts    InMcastPkts    InBcastPkts
------- ----------- -------------- -------------- -----------
g1      183892      1289           987            8

Port    OutOctets   OutUcastPkts   OutMcastPkts   OutBcastPkts
------- ----------- -------------- -------------- -----------
g1      9188        9              8              0

FCS Errors: 8

Single Collision Frames: 0

Multiple Collision Frames: 0

SQE Test Errors: 0

Deferred Transmissions: 0

Late Collisions: 0

Excessive Collisions: 0

Internal MAC Tx Errors: 0

Carrier Sense Errors: 0

Oversize Packets: 0

Internal MAC Rx Errors: 0

Received Pause Frames: 0

Transmitted Pause Frames: 0
```

Просмотр статистики протокола GVRP

На странице **GVRP Statistics** (Статистика GVRP) показана статистика для протокола GVRP. Чтобы открыть эту страницу, щелкните **Statistics/RMON** (Статистика/RMON)→ **Table Views** (Просмотр в виде таблиц)→ **GVRP Statistics** (Статистика интерфейса) на панели дерева.

Рис. 8-5. GVRP Statistics (Статистика GVRP)



- **Interface** (Интерфейс). Указывает, отображается статистика для порта или LAG.
- **Refresh Rate** (Частота обновления). Период времени между обновлениями статистики интерфейса.
- **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 Events** (Недопустимые события). Статистика Invalid Events протокола GVRP для устройства.

Отображение статистики GVRP для порта

1. Откройте страницу **GVRP Statistics** (Статистика GVRP).
2. Выберите интерфейс в поле **Interface** (Интерфейс).

   Отобразится статистика GVRP интерфейса.

Сброс статистики GVRP

1. Откройте страницу **GVRP Statistics** (Статистика GVRP).
2. Щелкните **Reset All Counters** (Сбросить все счетчики).

   Счетчики GVRP будут сброшены.

Просмотр статистики протокола GVRP с помощью команд консоли

В следующей таблице приведены команды консоли для просмотра статистики интерфейса GVRP.

Таблица 8-3. Команды консоли для просмотра статистики GVRP

Команда консоли	Описание
show gvrp statistics [**ethernet** *интерфейс* | **port-channel** *порт-канал-номер*]	Отображает статистику протокола GVRP.
show gvrp error-statistics [**ethernet** *интерфейс* | **port-channel** *порт-канал-номер*]	Отображает статистику ошибок протокола GVRP.

Далее приведен пример команд консоли.

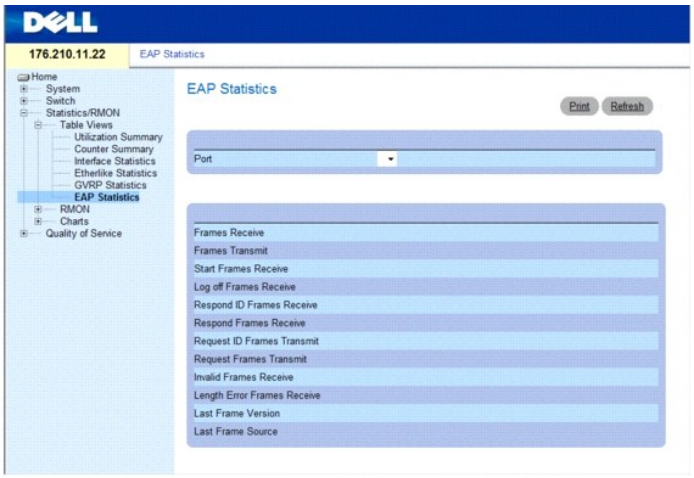
```
Console# show gvrp statistics

GVRP statistics:
----------------
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# 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  INVALEN  INVEVENT
----  -------  -------  -------  -------  --------
g1    0        0        0        0        0
g2    0        0        0        0        0
g3    0        0        0        0        0
g4    0        0        0        0        0
g5    0        0        0        0        0
g6    0        0        0        0        0
g7    0        0        0        0        0
g8    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. 8-6. Страница EAP Statistics (Статистика EAP)



- **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 Log off). Число кадров Log off по протоколу EAPOL, полученных для порта.
- **Respond ID Frames Receive** (Получено кадров с идентификаторами ответа). Число кадров Resp/Id по протоколу EAP, полученных на порте.
- **Respond Frames Receive** (Получено кадров ответа). Число верных кадров Response 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** (Поучено неверных 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.

Сброс статистики EAP

1. Откройте страницу **EAP Statistics** (Статистика EAP).
2. Щелкните **Reset All Counters** (Сбросить все счетчики) для сброса счетчика.

   Статистика EAP будет сброшена.

Просмотр статистики протокола EAP с помощью команд консоли

В следующей таблице приведены команды консоли для просмотра статистики интерфейса EAP.

Таблица 8-4. Команды консоли для просмотра статистики GVRP

Команда консоли	Описание
show dot1x statistics ethernet *интерфейс*	Отображает статистику 802.1X для указанного интерфейса.

Далее приведен пример команд консоли.

```
Switch# show dot1x statistics ethernet g1

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
```

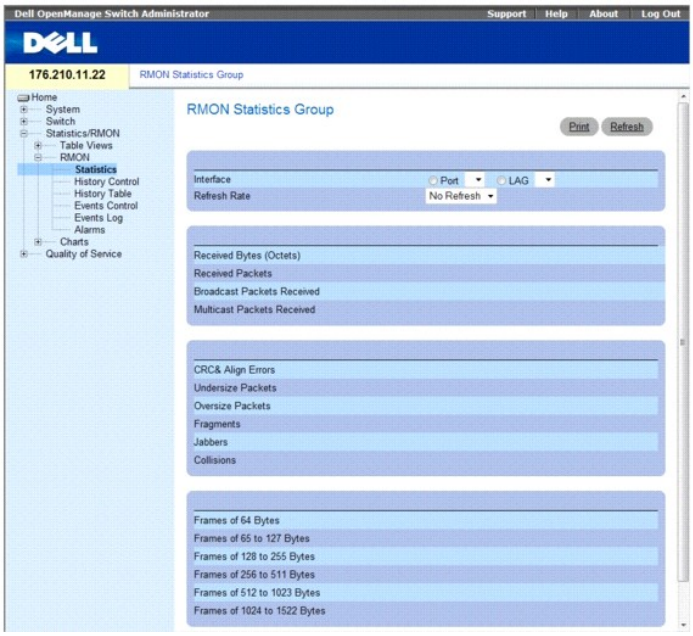
Просмотр статистики удаленного мониторинга RMON

Страница удаленного мониторинга (RMON) содержит ссылки для удаленного доступа к информации по сети. Чтобы открыть страницу **RMON**, щелкните **Statistics / RMON** (Статистика/RMON)→ **RMON** на панели дерева.

Просмотр группы статистики RMON

Страница **RMON Statistics Group** (Группа статистика RMON) содержит поля для просмотра информации по использованию устройства и возникающие на нем ошибки. Чтобы открыть страницу **RMON Statistics Group** (Статистика RMON), щелкните **Statistics / RMON** (Статистика/RMON)→ **RMON**→ **Statistics** (Статистика) на панели дерева.

Рис. 8-7. 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.
- **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 сбойных пакетов (пакеты длиннее 1518 октетов), полученных на интерфейс с момента последнего обновления устройства.
- **Collisions** (Коллизии). Число коллизий, полученных на интерфейс с момента последнего обновления устройства.
- **Frames of *xx* Bytes** (Кадры из xx байт). Число *xx*-байтовых кадров, полученных на интерфейс с момента последнего обновления устройства.

Просмотр статистики интерфейса

1. Откройте страницу **RMON Statistics Group** (Группа статистики RMON).
2. Выберите тип и номер интерфейса в поле **Interface** (Интерфейс).

   Отобразится статистика интерфейса.

Просмотр статистики удаленного мониторинга с помощью команд консоли

В следующей таблице приведены команды консоли для просмотра статистики интерфейса RMON.

Таблица 8-5. Команды консоли для просмотра статистики удаленного мониторинга

Команда консоли	Описание
show rmon statistics {**ethernet** *интерфейс* | **port-channel** *номер_канала_порта*}	Отображает статистику удаленного мониторинга по Ethernet.

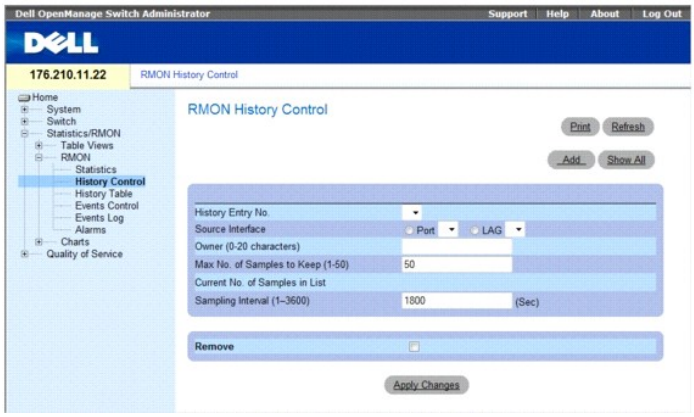
Далее приведен пример команд консоли.

```
console> enable

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 **RMON History Control** (Статистика RMON), щелкните **Statistics / RMON** (Статистика/RMON)→ **History Control** (Управление журналом) на панели дерева.

Рис. 8-8. RMON History Control (Управление журналом удаленного мониторинга)



- **History Entry No.** (Номер записи журнала). Номер записи для страницы **History Control Table** (Таблица управления журналом).
- **Source Interface** (Интерфейс-источник). Порт или LAG, из которых были получены выборки журнала.
- **Owner (0-20 characters)** (Владелец (0-20 символов)). Станция удаленного мониторинга или пользователя, запросившего информацию по удаленному доступу.
- **Max No. of Samples to Keep (1-50)** (Максимальное число выборок для хранения) (1-50). Число сохраняемых выборок. Значение по умолчанию - 50.
- **Current No. of Samples in List** (Текущее число выборок). Текущее количество полученных выборок.
- **Sampling Interval (1-3600)** (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** (Таблица управления журналом).

Добавление записи управления журналом

1. Откройте страницу **RMON History Control** (Управление журналом удаленного мониторинга).
2. Нажмите кнопку **Add** (Добавить).

   Откроется страница **Add History Entry** (Добавление записи журнала).
3. Введите значения в полях диалогового окна.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Запись добавится в **History Control Table** (Таблицу управления журналом).

Изменение записи таблицы управления журналом

1. Откройте страницу **RMON History Control** (Управление журналом удаленного мониторинга).
2. Выберите запись в поле **History Entry No.** (Номер записи журнала).
3. Выполните необходимые изменения полей.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Запись таблицы изменяется, а устройство обновляется.

Удаление записи таблицы управления журналом

1. Откройте страницу **RMON History Control** (Управление журналом удаленного мониторинга).
2. Выберите запись в поле **History Entry No.** (Номер записи журнала).
3. Щелкните **Remove** (Удалить).
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Выбранная 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 интерфейса GVRP.

Таблица 8-6. Команды консоли журнала удаленного мониторинга

Команда консоли	**Описание**
rmon collection history *индекс* [**owner** *имя владельца* | **buckets** *номер_блока*] [**interval** *секунды*]	Включает и настраивает удаленный мониторинг на интерфейсе.
show rmon collection history [**ethernet** *интерфейс* | **port-channel** *номер_канала_порта*]	Отображает статистику журнал совокупности удаленного мониторинга.

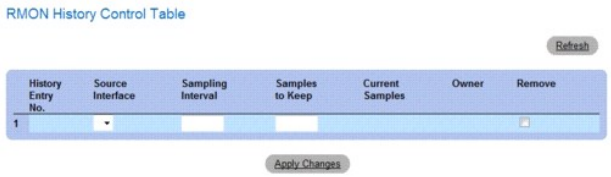
Далее приведен пример команд консоли.

```
Console (config)# interface ethernet g8

Console (config-if)# rmon collection history 1 interval 2400

Console (config-if)# exit

Console (config)# exit
```

Просмотр журнала удаленного мониторинга

Страница **RMON History Table** (Журнал удаленного мониторинга) содержит статистические сетевые выборки для конкретного интерфейса. Каждая запись таблицы представляет собой все значения счетчиков, скомпилированные в течение однократной выборки. Чтобы открыть страницу **RMON History Table** (Журнал удаленного мониторинга), щелкните **Statistics/RMON** (Статистика/RMON)→ **RMON**→ **History Table** (Управление журналом) на панели дерева.

Рис. 8-9. RMON History Table (Таблица журнала удаленного мониторинга)



- **Sample No.** (Номер выборки). Определенная выборка, 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 правильных многоадресных пакетов, полученных во время интервала выборки.
- **CRC Align Errors** (Ошибки выравнивания CRC). Число пакетов, полученных во время сеанса выборки с длинной в 64-1518 октетов, неверная последовательность проверки (FCS) с целым числом октетов или неверная FCS с нецелым числом.
- **Undersize Packets** (Пакеты с размером меньше допустимого). Число пакетов, полученных во время сеанса выборки, с длиной меньше 64 октетов.
- **Oversize Packets** (Пакеты с размером меньше допустимого). число пакетов, полученных во время сеанса выборки, с длиной больше 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 обнаруживают 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 журнала в поле **History Table No.** (Номер записи журнала).

   Статистика для записи будет отображена в таблице RMON History (Журнал удаленного мониторинга).

Просмотр управления журналом удаленного мониторинга с помощью команд консоли

В следующей таблице приведены команды консоли для просмотра журнала удаленного мониторинга.

Таблица 8-7. Команды консоли для управления журналом удаленного мониторинга

Команда консоли	**Описание**
show rmon history *индекс* {**throughput	errors	other**} [**period** *сек*]	Отображает журнал статистики удаленного мониторинга Ethernet.

Далее приведен пример команд консоли для отображения статистики удаленного мониторинга Ethernet для пропускной способности по индексу 1:

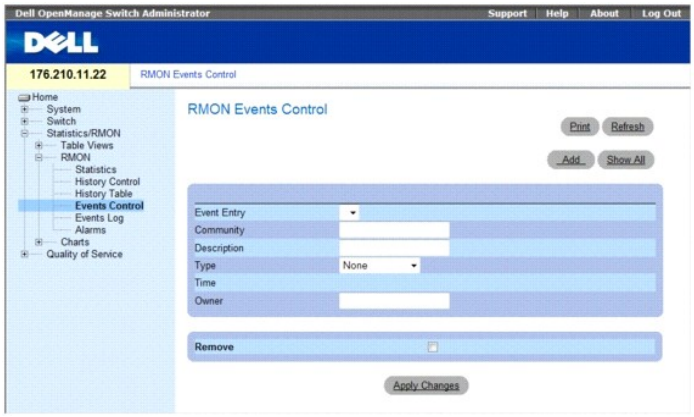
```
console> enable

Console# show rmon history 1 throughput
```

Sample Set: 1		Owner: CLI			
Interface: g1		Interval: 1800			
Requested samples: 50		Granted samples: 50			
Maximum table size: 500					
Time	Octets	Packets	Broadcast	Multicast	%
----------	----------	----------	----------	----------	----------
Jan 18 2004 21:57:00	303595962	357568	3289	7287	19.98%
Jan 18 2004 21:57:30	287696304	275686	2789	2789	20.17%

Определение событий удаленного мониторинга устройства

Страница **RMON Events Control** (Управление событиями удаленного мониторинга) содержит поля для определения событий удаленного мониторинга. Чтобы открыть страницу **RMON Events Control** (Управление событиями удаленного мониторинга) щелкните **Statistics / RMON** (Статистика/RMON)→ **RMON**→ **Events Control** (Управление событиями) на панели дерева.

Рис. 8-10. RMON Events Control (Управление событиями удаленного мониторинга)



- **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 (например, 29 марта 2004 года в 11:00 отображается в следующем формате 29/03/2004 11:00:00).
- **Owner** (Владелец). Устройство или пользователь, который определил событие.
- **Remove** (Удалить). Когда этот флажок установлен, событие удаляется из **таблицы журнала удаленного мониторинга**.

Добавление события удаленного мониторинга

1. Откройте страницу **RMON Events Control** (Управление событиями удаленного мониторинга).
2. Нажмите кнопку **Add** (Добавить).

   Откроется страница **Add an Event Entry** (Добавление записи журнала).
3. Введите данные в диалоговом окне и нажмите кнопку **Apply Changes** (Применить изменения).

   Запись таблицы **Event Table** (Таблица событий) будет добавлена, а устройство обновлено.

Изменение события удаленного мониторинга

1. Откройте страницу **RMON Events Control** (Управление событиями удаленного мониторинга)
2. Выберите запись в таблице **Event Table** (Таблица событий).
3. Измените значения в полях диалогового окна и нажмите кнопку **Apply Changes** (Применить изменения).

   Запись таблицы **Event Table** (Таблица событий) будет изменена, а устройство обновлено.

Удаление записей о событиях удаленного мониторинга

1. Откройте страницу **RMON Events Control** (Управление событиями удаленного мониторинга).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **Events Table** (Таблица событий).
3. Установите флажок **Remove** (Удалить) для каждого события, которое необходимо удалить, а затем нажмите кнопку **Apply Changes** (Применить изменения).

   Выбранная 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 эквивалентные команды консоли для определения событий устройства.

Таблица 8-8. Команды консоли для определения событий устройств

Команда консоли	Описание
rmon event *тип индекса* [**community** *текст сообщества*] [**description** *текст описания*] [**owner** *имя владельца*]	Настраивает события удаленного мониторинга.
show rmon events	Отображает таблицу событий удаленного мониторинга.

Далее приведен пример команд консоли.

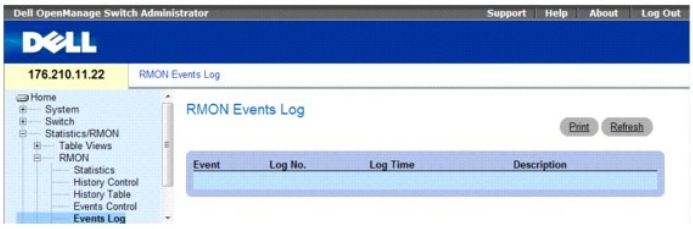
```
console> enable

console# config

console (config)# rmon event 1 log

console (config)# exit

Console# show rmon events
```

Index	Description	Type	Community	Owner	Last time sent
-----	----------	--------	---------	-------	-------------------
1	Errors	Log		CLI	Jan 18 2002 23:58:17
2	High Broadcast	Log-Trap	router	Manager	Jan 18 2002 23:59:48

Просмотр журнала событий удаленного мониторинга

На странице **RMON Events Log** (Журнал событий удаленного мониторинга) содержится список событий удаленного мониторинга. Чтобы открыть страницу **RMON Events Log** (Журнал событий удаленного мониторинга), щелкните **Statistics / RMON** (Статистика/RMON)→ **RMON**→ **Events** (События) на панели дерева.

Рис. 8-11. 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 эквивалентные команды консоли для определения событий устройства.

Таблица 8-9. Команды консоли для определения событий устройств

Команда консоли	**Описание**
show rmon log [*событие*]	Отображает таблицу журнала событий удаленного мониторинга.

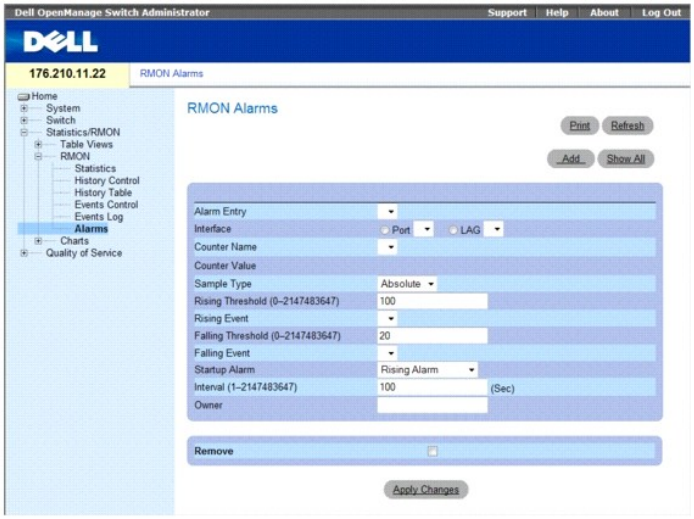
Далее приведен пример команд консоли.

```
console> enable

console# config

console (config)# rmon event 1 log

console (config)# exit

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

Console# show rmon log

Maximum table size: 500 (800 after reset)

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

Страница **RMON Alarms** (Сигналы удаленного мониторинга) содержит поля для настройки сетевых сигналов. Сетевая тревога происходит при обнаружении проблемы или события в сети. При повышении или понижении пороговых величин генерируются события. Чтобы открыть страницу **RMON Alarms** (Сигналы удаленного мониторинга), щелкните **Statistics / RMON** (Статистика/RMON)→ **RMON**→ **Alarms** (Сигналы) на панели дерева.

Рис. 8-12. RMON Alarms (Сигналы удаленного мониторинга)



- **Alarm Entry** (Запись сигнала). Показывает определенный сигнал.
- **Interface** (Интерфейс). указывает порт, для которого отображается статистика удаленного мониторинга.
- **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 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 нижней 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).

   Откроется страница **Add an Alarm Entry** (Добавление записи журнала):

Рис. 8-13. Страница Add an Alarm Entry (Добавление записи журнала)

3. Выберите интерфейс.
4. Введите значения в полях диалогового окна.
5. Нажмите кнопку **Apply Changes** (Применить изменения).

   Сигнал удаленного мониторинга будет добавлен, а устройство обновлено.

Изменение записи в таблице сигналов

1. Откройте страницу **RMON Alarms** (Сигналы удаленного мониторинга).
2. Выберите запись в раскрывающемся меню **Alarm Entry** (Запись сигнала).
3. Выполните необходимые изменения значений в полях диалогового окна.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Запись будет изменена, а устройство обновлено.

Отображение таблицы сигналов

1. Откройте страницу **RMON Alarms** (Сигналы удаленного мониторинга).
2. Нажмите кнопку **Show All** (Показать все).

   Откроется страница **Alarms Table** (Таблица сигналов).

Удаление записи в таблице сигналов

1. Откройте страницу **RMON Alarms** (Сигналы удаленного мониторинга).
2. Выберите запись в раскрывающемся меню **Alarm Entry** (Запись сигнала).
3. Установите флажок **Remove** (Удалить).
4. Нажмите кнопку **Apply Changes** (Применить изменения).

   Выбранная запись будет удалена, а устройство обновлено.

Определение сигналов устройств с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для определения сигналов устройства.

Таблица 8-10. Команды консоли для сигналов устройств

Команда консоли	Описание

rmon alarm *индекс переменная интервал порог_верх порог_нижн верх_событие нижн_событие* [**type** *тип*] [**startup** *направление*] [**owner** *имя*]	Настраивает условия выдачи сигналов удаленного мониторинга.
show rmon alarm-table	Отображает сводную таблицу сигналов.
show rmon alarm	Отображает конфигурацию сигналов удаленного мониторинга.

Далее приведен пример команд консоли.

```
console> enable

console# config

Console (config)# rmon alarm 1000 dell 360000 1000000 1000000 10 20

Console# show rmon alarm-table
```

Index	OID	Owner
------	-------------------	-------------
1	1.3.6.1.2.1.2.2.1.10.1	CLI
2	1.3.6.1.2.1.2.2.1.10.1	Manager
3	1.3.6.1.2.1.2.2.1.10.9	CLI

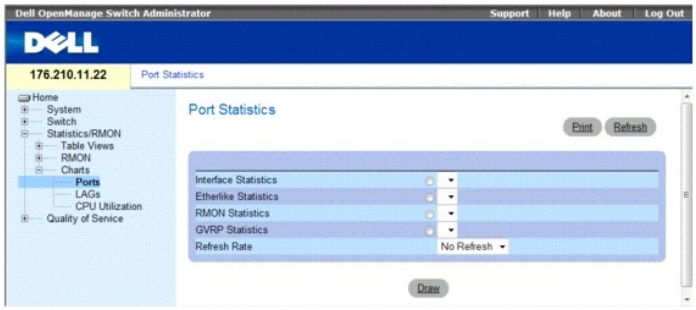
Просмотр диаграмм

На странице **Chart** (Диаграммы) содержатся ссылки для отображения статистики в виде диаграммы. Чтобы открыть страницу, щелкните **Statistics** (Статистика)→ **Charts** (Диаграммы) на панели дерева.

Просмотр статистики портов

Страница **Port Statistics** (Статистика портов) содержит поля для статистики открытия в виде диаграммы для элементов портов. Чтобы открыть страницу **Port Statistics** (Статистика портов), щелкните **Statistics** (Статистика)→ **Charts** (Диаграммы)→ **Ports** (Порты) на панели дерева.

Рис. 8-14. Port Statistics (Статистика портов)



- **Interface Statistics** (Статистика интерфейса). Выбор типа статистики интерфейса для открытия.
- **Etherlike Statistics** (Статистика Etherlike). Выбор типа статистики Etherlike для открытия.
- **RMON Statistics** (Статистика удаленного мониторинга). Выбор типа статистики удаленного мониторинга для отображения.
- **GVRP Statistics** (Статистика протокола GVRP). Выбор типа статистики GVRP для открытия.
- **Refresh Rate** (Частота обновления). Период времени между обновлениями статистики интерфейса.

Отображение статистики для порта

1. Откройте страницу **Port Statistics** (Статистика порта).
2. Выберите тип статистики для открытия.
3. Выберите необходимую частоту обновления в раскрывающемся меню **Refresh Rate** (Частота обновления).

4. Нажмите кнопку **Draw** (Нарисовать).

   Отобразится график для выбранной статистики.

Просмотр статистики порта с помощью команд консоли

В следующей таблице приведены команды консоли для просмотра статистики порта.

Таблица 8-11. 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.

Console# **show interfaces description ethernet g1**	
Port	Description
----	------------------
g1	Management_port
g2	R&D_port
g3	Finance_port
Ch	Description
----	------------------
1	Output

Просмотр статистики группы LAG

Страница **LAG Statistics** (Статистика LAG). Содержит поля для статистики открытия в виде диаграммы для LAG. Чтобы открыть страницу **LAG Statistics** (Статистика LAG), щелкните **Statistics** (Статистика)→ **Charts** (Диаграммы)→ **LAGs** на панели дерева.

Рис. 8-15. LAG Statistics (Статистика LAG)

- **Interface Statistics** (Статистика интерфейса). Выбор типа статистики интерфейса для открытия.
- **Etherlike Statistics** (Статистика Etherlike). Выбор типа статистики Etherlike для открытия.
- **RMON Statistics** (Статистика удаленного мониторинга). Выбор типа статистики удаленного мониторинга для открытия.
- **GVRP Statistics** (Статистика GVRP). Выбор типа статистики GVRP для открытия.
- **Refresh Rate** (Частота обновления). Период времени между обновлениями статистики интерфейса.

Отображение статистики LAG

1. Откройте страницу **LAG Statistics** (Статистика LAG).
2. Выберите тип статистики для открытия.
3. Выберите необходимую частоту обновления в раскрывающемся меню **Refresh Rate** (Частота обновления).
4. Нажмите кнопку **Draw** (Нарисовать).

   Отобразится график для выбранной статистики.

Просмотр статистики LAG с помощью команд консоли

В следующей таблице приведены команды консоли для просмотра статистики LAG.

Таблица 8-12. Команды консоли для статистики LAG

Команда консоли	Описание
show interfaces counters [**ethernet** *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.

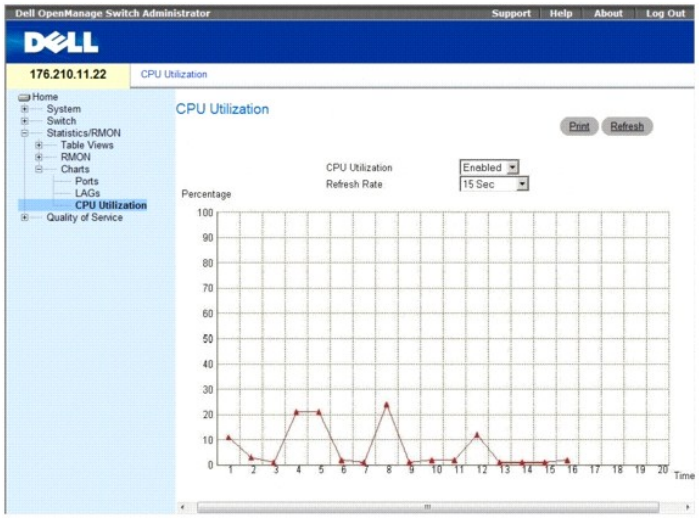
```
Console# show gvrp statistics

GVRP statistics:
----------------
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
```

Просмотр страницы использования ЦП

На странице **CPU Utilization** (Использование ЦП) содержится информация об использовании ЦП системы и ресурсах ЦП в процентах, используемых каждым компонентом стека. Каждому компоненту стека на графике соответствует какой-либо цвет.

Чтобы открыть страницу **CPU Utilization** (Использование ЦП), щелкните **Statistics / RMON** (Статистика/RMON)→ **Charts** (Диаграммы)→ **CPU Utilization** (Использование ЦП) на панели дерева.

Рис. 8-16. CPU Utilization (Использование ЦП)



На странице **CPU Utilization** (Использование ЦП) содержится следующая информация.

- **Refresh Rate** (Частота обновления). Период времени между обновлениями статистики интерфейса.

Просмотр страницы использования ЦП с помощью команд консоли

В следующей таблице приведены команды консоли для просмотра страницы использования ЦП.

Команда консоли	Описание
show cpu utilization	Отображает использование ЦП.

Далее приведен пример команд консоли.

```
Console# show cpu utilization

CPU utilization service is on.



CPU utilization

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

five seconds: 5%; one minute: 3%; five minutes: 3%
```

Назад на страницу Содержание