

Руководство пользователя системы Dell™ PowerConnect™ 5324

[Введение](#)

[Описание аппаратного обеспечения](#)

[Установка устройства PowerConnect](#)

[Запуск и настройка устройства](#)

[Использование Dell OpenManage Switch Administrator](#)

[Информация о настройке системы](#)

[Настройка сведений об устройстве](#)

[Просмотр статистики](#)

[Настройка качества обслуживания](#)

[Технические характеристики устройства](#)

[Глоссарий](#)

Примечания, уведомления и предупреждения



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



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



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

Информация, включенная в состав данного документа, может быть изменена без уведомления.

© 2003 - 2007 Dell Inc. Все права защищены.

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

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

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

Май 2007

Запуск и настройка устройства

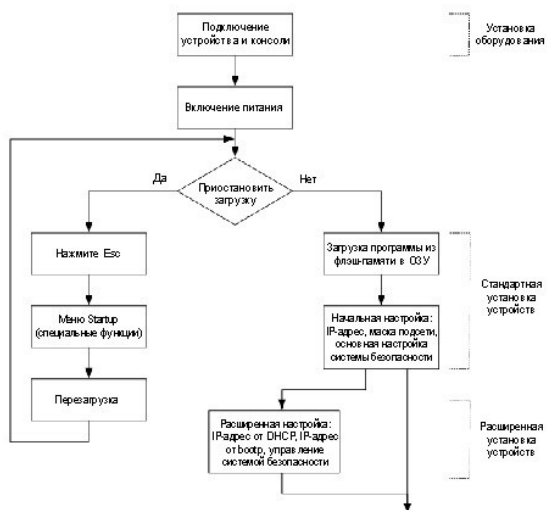
Руководство пользователя системы Dell™ PowerConnect™ 5324

- [Настройка терминала](#)
- [Загрузка устройства](#)
- [Обзор настройки](#)
- [Начальная настройка](#)
- [Имя пользователя](#)
- [Строки сообщества SNMP](#)
- [Расширенная настройка](#)
- [Получение IP-адреса от сервера DHCP](#)
- [Получение IP-адреса от сервера BOOTP](#)
- [Управление системой безопасности и настройка паролей](#)
- [Настройка паролей системы безопасности](#)
- [Процедуры запуска](#)

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. 4-12. 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 клавиш **Function** (Функциональные клавиши), **Arrow** (Клавиши со стрелками) и **Ctrl**. Убедитесь, что выбраны **Terminal keys**, а не **Windows keys**.

 **ЗАМЕЧАНИЕ.** 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

- n Устройство поставляется с настройками по умолчанию.
- n Имя пользователя и пароль по умолчанию 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-2004 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).

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. 1.0.0.15 Date 03-Mar-2004 Time 10:41:14 ***

HW version is 00.01.07

Base Mac address is: 00:00:07:77:77:77

Dram size is : 64M bytes

Dram first block size is : 40960K bytes

Dram first PTR is : 0x1800000

Flash size is: 16M

Device configuration:

Pretera based system

Slot 1 - Neyland24 HW Rev. 0.1

Tapi Version: v1.2.9

Core Version: v1.2.9

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

console> 01-Jan-2000 01:01:35 %LINK-W-Down: g1

01-Jan-2000 01:01:35 %LINK-W-Down: g2

01-Jan-2000 01:01:35 %LINK-W-Down: g3

01-Jan-2000 01:01:35 %LINK-W-Down: g4

01-Jan-2000 01:01:35 %LINK-W-Down: g5

01-Jan-2000 01:01:35 %LINK-W-Down: g6

01-Jan-2000 01:01:35 %LINK-W-Down: g7

01-Jan-2000 01:01:35 %LINK-W-Down: g8

01-Jan-2000 01:01:35 %LINK-W-Down: g9

01-Jan-2000 01:01:35 %LINK-W-Down: g10

01-Jan-2000 01:01:35 %LINK-W-Down: g11

01-Jan-2000 01:01:35 %LINK-W-Down: g12

01-Jan-2000 01:01:35 %LINK-W-Down: g13

01-Jan-2000 01:01:36 %LINK-W-Down: g14

01-Jan-2000 01:01:36 %LINK-W-Down: g15

01-Jan-2000 01:01:36 %LINK-W-Down: g16

01-Jan-2000 01:01:36 %LINK-W-Down: g17

01-Jan-2000 01:01:36 %LINK-W-Down: g18

01-Jan-2000 01:01:36 %LINK-W-Down: g19

01-Jan-2000 01:01:36 %LINK-W-Down: g20

01-Jan-2000 01:01:36 %LINK-W-Down: g21

01-Jan-2000 01:01:36 %LINK-W-Down: g22

01-Jan-2000 01:01:36 %LINK-I-Up: Vlan 3000

01-Jan-2000 01:01:36 %LINK-I-Up: Vlan 1

01-Jan-2000 01:01:36 %LINK-I-Up: g1

01-Jan-2000 01:01:36 %LINK-I-Up: g13

01-Jan-2000 01:01:36 %LINK-I-Up: g14

01-Jan-2000 01:01:36 %LINK-I-Up: g19

01-Jan-2000 01:01:36 %LINK-I-Up: g20

01-Jan-2000 01:01:36 %LINK-I-Up: g21

01-Jan-2000 01:01:36 %LINK-W-Down: g23

01-Jan-2000 01:01:36 %LINK-W-Down: g24

01-Jan-2000 01:01:36 %LINK-W-Down: chl

```
01-Jan-2000 01:01:36 %LINK-I-Up: Vlan 1000
```

```
01-Jan-2000 01:01:36 %TRUNK-I-PORTADDED: Port g24 added to chl
```

```
01-Jan-2000 01:01:36 %LINK-I-Up: g22
```

```
01-Jan-2000 01:01:36 %LINK-I-Up: g23
```

```
01-Jan-2000 01:01:36 %LINK-I-Up: g24
```

```
01-Jan-2000 01:01:36 %LINK-I-Up: chl
```

```
01-Jan-2000 01:01:36 %LINK-W-Down: g1
```

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

```
console>
```

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](#).

Обзор настройки

Перед назначением статического IP-адреса для устройства необходимо получить следующую информацию.

- 1 IP-адрес, назначенный сетевым администратором для настраиваемого коммутатора.
- 1 Маршрут по умолчанию.
- 1 Маска сети для сети.

Существует два типа настройки.

- 1 **Начальная настройка** - заключается в определении базовых функций конфигурации и основных настроек системы безопасности.
- 1 **Расширенная настройка** - выполняется настройка динамических IP-адресов и дополнительных параметров системы безопасности.




ПРИМЕЧАНИЕ. После внесения любых изменений в настройку необходимо сохранить новую настройку перед перезагрузкой устройства. Чтобы сохранить настройку, введите следующую команду:

```
console# copy running-config startup-config
```

Начальная настройка



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

 **ПРИМЕЧАНИЕ.** В начальной простой конфигурации используются следующие допущения:

- n Устройство PowerConnect ранее не настраивалось и находится том же состоянии, в котором оно было получено.
- n Устройство PowerConnect загружено успешно.
- n Установлено соединение консоли, а на экране устройства терминала VT100 отображается приглашение консоли (несколько раз нажмите клавишу <Enter>, чтобы проверить, что приглашение отображается правильно).
- n Имя пользователя и пароль по умолчанию не заданы.

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

Конфигурация по умолчанию включает следующее:

- 1 Задание имени пользователя «admin» и пароля «dell» с максимальным уровнем привилегий - 15.
- 1 Настройка статического IP-адреса и шлюза по умолчанию.
- 1 Настройка строки SNMP сообщества для чтения и записи.
- 1 Получение IP-адреса, назначаемого сервером DHCP.

Перед настройкой начальной конфигурации для устройства PowerConnect необходимо получить у сетевого администратора следующие данные:

- 1 IP-адрес, который необходимо назначить для VLAN, через который будет выполняться управление устройством.
- 1 IP-маска подсети для сети.
- 1 IP-адрес шлюза по умолчанию.
- 1 Сообщество SNMP.

Статический IP-адрес и маска подсети

IP-адрес можно настраивать через любой интерфейс, включая VLAN, LAG и физический порт. После ввода команды настройки рекомендуется проверить, был ли порт настроен с данным IP-адресом, введя команду `show ip interface` (показать IP-интерфейс).


Внимание! Если IP-адрес настраивается через LAG или физический порт (например, g10), этот интерфейс удаляется из VLAN 1.

Настройка статичного маршрута

Для управления устройством из удаленной сети необходимо настроить статичный маршрут, представляющий собой IP-адрес, на который передаются пакеты, когда записи не найдены в таблицах устройств. Настроенный IP-адрес должен принадлежать к той же подсети, что и один из IP-интерфейсов устройства.

Чтобы настроить статичный маршрут, введите команду в командной строке системы, как показано в следующем примере настройки, где 100.1.1.1 (маска 24) соответствует конкретной станции управления, а 100.1.1.10 является статичным маршрутом.

Назначение статического адреса IP для порта внутри диапазона

 **ПРИМЕЧАНИЕ.** В этом примере используются следующие допущения:

- n IP-адрес, который необходимо назначить для интерфейса VLAN коммутатора PowerConnect - 192.168.1.123
- n IP-маска подсети для сети - 255.255.255.0
- n IP-адрес маршрута по умолчанию - 192.168.1.1
- n Строка SNMP сообщества для чтения и записи - «private»

```
console> enable
```



```

console# configure

console(config)# username admin password dell level 15

Console(config)# interface vlan 1

console (config-if) # ip address 192.168.1.123 /24

console (config-if) # exit

console (config) # ip default-gateway 192.168.1.1

console (config) # snmp-server community private rw

Console (config) # ex it

console#

```

Проверка IP-адресов и адреса шлюза по умолчанию

Убедитесь, что IP-адрес и шлюз по умолчанию были назначены правильно. Для этого выполните следующую команду и просмотрите ее результат:


Команда

```
console# show ip interface vlan 1
```

Результат


Gateway IP Address	Activity status	
-----	-----	
192.168.1.1	Active	
IP Address	Interface	Type
-----	-----	-----

192.168.1.123 /24	VLAN 1	Static
-------------------	--------	--------

 **ПРИМЕЧАНИЕ.** Рекомендуется загрузить самую последнюю версию документации пользователя с веб-сайта поддержки Dell support.dell.com.

Имя пользователя

Необходимо настроить имя пользователя для удаленного управления устройством, например, через SSH, Telnet или веб-интерфейс. Чтобы получить полные права управления устройством, необходимо указать максимальный уровень привилегий (15).

 **ПРИМЕЧАНИЕ.** Только администратор (суперпользователь) с наивысшим уровнем привилегий (15) имеет право управлять устройством через веб-интерфейс.

Дополнительную информацию об уровнях привилегий см. в «Справочном руководстве по интерфейсу командной строки».

Настроенное имя пользователя вводится при входе в систему во время сеансов удаленного администрирования. Для настройки имени пользователя и уровня привилегий введите команду в командной строке системы, как показано в следующем примере настройки:


```
console> enable
console# configure
console(config)# username admin password abc level 15
```

Строки сообщества SNMP

Протокол SNMP (Simple Network Management Protocol) обеспечивает способ управления устройствами в сети. На устройствах, поддерживающих SNMP, работает локальная программа (агент). Агенты SNMP ведут список переменных, которые используются для управления устройством. Эти переменные задаются в базе данных Management Information Base (MIB). База данных MIB содержит переменные, которые контролируются агентом. Агент задает SNMP формат спецификации MIB и формат для доступа к информации через сеть. Управление правами доступа для агентов SNMP осуществляется с помощью строк доступа и строк сообщества SNMP.

Устройство поддерживает протокол SNMP и содержит агента SNMP, который поддерживает набор стандартных или индивидуальных переменных MIB. Разработчики станций управления сетью требуют точную структуру дерева MIB и получают полную индивидуальную информацию MIB перед тем, как они смогут выполнять администрирование баз данных MIB.

Всеми параметрами можно управлять с любой управляющей платформы SNMP, за исключением IP-адреса и сообщества станции управления SNMP (имя сообщества и права доступа). Когда строк сообщества нет, то доступ администрирования SNMP к устройству запрещен.

 **ПРИМЕЧАНИЕ.** Устройство поставляется без настроенных строк сообщества. Устройство поддерживает SNMPv1 и SNMPv2. В этом разделе описываются параметры настройки SNMPv1/v2.

Далее показан экран настройки устройства по умолчанию:

console# show snmp		
Community- String	Community-Access	IP Address
-----	-----	-----
Traps are enabled.		

Authentication trap is enabled.		
Trap-Rec- Address	Trap-Rec- Community	Version
System Contact:		
System Location:		

Настройки строки сообщества, доступа сообщества и IP-адрес могут быть заданы с локального терминала во время процедуры начальной настройки.

Возможные варианты настройки SNMP:

- 1 Строка сообщества.
 - o **Только для чтения** - параметр, указывающий, что члены сообщества могут просматривать информацию о настройках, но не могут изменять ее.
 - o **Для чтения и записи** - параметр, указывающий, что члены сообщества могут просматривать и изменять информацию о настройках.
 - o **Супер** - параметр, указывающий, члены сообщества обладают правами доступа администратора.
- 1 Настраиваемый IP-адрес. Если IP-адрес не настроен, то все члены сообщества с одинаковым именем сообщества обладают одинаковыми правами доступа.

Как правило, используют две строки сообщества для устройства - одна (сообщество public) с доступом только для чтения, а вторая (сообщество private) - с доступом для чтения и записи. Строка public позволяет авторизованным станциям управления считывать объекты MIB, строка private позволяет авторизованным станциям считывать и изменять объекты MIB.

Во время начальной настройки рекомендуется настроить устройство согласно требованиям сетевого администратора, в соответствии с использованием станции управления на базе протокола SNMP.

Настройка SNMP

Чтобы настроить IP-адрес и строки сообщества станции SNMP для общих таблиц маршрутизатора устройства, выполните следующие действия.

1. В командной строке системы введите команду **Enable**. Строка приглашения отображается как #.
2. Введите команду **configure** и нажмите клавишу <Enter>.
3. В режиме настройки введите команду настройки SNMP с параметрами, включая имя сообщества (private), права доступа сообщества (чтение и запись) и IP-адрес, как показано в следующем примере.

```
console# configure
```

```
config(config)# snmp-server community private rw 11.1.1.2
```

Просмотр таблиц сообщества SNMP

Чтобы настроить IP-адрес и таблицы сообщества станции SNMP:

1. В командной строке системы введите команду **exit**. Строка приглашения отображается как #.
2. В режиме Privileged Exec введите команду **show**, как показано в следующем примере.

Настроенные параметры позволяют выполнить дальнейшую настройку устройства с любого удаленного местоположения.

console# show snmp		
Community- String	Community-Access	IP Address
-----	-----	-----
private	read write	11.1.1.2
Traps are enabled.		
Authentication trap is enabled.		
Trap-Rec- Address	Trap-Rec- Community	Version
System Contact:		
System Location:		

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.

- 1 Настройка IP-адресов с использованием протокола DHCP.
- 1 Настройка IP-адресов с использованием протокола BOOTP.
- 1 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.
 - 1 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)#
```

- 1 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 работает как клиент BOOTP.

Чтобы получить IP-адрес от сервера BOOTP:

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

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

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

Этот процесс показан в следующем примере:

```
console> enable

console# delete startup-config

Startup file was deleted

console# reload

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

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

*****

/* the 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:

- 1 Терминал
- 1 Telnet
- 1 SSH
- 1 HTTP
- 1 HTTPS

 **ПРИМЕЧАНИЕ.** Пароли определяются пользователем.

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

Настройка первоначального пароля 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
```

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

Настройка первоначального пароля Telnet

Для настройки первоначального пароля Telnet введите следующие команды:

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

console(config)# aaa authentication enable default line

console(config)# line telnet

console(config-line)# login authentication default

console(config-line)# enable authentication default

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

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

Настройка первоначального пароля SSH

Для настройки начального пароля SSH введите следующие команды:

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

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

```
console(config)# line ssh
```

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

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

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

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

Настройка первоначального пароля HTTP

Для настройки первоначального пароля HTTP введите следующие команды:

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

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


Настройка первоначального пароля HTTPS

Для настройки первоначального пароля HTTPS введите следующие команды:

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

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


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.

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-2004 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 (Загрузка программного обеспечения)

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

[3] Password Recovery Procedure (Процедура восстановления пароля)


[4] Enter Diagnostic Mode (Запуск режима диагностики)

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

[6] Back (Назад)

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 будет удалена, а устройство перезагружено.
4. Повторите начальную настройку устройства.


Восстановление пароля

Если определенный пользователем пароль утрачен, то можно вызвать процедуру восстановления пароля из меню Startup (Запуск). Эта процедура позволяет пользователю один раз войти в устройство без пароля.

Восстановление пароля возможно только с локального терминала:

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

Пароль будет удален.

 **ПРИМЕЧАНИЕ.** Чтобы обеспечить 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 проверьте соединение с сервером TFTP с помощью команды ping.
2. Убедитесь, что файл, который нужно загрузить, сохранен на сервере TFTP (файл `tos`).
3. Чтобы проверить номер версии программного обеспечения, запущенного на устройстве, введите команду `show version`. Далее приведен пример отображаемой на экране информации:

```
console# show version
```

```
SW version 1.0.0.42 (date 22-Jul-2004 time 13:42:41)
```

Boot version 1.0.0.18 (date 01-Jun-2004 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 загрузки системы, 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 через сервер TFTP:

1. Убедитесь, что IP-адрес настроен для одного из портов устройства, и проверьте соединение с сервером TFTP с помощью команды `ping`.
2. Убедитесь, что файл, который нужно загрузить (файл `ftb`), сохранен на сервере TFTP.
3. Чтобы проверить номер версии программного обеспечения, запущенного на устройстве, введите команду `show version`. Далее приведен пример отображаемой на экране информации:

```
console# sh ver
```

SW version 1.0.0.42 (date 22-Jul-2004 time 13:42:41)

Boot version 1.0.0.18 (date 01-Jun-2004 time 15:12:20)

HW version 00.00.01 (date 01-May-2004 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://1 76.215.31.3/332448-10018.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 системы Dell™ PowerConnect™ 5324

[А](#) [Б](#) [В](#) [Д](#) [Е](#) [З](#) [И](#) [К](#) [Л](#) [М](#) [Н](#) [О](#) [П](#) [Р](#) [С](#) [Т](#) [У](#) [Ф](#) [Х](#) [Ц](#) [Ш](#) [D](#) [E](#) [G](#) [I](#) [L](#) [N](#) [Q](#) [R](#) [S](#) [U](#) [V](#) [W](#)

Этот глоссарий содержит основные технические термины, представляющие интерес.

А	Б	В	Д	Е	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ш	D	E	G	I	L	N	Q	R	S	U	V	W
-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------

А

ARP

Протокол ARP (Address Resolution Protocol). 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.

Автоматическое согласование

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

- 1 Дуплексный и полудуплексный режим
 - 1 Управление потоком
 - 1 Скорость
-

Б

Бод

Число сигнальных элементов, передаваемых за одну секунду.

Большие кадры

Позволяют передавать данные меньшим числом пакетов. Большие пакеты уменьшают объем служебной информации, время обработки и сокращают число перерывов.

В

BootP

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.

Версия загрузчика

Версия загрузчика.

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.

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:

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

Е

Ethernet

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

EWS

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

З

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).

Дополнительную информацию о зеркалировании портов см. в разделе **Определение сеансов с зеркалированием портов**.

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.

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.

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

Коммутатор

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

Л

«Лавина» широковещательной передачи

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

Дополнительную информацию о «лавинах» широковещательной передачи см. в разделе [«Определение параметров LAG»](#).

ЛВС

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

М

MAC-адрес

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

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.

Максимально возможная скорость доставки

Трафик назначается для очереди с низшим приоритетом, и доставка пакетов не гарантируется.

Маршрутизатор

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

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.

Например, если IP-адрес источника - 149.36.184.198, а маска ввода - 255.36.184.00, то первые два бита IP-адреса игнорируются, а используются последние два бита.

Маска подсети

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

Многоадресная передача

Передаёт 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.

H

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.

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.

O

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.

Обратное давление

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

Объединенные VLAN

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

Объединительная плата

Основная шина, которая используется для передачи информации в устройстве.

Одноадресная передача

Форма пересылки, при которой один пакет передается одному пользователю.

Оконечная система

Устройство конечного пользователя в сети.

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 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.

Протокол

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

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:

- 1 входящими интерфейсами;
- 1 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

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.

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.

C

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 командной строки см. в разделе «Использование режима командной строки».

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:

- 1 Ethernet 10 Мбит/с
- 1 Fast Ethernet 100 Мбит/с
- 1 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.

T

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.

Telnet

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

TFTP

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

У

Узел

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

- 1 процессоры;
- 1 контроллеры;

1 рабочие станции.

Управление потоком

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

Уровень MAC

Подуровень уровня DTL (Data Link Control).

Ф

Файл образа

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

Файл рабочей настройки

Содержит все команды файла 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 состоит из управляющего устройства и арифметико-логического устройства.

Ш

Широковещательная передача

Метод передачи пакетов на все порты в сети.

Широковещательный домен

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

D

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 не известен, 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

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.

IEEE

Institute of Electrical and Electronics Engineers – Институт инженеров по электротехнике и электронике. Организация, занимающаяся разработкой стандартов связи и использования сетей.

IEEE 802.1d

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

IEEE 802.1p

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

IEEE 802.1Q

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

IP

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

IP-адрес

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

IPX

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

L

LAG

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

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

Layer 2

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

Layer 4

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

N

NMS

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

Q

QoS

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

R

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.

RSTP

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

S

SNMP

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

SNTP

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

SoC

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

SSH

Протокол SSH (Secure Shell). Обеспечивает вход 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 системы Dell™ PowerConnect™ 5324

- [Конфигурации портов устройства](#)
- [Фактические размеры](#)
- [Описания индикаторов](#)
- [Компоненты оборудования](#)

Конфигурации портов устройства

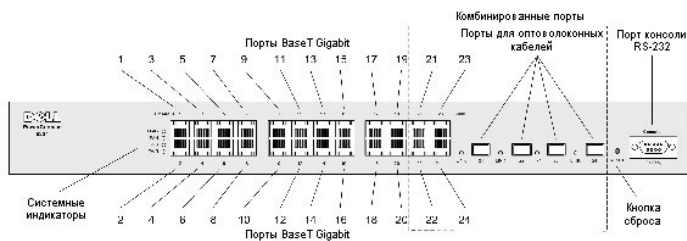
Описание портов передней панели системы PowerConnect 5324

Устройство PowerConnect 5324 оборудовано следующими портами.

- 1 **24 порта для медного кабеля** - порты RJ-45, назначенные как порты 10/100/1000 BaseT Gigabit Ethernet
- 1 **4 порта для оптоволоконного кабеля** - назначены как порты Gigabit
- 1 Порт **терминала** - порт консоли RS-232

На следующем рисунке изображена передняя панель устройства PowerConnect 5324.

Рис 2-3. Передняя панель устройства PowerConnect 5324



На передней панели располагаются порты с 1 по 24. 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. 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 1-23, а порты нижнего ряда четными числами 2-24.

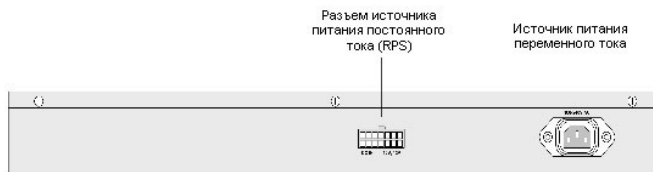
На передней панели находится порт RS-232 консоли, все индикаторы устройства и кнопка Reset (Сброс), используемая для сброса устройства вручную.

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. 2-4](#).

Рис. 2-4. Задняя панель устройства



На задней панели устройства находятся два разъема питания. 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

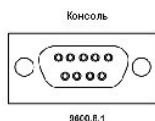
Порты SFP

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. 2-5. Порт консоли



Комбинированные порты

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

- 1 Разъем RJ-45 для подключения кабеля медной витой пары
- 1 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.

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

Описания индикаторов

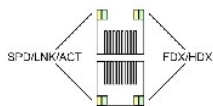
На передней панели находятся светодиоды (индикаторы), которые показывают состояние связи, питания, вентиляторов и системы диагностики.

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. 2-6. Индикаторы порта RJ-45 10/100/1000 Base-T



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

Табл. 2-1. Показания индикатора порта для медного кабеля RJ-45 10/100/1000BaseT

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.
Правый индикатор	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.
	Не горит	Порт работает в полудуплексном режиме.

Индикаторы SFP

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

Рис. 2-7.



Индикаторы 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. 2-8](#) изображены системные индикаторы.

Рис. 2-8. Системные индикаторы

DIAG 
FAN 
RPS 
PWR 

Описание показаний индикаторов приведено в следующей таблице.

Табл. 2-3. Показания системных индикаторов

Индикатор	Цвет	Описание
Диагностика (DIAG)	Мигает зеленым	В системе запущена 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.
	Горит красным	Произошел сбой источника питания.

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 системы Dell™ PowerConnect™ 5324

- [Меры предосторожности при монтаже](#)
- [Требования к месту размещения](#)
- [Распаковка](#)
- [Установка устройства](#)
- [Подключение к устройству](#)
- [Подключение портов, кабели и расположение контактов](#)
- [Настройки порта по умолчанию](#)

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

Меры предосторожности при монтаже

ВНИМАНИЕ! 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.

ВНИМАНИЕ! Обратите внимание на следующие пункты до выполнения процедур, описанных в этом разделе:

- 1 Убедись, что стойка или шкаф, в котором размещается устройство, надежно закреплены, чтобы предотвратить их шатание или опрокидывание.
 - 1 Убедитесь, что цепи источника питания надлежащим образом заземлены.
 - 1 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.
 - 1 Убедитесь, что кабель питания, удлинитель и разъем не повреждены.
 - 1 Убедитесь, что устройство не подвергается воздействию влаги.
 - 1 Убедитесь, что устройство не размещается вблизи радиаторов отопления и других источников тепла.
 - 1 Убедитесь, что охлаждающие вентиляторы не заблокированы.
 - 1 Не вставляете посторонние предметы в устройство, так как это может вызвать возгорание или поражение электрическим током.
 - 1 Используйте устройство только с оборудованием, для которого оно предназначено.
 - 1 Прежде чем снимать крышки или прикасаться к внутреннему оборудованию, дайте устройству остыть.
 - 1 Убедитесь, что устройство не перегружает силовые цепи, электропроводку и схемы защиты от перегрузки. Для определения вероятности перегрузки цепей питания необходимо просуммировать силы электрического тока для всех устройств, смонтированных в одной цепи. Сравните это суммарное значение с заданным ограничением для цепи.
 - 1 Не монтируйте устройство в среде, в которой окружающая температура может превысить 40°C (122°F).
 - 1 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:

- 1 **Общее** - Убедитесь, что подача питания производится правильно.
- 1 **Питание** - Устройство установлено на расстоянии 1,5 м (5 футов) от заземленной легко доступной розетки 220/110 В переменного тока, 50/60 Гц.
- 1 **Расстояние** - Имеется достаточное расстояние спереди для доступа оператора. Оставьте некоторое расстояние для силовых и сигнальных кабелей, а также для вентиляции.
- 1 **Прокладка кабелей** - Кабели следует прокладывать подальше от источников электрических помех, например, радиопередатчиков, усилителей, линий питания и осветительных приборов с флуоресцентными лампами.
- 1 **Требования к окружающей среде** - Во время работы температура окружающей среды должна быть в диапазоне от 0 до 40°C при

относительной влажности от 10% до 95 % 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:

- 1 Устройство
- 1 Кабель питания переменного тока
- 1 Кроссоверный кабель RS-232
- 1 Самоклеющиеся резиновые прокладки
- 1 Крепежный набор для монтажа в стойке
- 1 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

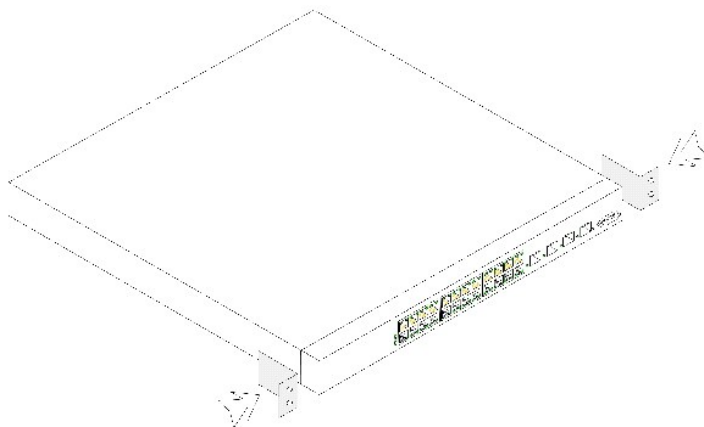
Монтаж устройства в стойке

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

 **ПРЕДУПРЕЖДЕНИЕ.** 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. 3-9](#) показано, куда следует устанавливать кронштейны.

Рис. 3-9. Подсоединение кронштейнов для монтажа в стойке



2. Вставьте прилагаемые винты в отверстия и затяните с помощью отвертки.
3. Повторите то же самое для кронштейна установки в стойку с другой стороны устройства.
4. Вставьте устройство в 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:

1. VT100-совместимый терминал или настольный или переносной компьютер с последовательным портом, на котором установлено программное обеспечение эмуляции терминала VT100.
1. 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.

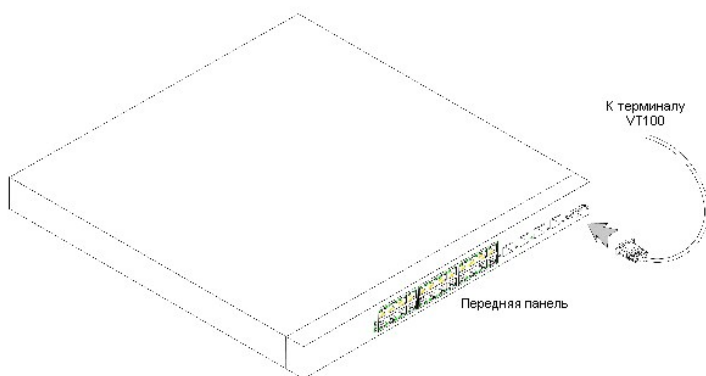
- a. Выберите соответствующий последовательный порт (последовательный порт 1 или последовательный порт 2) для подключения к консоли.
- b. Задайте скорость передачи данных 9600 бод.
- c. Задайте следующий формат данных: 8-битные данные, 1 стоповый бит, без контроля четности.
- d. Присвойте управлению 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**, а не **Windows keys**.

ЗАМЕЧАНИЕ. 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 передней панели.

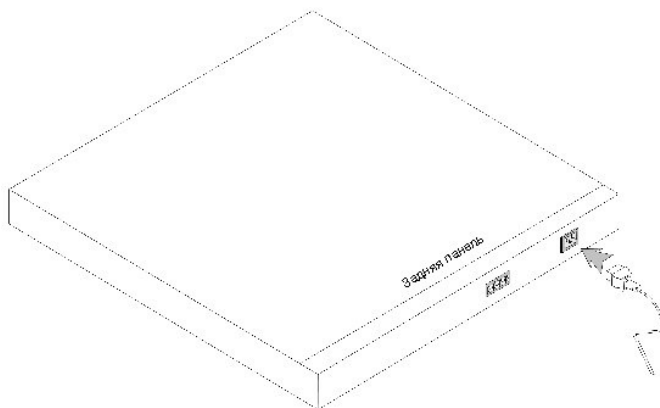
Рис. 3-10. Подключение к порту консоли PowerConnect 5324



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. 3-11. 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 3-4.

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

Порты и разъемы и кабели

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

Таблица 3-5. 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.

Когда включен интерфейс MDI/MDIX (Media Dependent Interface with Crossover), возможно автоматическое исправление ошибок при выборе кабелей, что устраняет необходимость распознавания кабеля прямого подключения и кроссового кабеля. (Стандарт кабелей для конечных станций называется MDI (MDI Media-Dependent Interface), а стандарт кабелей для концентраторов и коммутаторов называется 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 3-6. Настройки порта по умолчанию

Функция	Настройка по умолчанию
Скорость и режим работы порта	10/100/1000BaseT (для медных кабелей): автоматическое согласование, полнодуплексный 100
Состояние пересылки пакетов для порта	Включено
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 системы Dell™ PowerConnect™ 5324

- [PowerConnect 5324](#)
- [Функциональные возможности](#)
- [Дополнительная документация по режиму командной строки](#)

 **ЗАМЕЧАНИЕ.** Перед дальнейшими действиями 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.

PowerConnect 5324

Устройство PowerConnect 5324 имеет 24 порта Gigabit Ethernet. Также оно имеет четыре оптоволоконных порта SFP назначенные как комбинированные порты являющиеся альтернативой портам Ethernet с 21 по 24. Комбинированные порты представляет собой один порт, имеющий два физических подключения. Когда одно подключено, другое отключено.

На [рис. 1-1](#) и [рис. 1-2](#) показаны передняя и задняя панели PowerConnect 5324.

Рис. 1-1. Передняя панель устройства PowerConnect 5324



Рис. 1-2. Задняя панель коммутатора PowerConnect 5324



Функциональные возможности

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

Общие функции

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 /MDI X

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

Стандарт кабелей для конечных станций - MDI (MDI Media-Dependent Interface), а стандарт кабелей для концентраторов и коммутаторов называется MDI X (MDI X Media-Dependent Interface with Crossover).

Дополнительную информацию о настройке MDI/MDI для портов или объединенных групп каналов (LAG) см. в разделах [«Определение параметров порта»](#) или [«Определение параметров LAG»](#).

Поддержка управления потоком (IEEE 802.3X)

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

Дополнительную информацию о настройке управления потоком для портов или групп LAG см. в разделах [«Определение параметров порта»](#) или [«Определение параметров LAG»](#).

Поддержка обратного давления

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

Дополнительную информацию о настройке обратного давления для портов или групп LAG см. в разделах [«Определение параметров порта»](#) или [«Определение параметров LAG»](#).

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.

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 сетей VLAN»](#).

VLAN, основанные на портах

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

Дополнительную информацию см. в разделе [«Определение параметров портов VLAN»](#).

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).

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 сходимости для протокола STP без образования циклов пересылки.

Дополнительную информацию см. в разделе [«Настройка протокола RSTP»](#).

Страница Link Aggregation

Дополнительную информацию см. в разделе [«Объединение портов»](#).

Страница Link Aggregation

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:

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

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

Дополнительную информацию см. в разделе [«Определение членства в 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 [«Определение параметров SNMP»](#).

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.

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, относящиеся 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 (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 консоли (CLI) максимально соответствуют 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 ноль - это самый высокий уровень), тем более точный генератор.

Дополнительную информацию см. в разделе [«Настройка параметров SNMP»](#).

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.

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).

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 этим 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 кодированное 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+»](#).

Дополнительная документация по режиму командной строки

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 системы Dell™ PowerConnect™ 5324

- [Обзор качества обслуживания QoS](#)
- [Определение общих параметров CoS](#)

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.

Обзор качества обслуживания QoS

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.

К реализации, для которой необходима функция качества обслуживания (QoS), относятся некоторые типы трафика, например передача голоса, видеоизображения и трафик в реальном времени, для которых можно назначить очередь с высоким приоритетом, а для другого трафика можно назначить очередь с низким приоритетом. Это позволяет ускорить прохождение первоочередного трафика.

Показатель QoS характеризуется следующими элементами.

- 1 Classification (Классификация) - определяет, какие поля соответствуют тем или иным значениям. Все пакеты, соответствующие пользовательским спецификациям, классифицируются вместе.
- 1 Action (Действие) - определяет управление трафиком, в котором пакеты пересылаются по информации о пакете, а также определяет значения полей пакетов, например приоритет VLAN (VPT) и DSCP (DiffServ Code Point).

Информация о классификации 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.

Таблица 9-92. Значения по умолчанию для таблицы привязки CoS к очереди

Значение CoS	Значения очереди пересылки
0	q2
1	q1 (низший приоритет = максимально возможная скорость доставки)
2	q1 (низший приоритет = максимально возможная скорость доставки)
3	q2
4	q3
5	q3
6	q4 (высший приоритет)
7	q4 (высший приоритет)

Для непометенных 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.

Таблица 9-93. Значения по умолчанию для таблицы привязки DSCP к очереди

Значение DSCP	Значения очереди пересылки
0-7	q2 (низший приоритет)
8-15	q1
16-23	q1
24-31	q2
32-39	q3
40-47	q3
48-55	q4
55-63	q4 (высший приоритет)

Привязка DSCP активируется 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.

1. 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.
1. 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 четыре очереди имеют веса 1, 2, 3 и 4, пакеты с высшим приоритетом пересылки будут назначены для очереди 4, а пакеты с низким приоритетом пересылки - для очереди 1.
Устанавливая высший приоритет пересылки для очередей с длиной 4, WRR обрабатывает трафик высшего приоритета и гарантирует, что пересылка трафика низшего приоритета осуществляется надлежащим образом.

Схема планирования активируется для системы в целом. Для очередей, которым назначена политика строгого приоритета, автоматически назначается очередь с высшим приоритетом. По умолчанию для всех очередей установлен Strict Priority (Строгий приоритет). При переключении в режим WRR значение веса по умолчанию будет равно единице. 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.

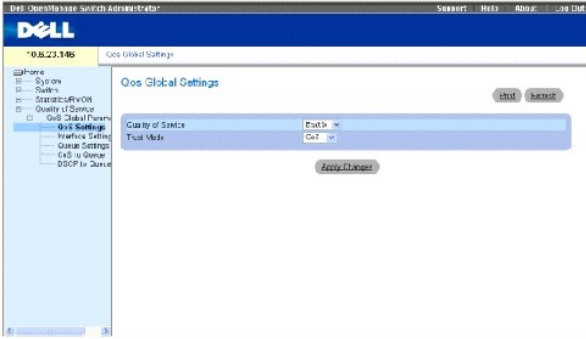
Определение общих параметров CoS

Общие параметры класса обслуживания устанавливаются на странице [CoS Global Parameter](#) (Общие параметры CoS).

Настройка общих параметров QoS

На странице [QoS Global Settings](#) (Общие параметры QoS) имеются поля для включения или отключения QoS. Кроме того, можно выбрать Trust (Доверие). Режим доверия основывается на предварительно определенных полях в пакете для определения очереди вывода. Чтобы открыть страницу [QoS Settings](#) (Параметры QoS), выберите Quality of Service (Качество обслуживания) → CoS Global Parameters (Общие параметры CoS) → CoS Settings (Параметры CoS) на панели дерева.

Рис. 9-130. Страница QoS Settings (Параметры QoS)



Quality of Service (Качество обслуживания) - включает или отключает управление сетевым трафиком с помощью функции Quality of Service (Качество обслуживания).

Trust Mode (Режим доверия) - определяет, какие поля 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 - 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.

ПРИМЕЧАНИЕ. Параметры интерфейса Trust (Доверие) заменяют общие параметры Trust (Доверие).

Включение функции Class of Service (Качество обслуживания):

1. Откройте страницу [QoS Settings](#) (Параметры QoS).
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 [QoS Settings](#) (Параметры QoS).
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 команды консоли для настройки полей, отображаемых на странице [QoS Settings](#) (Параметры QoS).

Таблица 9-94. Команды консоли для параметров 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».
--------------	------------------------------------

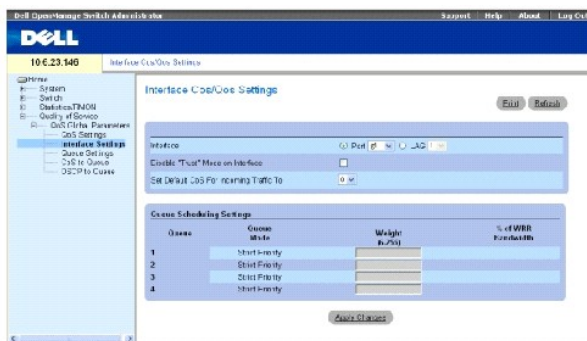
Далее приведен пример команд консоли.

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

Определение параметров интерфейса QoS

На странице [Interface Cos/QoS Settings](#) (Параметры интерфейса Cos/QoS) имеются поля для каждого интерфейса, позволяющие определить, должен ли быть включен выбранный режим Trust (Доверие). Приоритет по умолчанию для входящих непомеченных пакетов также выбирается на странице [Interface Cos/QoS Settings](#) (Параметры QoS): выберите Quality of Service (Качество обслуживания) → CoS Global Parameters (Общие параметры CoS) → Interface Settings (Параметры интерфейса) на панели дерева.

Рис. 9-131. Страница Interface Cos/QoS Settings (Параметры интерфейса Cos/QoS)



Interface (Интерфейс) - определенный порт или группа LAG для настройки:

Disable «Trust» Mode on Interface (Отключить режим доверия для интерфейса) - отключает режим доверия для выбранного интерфейса. Этот параметр заменяет режим Trust (Доверие), настроенный на устройстве.

Set Default CoS For Incoming Traffic To (Задать CoS по умолчанию для входящего трафика) - определяет значение метки CoS по умолчанию для входящих непомеченных пакетов. Метки CoS могут иметь значения от 0 до 7. Значение по умолчанию - 0.

Queue (Очередь) - номер очереди.

Queue Mode (Режим очереди) - указывает на состояние очереди: Strict Priority (Строгий приоритет) или WRR. Определяется на экране Queue Settings (Параметры очереди).

- 1 Режим SP можно настроить во всех очередях с 1 по 4.
- 1 Режим WRR можно настроить во всех очередях с 1 по 4.
- 1 Режим SP можно настроить в очередях с 1 по 2, а WRR - в очередях с 3 по 4.
- 1 Режим WRR можно настроить в очередях с 1 по 2, а SP - в очередях с 3 по 4.

Weight (6-255) (Вес (6-255)) - назначает веса WRR для очередей. Это поле работает только для очередей в режиме WRR.

% of WRR Bandwidth - процентное выражение веса, определяемое в поле Weight (6-255) (Вес).

Назначение параметров QoS/CoS для интерфейса

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

Параметры CoS будут назначены для интерфейса.

Назначение CoS для интерфейсов с помощью команд консоли

В следующей таблице приведены команды консоли для настройки полей, отображаемых на странице [Interface Cos/QoS Settings](#) (Параметры интерфейса Cos/QoS).

Таблица 9-95. Команды консоли для интерфейса CoS

Команда консоли	Описание
qos trust	Включение состояния доверия для каждого порта.
qos cos default-cos	Настройка значения по умолчанию для порта CoS.
no qos trust	Отключение состояния доверия для каждого порта.

Далее приведен пример команд консоли.

```
Console (config)# interface ethernet g5

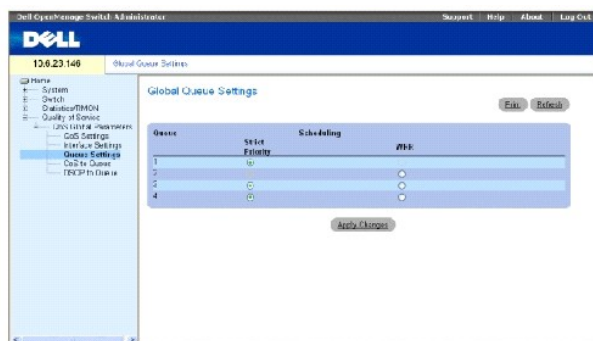
Console (config-if)# qos trust

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

Определение параметров очереди

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

Рис. 9-132. Страница Global Queue Setting (Общие параметры очереди)



Queues (Очередь) - 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.

Определение параметров очереди

1. Откройте страницу [Global Queue Setting](#) (Общие параметры очереди).
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 команды консоли для настройки полей, отображаемых на странице [Global Queue Setting](#) (Общие параметры очереди).

Таблица 9-96. Команды консоли для параметров очереди

Команда консоли	Описание
wrr-queue bandwidth weight1 weight2 . weight_n	Назначает веса WRR для очередей выхода.
show qos interface [ethernet номер_интерфейса] [queuing]	Отображает данные 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 queuing

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	125	Disable	N/A
2	125	Disable	N/A
3	125	Disable	N/A
4	125	Disable	N/A

Cos queue map:

Cos qid

0 2

1 1

2 1

3 2

4 3

5 3

6 4

7 4

Привязка значений CoS к очередям

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

Рис. 9-133. Страница CoS to Queue Mapping Table (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 четыре очереди приоритета трафика.

Restore Defaults (Восстановить значения по умолчанию) - восстанавливает заводские файлы устройства для привязки значений CoS к очереди пересылки.

Привязка значения CoS к очереди

1. Откройте страницу [CoS to Queue 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).

Таблица 9-97. Команды консоли для параметров привязки CoS к очереди

Команда консоли	Описание
wrr-queue cos-map queue-id cos1..cos8	Связывает значения 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 Mapping](#) (Привязка DSCP) представлены поля для определения очереди вывода для тех ли иных полей DSCP. Чтобы открыть страницу [DSCP Mapping](#) (Привязка DSCP), выберите Quality of Service (Качество обслуживания)→ CoS Global Parameters (Общие параметры CoS)→ DSCP Mapping (Привязка DSCP) на панели дерева.


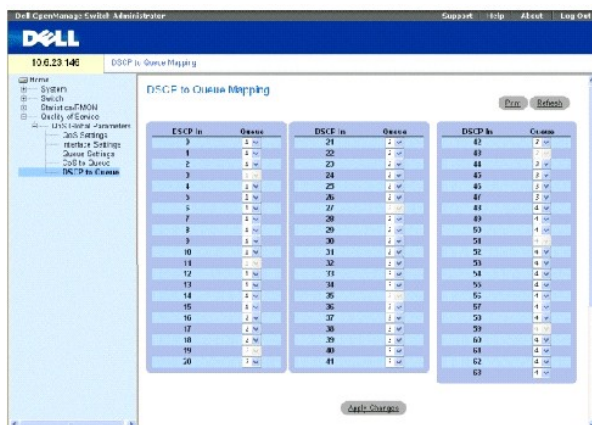
 **ПРИМЕЧАНИЕ.** Список параметров очереди по умолчанию DSCP представлен в разделе «Значения по умолчанию для таблицы привязки DSCP к очереди».

Рис. 9-134. Страница DSCP Mapping (Привязка DSCP)



DSCP In (DSCP входящего пакета) - значения в поле DSCP внутри ходящего пакета.

Queue (Очередь) - очередь, для которой назначены пакеты с определенным значением DSCP. Значения: от 1 до 4, где 1 - это наименьшее значение, а 4 - наибольшее.

Привязка значения DSCP и назначение очереди приоритета

1. Откройте страницу [DSCP Mapping](#) (Привязка DSCP).
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.

Привязка значений DSCP с помощью команд консоли

В таблице перечислены команды консоли, соответствующие полям настройки на странице [DSCP Mapping](#) (Привязка DSCP).

Таблица 9-98. Команды консоли для привязки значений DSCP к очередям

Команда консоли	Описание
<code>qos map dscp-queue dscp-list to queue-id</code>	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 системы Dell™ PowerConnect™ 5324

- [Характеристики портов и кабелей](#)
- [Условия работы](#)
- [Физические характеристики устройства](#)
- [Характеристики памяти устройства](#)
- [Характеристики функций](#)

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 10-99.

Устройство	Характеристика
PowerConnect 5324	<ul style="list-style-type: none">1 24 порта GE1 4 порта SFP1 Порт консоли RS-232
Типы портов	
RJ-45	<ul style="list-style-type: none">1 10 Base-T1 100 Base-T1 1000 Base-T
SFP	Поддерживает стандартные миниатюрные разъемы Подключаемые гигабитные трансиверы
Параметры порта	
	<ul style="list-style-type: none">1 Автоматическое согласование скорости, дуплексный режим и управление потоком1 Обратное давление1 Защита от блокировки очереди1 Автоматический выбор MDI/MDIX1 Зеркалирование портов1 Защита от «лавины» широкополосной передачи

Характеристики портов

Условия работы

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

Таблица 10-100.

Параметр	Характеристика
Рабочая температура	от 0 до 40 C / от 32 до 104 F
Относительная влажность при работе	от 10% до 90% (без конденсации)

Условия работы

Физические характеристики устройства

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

Таблица 10-101.

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

Физические характеристики устройства

Характеристики памяти устройства

В этом разделе описаны характеристики памяти устройства.

Таблица 10-102.

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

Характеристики памяти устройства

Характеристики функций

VLAN

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

Качество обслуживания

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

Многоадресная передача Layer 2

- 1 Поддержка динамической многоадресной передачи - поддерживаются до 256 групп многоадресной передачи в наблюдении по протоколу IGMP или статической многоадресной рассылке

Безопасность устройства

- 1 Защита доступа к коммутатору с помощью пароля
- 1 Сигналы и блокировки на основе MAC-адреса порта
- 1 Удаленная проверка подлинности RADIUS для доступа к коммутатору с целью управления
- 1 TACACS+

- 1 Фильтрация доступа для управления с помощью профилей доступа для управления
- 1 Шифрование управления SSH/SSL

Дополнительные функции коммутатора

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

Управление устройством

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

[Назад на страницу «Содержание»](#)

[Назад на страницу «Содержание»](#)

Настройка сведений об устройстве

Руководство пользователя системы Dell™ PowerConnect™ 5324

- [Настройка безопасности сети](#)
- [Настройка портов](#)
- [Настройка адресных таблиц](#)
- [Настройка протокола GARP](#)
- [Настройка протокола STP](#)
- [Настройка сетей VLAN](#)
- [Объединение портов](#)
- [Поддержка пересылки многоадресного трафика](#)

В этом разделе 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 на основе порта включает:

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

Проверка подлинности на основе портов формирует два состояния доступа:

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

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

Расширенная проверка подлинности на основе порта

Расширенная проверка подлинности на основе порта позволяет нескольким хостам подключаться к одному порту. Расширенная проверка подлинности на основе порта требует авторизации только одного хоста, чтобы доступ к системе имели все хосты. Если порт не проходит авторизацию, всем подключенным хостам будет отказано в доступе к сети.

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

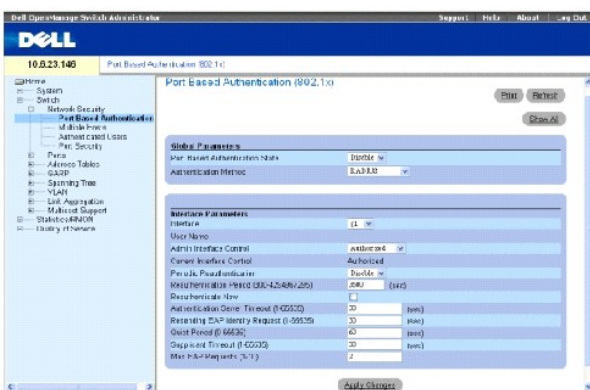
Расширенная проверка подлинности на основе порта реализована в следующих режимах:

- 1 **Single Host Mode** (режим одного хоста) - разрешает доступ к порту только проверенному хосту.
- 1 **Режим нескольких хостов** - позволяет нескольким хостам подключаться к одному порту. Требуется авторизация только одного хоста, чтобы доступ к сети имели все хосты. В случае неудачной проверки подлинности хоста или появления сообщения выхода EAPOL доступ запрещается для всех подключенных клиентов.

Настройка проверки подлинности на основе порта

Страница [Port Based Authentication](#) (Проверка подлинности на основе порта) содержит поля для настройки проверки подлинности на основе порта. Чтобы открыть страницу [Port Based Authentication](#) (Проверка подлинности на основе порта), выберите Switch (Коммутатор) → Network Security (Безопасность сети) → Port Based Authentication (Проверка подлинности на основе порта).

Рис. 7-80. 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.

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 (Авторизован) - устанавливает интерфейс в авторизованное состояние (трафик разрешен).

Unauthorized (Не авторизован) - устанавливает интерфейс в неавторизованное состояние (трафик запрещен).

Auto (Автоматически) - состояние авторизации устанавливается методом авторизации.

Current Interface Control (Текущее управление интерфейсом) - определяет текущее состояние авторизации настроенного порта.

Periodic Reauthentication (Периодическое повторение проверки подлинности) - для выбранного порта, если это возможно, выполняется периодическая проверка подлинности. Период повторения проверки подлинности определяется в поле **Reauthentication Period (300-4294967295)** (Период повторения проверки подлинности).

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 (1-65535)) - 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 (1-65535)) - определяет время до повторной отправки запроса EAP. Значение по умолчанию: 30 секунд.

Quiet Period (0-65535) (Период молчания (0-65535)) 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 (1-65535)) - 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 (1-10)) - 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](#) (Проверка подлинности на основе порта):

Рис. 7-81. Страница Port Based Authentication Table (Проверка 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](#) (Проверка 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).

Таблица 7-49. Команды консоли для проверки подлинности на основе порта

Команда консоли	Описание
aaa authentication dot1x default <i>метод1 [метод2]</i>	Указывает один или несколько методов проверки подлинности, авторизации и учета (AAA), используемые на интерфейсах IEEE 802.1X.
dot1x max-req <i>число</i>	Устанавливает максимальное число попыток отправки запросов EAP клиенту перед возобновлением процесса проверки подлинности.
dot1x re-authenticate [ethernet <i>интерфейс</i>]	Инициализирует ручную 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 <i>секунды</i>	Устанавливает число секунд, в течение которых устройство остается в состоянии молчания после обмена данными в ходе неудачной проверки подлинности.

<code>dot1x timeout re-authperiod</code> секунды	Устанавливает число секунд между попытками повторной проверки подлинности.
<code>dot1x timeout server-timeout</code> секунды	Устанавливает время повторной передачи пакетов на сервер проверки подлинности.
<code>dot1x timeout supp-timeout</code> секунды	Устанавливает время для повторной отправки кадра запроса EAP клиенту.
<code>dot1x timeout tx-period</code> секунды	Устанавливает число секунд, в течение которых устройство ожидает ответа на запрос EAP от клиента перед повторной отправкой запроса.
<code>show dot1x [ethernet интерфейс]</code>	Отображает состояние 802.1X для устройства или указанного интерфейса.
<code>show dot1x users [username username]</code>	Отображает пользователей 802.1X для устройства.

Далее приведен пример команд консоли.

```

console> enable

Console# show dot1x

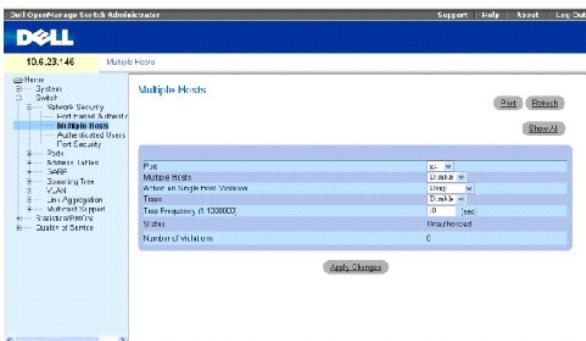
```

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. 7-82. Страница Multiple Hosts (Несколько хостов)



Port (Порт) - номер порта, для которого включен режим расширенной проверки подлинности на основе порта.

Multiple Hosts (Несколько хостов) - включает или отключает один хост для авторизации нескольких хостов для доступа к системе. Этот параметр необходимо включить, чтобы отключить фильтр на входе или использовать защиту блокировки для выбранного порта.

Action on Single Host Violation (Действие при нарушении доступа одного хоста) - определяет действие, которое необходимо применять для пакетов, поступающих в режиме одного хоста от хоста, MAC-адрес которого отличается от MAC-адреса клиента (просителя). 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.

Permit (Разрешить) - пересылает пакет от неизвестного источника, но MAC-адреса не распознаются.

Deny (Отклонить) - 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 (1-1000000) (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** 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.

No single-host (Не один хост) - включен параметр **Multiple Hosts** (Несколько хостов).

Number of Violations (Число нарушений) - число пакетов, поступивших на интерфейс в режиме одного хоста от хоста, MAC-адрес которого отличается от MAC-адреса клиента (просителя).

Отображение таблицы [Multiple Hosts Table](#) (Таблица нескольких хостов)

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

Откроется страница [Multiple Hosts Table](#) (Таблица нескольких хостов):

Рис. 7-83. Страница Multiple Hosts Table (Таблица нескольких хостов)

Multicla Hosts Table

Default

Port	Enable Multiple Hosts	Action on Violation	Enable Traps	Trap Frequency	Status	Number of Violations
1	g1	Deny	<input type="checkbox"/>	10	Unauthorized	0
2	g2	Deny	<input type="checkbox"/>	10	Unauthorized	0
3	g3	Deny	<input type="checkbox"/>	10	Unauthorized	0
4	g4	Deny	<input type="checkbox"/>	10	Unauthorized	0
5	g5	Deny	<input type="checkbox"/>	10	Unauthorized	0
6	g6	Deny	<input type="checkbox"/>	10	Unauthorized	0
7	g7	Deny	<input type="checkbox"/>	10	Unauthorized	0
8	g8	Deny	<input type="checkbox"/>	10	Unauthorized	0
9	g9	Deny	<input type="checkbox"/>	10	Unauthorized	0
10	g10	Deny	<input type="checkbox"/>	10	Unauthorized	0
11	g11	Deny	<input type="checkbox"/>	10	Unauthorized	0
12	g12	Deny	<input type="checkbox"/>	10	Unauthorized	0
13	g13	Deny	<input type="checkbox"/>	10	Unauthorized	0
14	g14	Deny	<input type="checkbox"/>	10	Unauthorized	0
15	g15	Deny	<input type="checkbox"/>	10	Unauthorized	0
16	g16	Deny	<input type="checkbox"/>	10	Unauthorized	0
17	g17	Deny	<input type="checkbox"/>	10	Unauthorized	0
18	g18	Deny	<input type="checkbox"/>	10	Unauthorized	0
19	g19	Deny	<input type="checkbox"/>	10	Unauthorized	0
20	g20	Deny	<input type="checkbox"/>	10	Unauthorized	0
21	g21	Deny	<input type="checkbox"/>	10	Unauthorized	0
22	g22	Deny	<input type="checkbox"/>	10	Unauthorized	0
23	g23	Deny	<input type="checkbox"/>	10	Unauthorized	0
24	g24	Deny	<input type="checkbox"/>	10	Unauthorized	0

Apply Changes

Включение нескольких хостов с использованием команд консоли

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

Таблица 7-50. Команды консоли для нескольких хостов

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

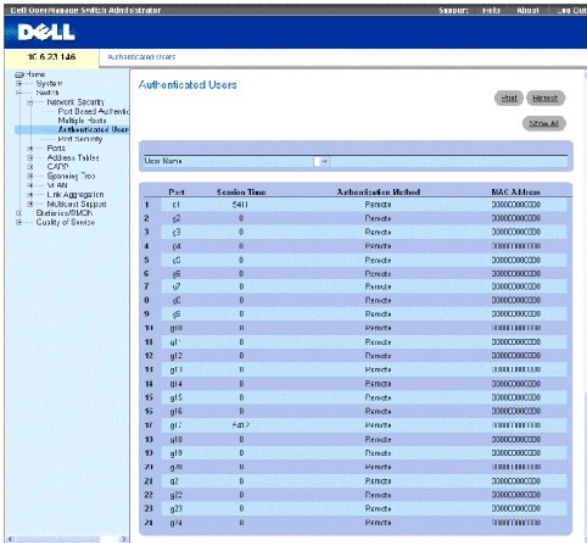
Далее приведен пример команды консоли.

```
Neyland# configure
Neyland(config)# interface ethernet g1
Neyland(config-if)# dot1x multiple-hosts
```

Проверка подлинности пользователей

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

Рис. 7-84. Страница Authenticated Users (Проверка подлинности пользователей)



User Name (Имя пользователя) - список пользователей, авторизованных с использованием сервера RADIUS.

Port (Порт) - номера портов, используемые для проверки подлинности - для каждого имени пользователя.

Session Time (Время сеанса) - время с момента входа пользователя на устройство. Формат поля **дни:часы:минуты:секунды**, например 3 дня: 2 часа: 4 минуты: 39 секунд.

Last Authentication (Последняя проверка подлинности) - время, прошедшее с момента последней проверки подлинности пользователя. 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. 7-85. 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).

Таблица 7-51. Команды консоли для добавления имени пользователя

Команда консоли	Описание
show dot1x users [username username]	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

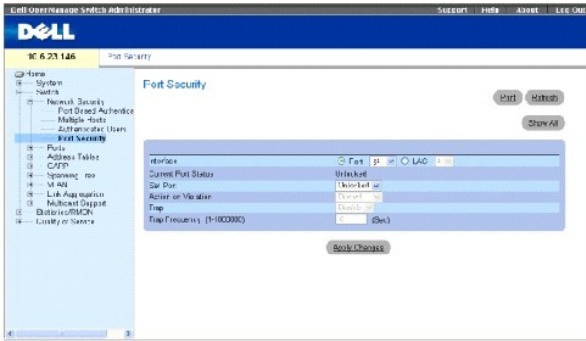
Безопасность сети можно повысить, если разрешить доступ к определенным портам только пользователям с определенными MAC-адресами. MAC-адреса определяются динамически в процессе подключения или настраиваются статически. Функция безопасности блокировки портов проверяет полученные пакеты и определяет, откуда 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:

- 1 Пересылаются
- 1 Игнорируются без системного прерывания
- 1 Игнорируются с системным прерыванием
- 1 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. 7-86. 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.

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 (1-1000000)) - 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. 7-87. Страница Port Security Table (Таблица безопасности портов)

Port	Current Port Status	Set Port	Action	Trap	Trap Frequency	Apply Select All
1 g1	Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
2 g2	Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
3 g3	Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
4 g4	Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
5 g5	Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
6 g6	Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
7 g7	Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
8 g8	Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
9 g9	Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
10 g10	Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
11 g11	Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
12 g12	Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
13 g13	Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
14 g14	Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
15 g15	Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
16 g16	Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
17 g17	Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
18 g18	Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
19 g19	Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
20 g20	Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
21 g21	Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
22 g22	Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
23 g23	Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
24 g24	Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
Global System LAGs						
25 LAG 1	Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
26 LAG 2	Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
27 LAG 3	Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
28 LAG 4	Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
29 LAG 5	Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
30 LAG 6	Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
31 LAG 7	Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
32 LAG 8	Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>

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).

Таблица 7-52. Команды консоли для настройки безопасности портов

Команда консоли	Описание
shutdown	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 порт-канал-номер}	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	-	-	-	-

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) → (Настройка портов) на панели дерева.

Рис. 7-88. 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 Port (Возврат порта к работе) - заново активизирует порт, если он был отключен системой безопасности.

Operational Status (Рабочее состояние) - рабочее состояние порта. Возможные значения этого поля:

Suspended (Приостановлен) - порт активен и в настоящий момент не получает и не передает трафик.

Active (Активен) - порт активен и в настоящий момент получает и передает трафик.

Disable (Отключен) - порт отключен и в настоящий момент не получает и не передает трафик.

Admin Speed (Администрирование скорости) - настроенная скорость порта. Тип порта определяет доступные параметры скорости. Значение скорости порта может быть изменено только в том случае, если 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.

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.

Определение параметров порта

1. Откройте страницу [Port Configuration](#) (Настройка портов).
2. Выберите порт в поле **Port** (Порт).
3. Определите 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. 7-89. Страница Ports Configuration Table (Таблица настройки портов)

Port Configuration Table

Port	Port Type	Port Status	Port Speed	Duplex Mode	Auto Negotiation	Back Pressure	Flow Control	MDI/MDIX	1 GbE
1	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
2	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
3	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
4	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
5	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
6	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
7	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
8	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
9	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
10	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
11	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
12	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
13	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
14	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
15	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
16	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
17	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
18	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
19	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
20	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
21	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
22	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
23	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
24	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
25	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
26	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
27	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
28	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
29	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
30	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
31	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
32	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
33	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
34	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
35	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
36	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
37	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
38	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
39	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
40	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
41	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
42	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
43	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
44	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
45	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
46	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
47	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
48	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
49	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
50	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
51	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
52	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
53	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
54	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
55	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
56	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
57	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
58	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
59	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
60	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
61	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
62	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
63	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
64	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
65	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
66	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
67	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
68	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
69	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
70	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
71	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
72	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
73	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
74	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
75	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
76	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
77	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
78	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
79	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
80	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
81	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
82	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
83	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
84	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
85	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
86	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
87	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
88	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
89	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
90	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
91	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
92	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
93	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
94	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
95	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
96	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
97	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
98	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
99	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
100	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A

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).

Таблица 7-53. Команды консоли для настройки портов

Команда консоли	Описание
<code>interface ethernet <i>интерфейс</i></code>	Включает режим настройки интерфейса для настройки типа интерфейса Ethernet.
<code>description <i>строка</i></code>	Добавляет описание в конфигурацию интерфейса.
<code>shutdown</code>	Выключает интерфейсы, которые входят в состав текущего заданного контекста.
<code>set interface active {ethernet <i>интерфейс</i> port-channel <i>номер_канала_порта</i>}</code>	Вновь активизирует интерфейс, отключенный по причинам безопасности.
<code>speed <i>бит/с</i></code>	Настраивает скорость заданного интерфейса Ethernet, если не используется автоматическое согласование.
<code>autobaud</code>	Устанавливает автоматическое определение скорости канала.
<code>duplex {half full}</code>	Настраивает дуплексный или полудуплексный режим для заданного интерфейса Ethernet, если не используется автоматическое согласование.
<code>negotiation</code>	Включает автоматическое согласование для параметров скорости и дуплексного режима данного интерфейса.
<code>back-pressure</code>	Включает режим обратного давления для заданного интерфейса.
<code>flowcontrol {auto on off rx tx}</code>	Настраивает управление потоком для заданного интерфейса.
<code>mdi {on auto}</code>	Включает автоматическое использование перекрестного кабеля для заданного интерфейса или канала порта.
<code>show interfaces configuration [ethernet <i>интерфейс</i> port-channel <i>порт-канал-номер</i>]</code>	Отображает конфигурацию для всех настроенных интерфейсов.
<code>show interfaces status [ethernet <i>интерфейс</i> port-channel <i>порт-канал-номер</i>]</code>	Отображает состояние для всех настроенных интерфейсов.
<code>show interfaces description [ethernet <i>интерфейс</i> port-channel <i>порт-канал-номер</i>]</code>	Отображает описание для всех настроенных интерфейсов.

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		

Определение параметров LAG

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 портов в группы LAG см. в разделе [Объединение портов](#).

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


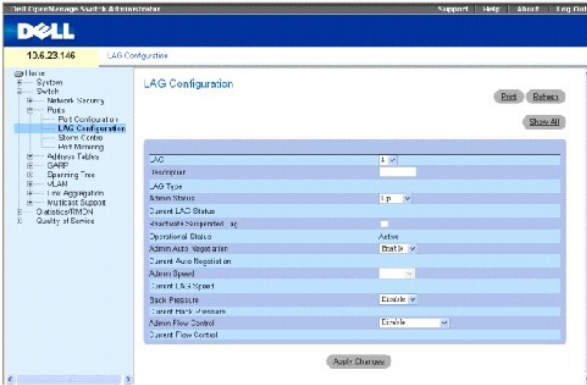
 **ПРИМЕЧАНИЕ.** Если конфигурация порта изменяется порт входит в группу LAG, изменения вступают в действие только после удаления порта из этой группы.

Рис. 7-90. Страница LAG Configuration (Настройка LAG)



LAG - номер группы LAG.

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 Back Pressure (Обратное давление) - включает или отключает режим обратного давления для группы LAG. Режим обратного давления поддерживается, если порты в группе LAG работают в полудуплексном режиме.

Current Back Pressure (Текущий режим обратного давления) - текущая настройка параметра режима обратного давления.

Admin Flow Control (Управление потоком) - включает или отключает управление потоком или включает автоматическое согласование управления потоком для LAG. Режим управления потоком поддерживается, если порты в группе LAG работают в дуплексном режиме.

Current Flow Control (Текущее управление потоком) - определяемая пользователем настройка управления потоком.

Определение параметров LAG

1. Откройте страницу [LAG Configuration](#) (Настройка LAG).
2. Выберите группу LAG в поле **LAG**.
3. 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. 7-91. Страница LAG Configuration Table (Таблица настройки LAG)

LAG Configuration Table

LAG	Description	LAG Type	LAG Status	LAG Speed	Auto Negotiation	Back Pressure	Flow Control
1		Up			Enable	Disable	Disable
2		Up			Enable	Disable	Disable
3		Up			Enable	Disable	Disable
4		Up			Enable	Disable	Disable
5		Up			Enable	Disable	Disable
6		Up			Enable	Disable	Disable
7		Up			Enable	Disable	Disable
8		Up			Enable	Disable	Disable

Настройка групп LAG с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для настройки групп LAG, как показано на странице [LAG Configuration](#) (Настройка LAG).

Таблица 7-54. Команды консоли для настройки LAG

Команда консоли	Описание
<code>interface port-channel номер_канала_порта</code>	Включает режим настройки интерфейса для указанного канала-порта.
<code>description строка</code>	Добавляет описание в конфигурацию интерфейса.
<code>shutdown</code>	Выключает интерфейсы, которые входят в состав текущего заданного контекста.
<code>speed бит/с</code>	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 порт-канал-номер]	Отображает конфигурацию для всех настроенных интерфейсов.
show interfaces status [ethernet интерфейс port-channel порт-канал-номер]	Отображает состояние для всех настроенных интерфейсов.
show interfaces description [ethernet интерфейс port-channel порт-канал-номер]	Отображает описание для всех настроенных интерфейсов.
show interfaces port-channel [номер_канала_порта]	Выводит сведения о канале порта (какие порты входят в канал порта, активны они на данный момент или нет).

Далее приведен пример команд консоли.

<pre> 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 </pre>	
<pre> console# show interfaces port-channel </pre>	
Channel	Ports
-----	-----
ch1	Inactive: g(21-24)
ch2	Active: g5
ch3	

ch4	
ch5	
ch6	
ch7	
ch8	
console#	

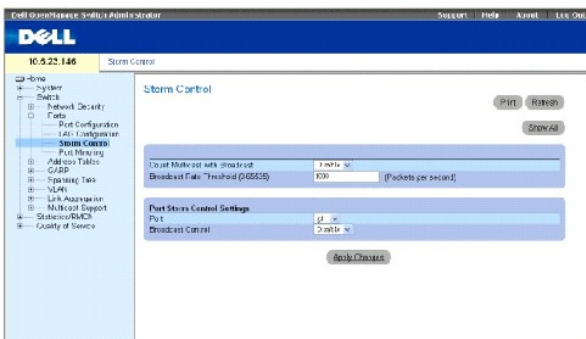
Включение контроля «лавины»

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 широковещательно 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. 7-92. Страница Storm Control (Контроль «лавины»)



Count Multicast with Broadcast (Подсчитывать многоадресные и широковещательные) - выполняется подсчет широковещательного и многоадресного трафика. Ниже указаны возможные значения.

- **Enable** (Включено) - выполняется подсчет широковещательного и многоадресного трафика.
- **Disable** (Отключено) - выполняется подсчет только широковещательного трафика.

Broadcast Rate Threshold (1-1000000) (Порог скорости широковещательных пакетов (1-1000000)) - максимальная скорость (в пакетах в секунду), при которой пересылаются неизвестные пакеты. Диапазон значений: 0-1000000. Значение по умолчанию: 0. Все значения округляются до 64 Кбит/с. Если значение поля меньше 64 Кбит/с, значение округляется до 64 Кбит/с, исключение составляет нулевое значение.

Port (Порт) - порт, для которого включен контроль «лавины».

Broadcast Control (Управление широковещательными передачами) - включает или отключает пересылку пакетов широковещательного типа на

устройство.

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.

Изменение параметров контроля «лавины» порта

1. Откройте [страницу Storm Control](#) (Контроль «лавины»).
2. Измените поля.
3. Нажмите кнопку **Show All** (Показать все).

Параметры контроля «лавины» порта будут сохранены для этого устройства.

Отображение таблицы параметров порта

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

Откроется страница [Storm Control Settings Table](#) (Таблица параметров контроля «лавины»):

Рис. 7-93. Таблица Storm Control Settings Table (Таблица параметров контроля «лавины»)

Port	Breakage Control
g1	Disable ▾
g2	Disable ▾
g3	Disable ▾
g4	Disable ▾
g5	Disable ▾
g6	Disable ▾
g7	Disable ▾
g8	Disable ▾
g9	Disable ▾
g10	Disable ▾
g11	Disable ▾
g12	Disable ▾
g13	Disable ▾
g14	Disable ▾
g15	Disable ▾
g16	Disable ▾
g17	Disable ▾
g18	Disable ▾
g19	Disable ▾
g20	Disable ▾
g21	Disable ▾
g22	Disable ▾
g23	Disable ▾
u24	Disable ▾

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 7-55. Команды консоли для настройки контроля «лавина»

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 «лавина».
port storm-control broadcast rate <i>скорость</i>	Настраивает максимальную скорость для широковещательных пакетов.
show ports storm-control [ethernet <i>интерфейс</i>]	Отображает конфигурацию контроля «лавина».

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:

Перед настройкой зеркалирования портов учтите следующее:

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

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

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

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

- 1 Порты-источники не могут входить в группу LAG.
- 1 Порты нельзя настроить в качестве портов назначения.
- 1 Все пакеты помечаются при их передаче из порта назначения.
- 1 Все пакеты 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.


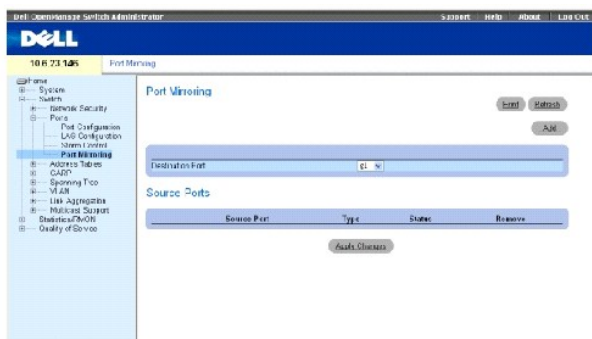
 **ПРИМЕЧАНИЕ.** Если порт выбран в качестве порта назначения для сеанса с зеркалированием портов, все обычные операции с ним откладываются. К ним относятся операции Spanning Tree и LACP.

Рис. 7-94. 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.

Тип (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.

Таблица 7-56. Команды консоли для настройки сеанса зеркалирования портов

Команда консоли	Описание
<code>port monitor <i>интерфейс_src</i> [rx tx]</code>	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

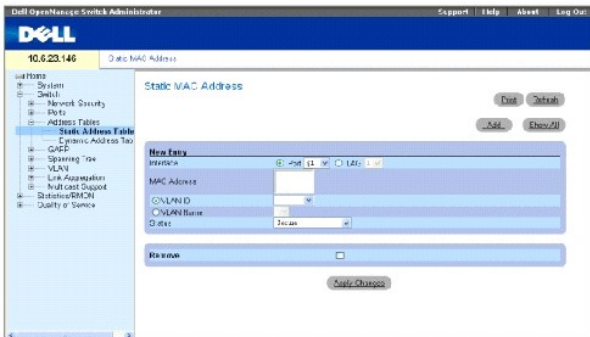
Настройка адресных таблиц

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 «лавинной» 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 (Таблицы 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](#) (Статические MAC-адреса), выберите Switch (Коммутатор) → Address Table (Таблицы адресов) → Static Address (Статические адреса) на панели дерева.

Рис. 7-95. Страница Static MAC Address (Статические MAC-адреса)



Interface (Интерфейс) - порт или группа LAG, для которых назначены статические MAC-адреса.

MAC Address (MAC-адрес) - список MAC-адрес в текущем списке статических адресов.

VLAN ID (Идентификатор сети VLAN) - номер группы VLAN, связанной с MAC-адресом.

VLAN Name (Имя сети VLAN) - имя сети VLAN, задаваемое пользователем.

Status (Состояние) - состояние MAC-адреса. Возможные значения:

Secure (Защищенный) - гарантирует, что MAC-адрес заблокированного порта не будет удален.

Permanent (Постоянный) - показывает, что MAC-адрес является постоянным.

Delete on Reset (Удаляется при перезагрузке) - показывает, что MAC-адрес удаляется при перезагрузке устройства.

Delete on Timeout (Удаляется по истечении времени ожидания) - показывает, что MAC-адрес удаляется по истечении времени ожидания.

Remove (Удалить) - когда этот флажок установлен, MAC-адрес удаляется из таблицы MAC-адресов.

Добавление статического MAC-адреса

1. Откройте страницу [Static MAC Address](#) (Статические MAC-адреса).
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](#) (Статические MAC-адреса).
2. Измените поля.
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Статический MAC-адрес будет изменен, а устройство обновлено.

Удаление статического адреса из таблицы статических адресов

1. Откройте страницу [Static MAC Address](#) (Статические MAC-адреса).
2. Нажмите кнопку **Show All** (Показать все).

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](#) (Статические MAC-адреса).

Таблица 7-57. Команды консоли настройки статических адресов

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

`bridge address mac-адрес { ethernet интерфейс | 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 интерфейс | 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

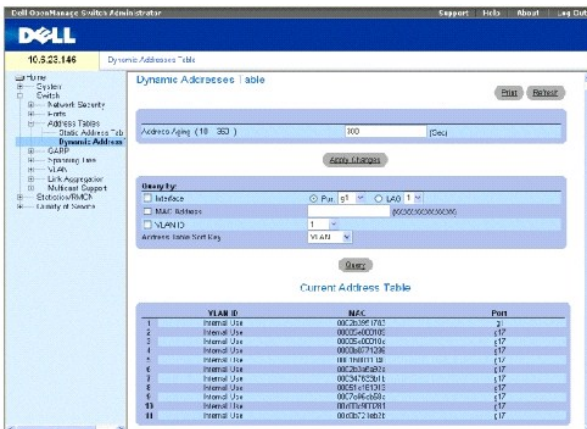
vlan	mac address	port	type
----	-----	----	-----
1	00:60:70:4C:73:FF	g8	dynamic
1	00:60:70:8C:73:FF	g8	dynamic
200	00:10:0D:48:37:FF	g9	static
g8	00:10:0D:98:37:88	g8	dynamic

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 содержит параметры для запросов и просмотра списка динамических адресов. Таблица текущих адресов содержит параметры динамических адресов, по которым пакеты передаются непосредственно на порты.

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

Рис. 7-96. Страница Dynamic Address Table (Таблица динамических адресов)



Address Aging (10-360) (Срок хранения адреса (10-360)) - 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) - идентификатор VLAN, для которой будет выполнен запрос по таблице.

Address Table Sort Key (Ключ для сортировки таблицы адресов) - определяет, по какому полю сортируется таблица динамических адресов.

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 раскрывающемся меню **Address Table Sort Key** (Ключ сортировки таблицы адресов) выберите поле, по которому будут отсортированы адреса - по адресу, идентификатору VLAN или интерфейсу.
3. Нажмите кнопку **Query** (Запрос).

[Dynamic Address Table](#) (Таблица динамических адресов) отсортирована.

Опрос и сортировка динамических адресов с помощью команд консоли

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

Таблица 7-58. Команд консоли для опроса и сортировка динамических адресов

Команда консоли	Описание
<code>bridge aging-time</code> <i>секунды</i>	Задаёт срок хранения для таблиц адресов.
<code>show bridge address-table</code> [<i>vlan vlan</i>] [<i>ethernet интерфейс</i> <i>port-channel номер_канала_порта</i>]	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:

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

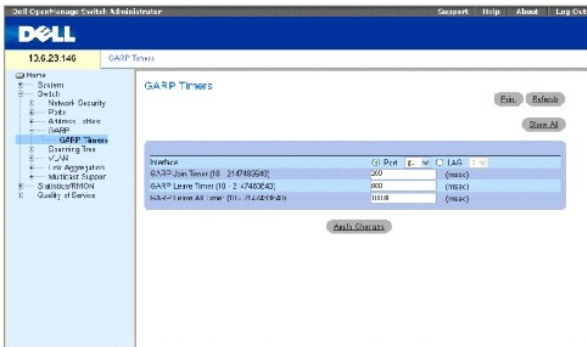
Устанавливает те же значения таймера GARP для всех устройств подключенных к уровню 2. Если таймеры GARP установлены по-разному на устройствах Layer 2, приложение GARP не сможет правильно работать.

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. 7-97. Страница GARP Timers (Таймеры GARP)



Interface (Интерфейс) - определяет, где включен таймер - для порта или группы LAG.

GARP Join Timer (10 - 2147483640) (Таймер соединения GARP (10 - 2147483640)) - показывает время в миллисекундах, когда передаются модули PDU. Возможные значения поля: 10-2147483640. Значение по умолчанию: 200 мсек.

GARP Leave Timer (10 - 2147483640) (Таймер отключения GARP (10 - 2147483640)) - 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 (10 - 2147483640)) - время (в миллисекундах), в течение которого 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 7-59. Команды консоли для определения таймеров GARP

Команда консоли	Описание
<code>garp timer {join leave leaveall} время</code>	Задаёт значения таймеров GARP для времени соединения, отключения и полного отключения приложений GARP.

Далее приведен пример команд консоли.

```

console(config)# interface ethernet 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:

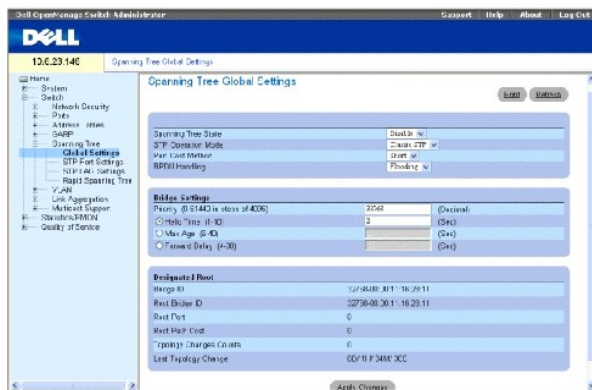
- 1 Classic STP (Классический STP) - обеспечивает единственный путь между конечными станциями сети и исключает циклы. Дополнительную информацию о настройке классического STP см. в разделе [«Определение общих параметров STP»](#).
- 1 Rapid STP (Быстрый STP) - выявляет и использует топологию сети, обеспечивая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

Чтобы открыть страницу 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. 7-98. Страница STP Global Settings (Общие параметры STP)



Spanning Tree State (Состояние Spanning Tree) - включает или отключает протокол STP для устройства. Ниже указаны возможные значения.

- o Enable (Включить) - включает протокол STP
- o 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.

Port Cost Method (Метод 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.

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) - оплавка пакетов BPDU «лавиной», если протокол Spanning Tree отключен для интерфейса. Это значение по умолчанию.

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 (4К). Например 0, 4096, 8192 и т.д.

Hello Time (1-10) (Интервал приветствия (1-10)) - 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 (6-40)) - 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 (4-30)) - 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 корневному 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.

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 7-60. Команды консоли для определения общих параметров протокола STP

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

Далее приведен пример команд консоли.

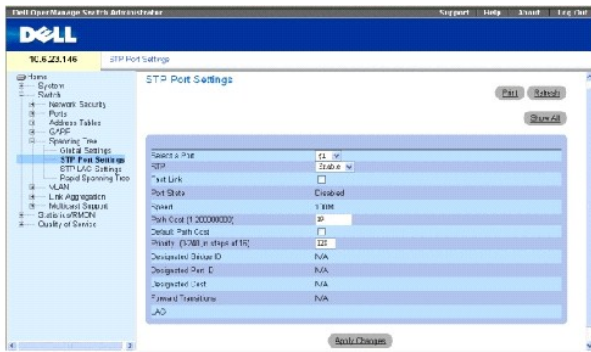
<pre>console(config)# spanning-tree console(config)# spanning-tree mode rstp console(config)# spanning-tree priority 12288 console(config)# spanning-tree hello-time 5 console(config)# spanning-tree max-age 15 console(config)# spanning-tree forward-time 25 console(config)# exit console# show spanning-tree Spanning tree enabled mode RSTP Default port cost method: short</pre>	
--	--

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 параметров STP для 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. 7-99. 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)** сразу после появления связи. Режим Fast Link (Быстрая связь) оптимизирует время, которое требуется протоколу STP для сходимости. Для сходимости протокола STP в больших сетях может потребоваться от 30 до 60 секунд.

Port State (Состояние порта) - показывает текущее состояние протокола STP для порта. Если этот параметр включен, он определяет, какое действие пересылки выполняется для трафика. Ниже перечислены возможные состояния порта.

Disabled (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.

Speed (Скорость) - скорость, на которой работает порт.

Path Cost (1-200000000) (Стоимость пути (1-200000000)) - 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 предоставляются 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 7-61. Команды консоли для определения параметров STP для порта

Команда консоли	Описание
<code>spanning-tree disable</code>	Отключение протокола STP на определенном порте.
<code>spanning-tree cost <i>стоимость</i></code>	Настройка стоимости пути для порта.
<code>spanning-tree port-priority <i>приоритет</i></code>	Настройка приоритета порта.
<code>spanning-tree portfast</code>	Включение режима PortFast.
<code>show spanning-tree [ethernet <i>интерфейс</i> port-channel <i>номер_канала_порта</i>]</code>	Отображение конфигурации протокола STP.

Далее приведен пример команд консоли.

<pre>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</pre>	
Port g5 disabled	
State: disabled	Role: disabled
Port id: 96.5	Port cost: 35000
Type: P2p (configured: Auto) STP	Port Fast: No (configured: No)
Designated bridge Priority : 32768	Address: 00:e8:00:b4:c0:00

```
Designated port id: 96.5
Designated path cost: 19

Number of transitions to forwarding
state: 0

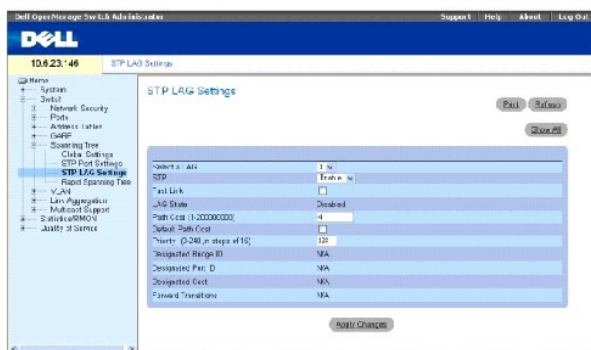
BPDUs: sent 0, received 0

console#
```

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. 7-100. Страница STP LAG Settings (Параметры STP для LAG)



Select a LAG (Выбор LAG) - группа LAG, определенная пользователем. Дополнительную информацию см. в разделе [«Определение членства в 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.

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 не правильно, и ее нельзя использовать для пересылки трафика.

Path Cost (1-200000000) (Стоимость пути (1-200000000)) - 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 (0-240, in steps of 16) (Приоритет от 0 до 240 с шагом 16) - 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 7-62. Команды консоли для определения параметров STP для LAG

Команда консоли	Описание
<code>spanning-tree</code>	Включает STP.
<code>spanning-tree disable</code>	Отключает протокол STP для определенной группы LAG.
<code>spanning-tree cost стоимость</code>	Настраивает стоимость пути для группы LAG.
<code>spanning-tree port-priority приоритет</code>	Настраивает приоритет порта.
<code>show spanning-tree [ethernet интерфейс port-channel</code>	Отображает конфигурацию протокола STP.

номер_канала_порта]	
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:

- 1 Disabled (Отключен)
- 1 Learning (Распознавание)
- 1 Discarding (Отбрасывание)
- 1 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. 7-101. 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).

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 7-63. Команды консоли для определения параметров Rapid STP

Команда консоли	Описание
<code>spanning-tree link-type { point-to-point shared }</code>	Переопределяет тип связи по умолчанию.
<code>spanning tree mode { stp rstp }</code>	Настраивает работающий в данный момент протокол STP.
<code>clear spanning-tree detected-protocols [ethernet интерфейс port-channel номер_канала_порта]</code>	Перезапускает процесс миграции протоколов.
<code>show spanning-tree [ethernet интерфейс port-channel номер_канала_порта]</code>	Отображение конфигурации протокола STP.

Далее приведен пример команд консоли.

```
Console(config)# interface ethernet g5

Console(config-if)# spanning-tree link-type shared
```


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.

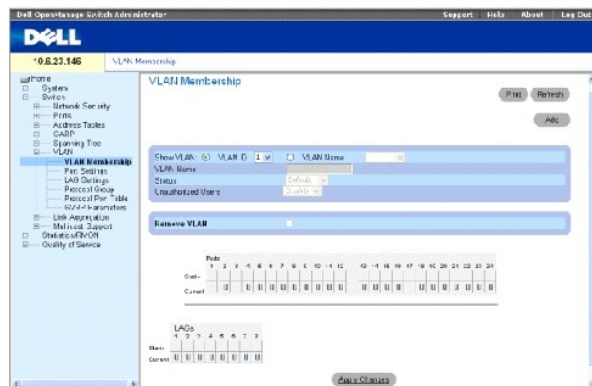
Сети VLAN работают на уровне Layer 2. Поскольку они изолируют трафик внутри себя, для обеспечения трафика между группами VLAN необходим маршрутизатор уровня Layer 3, поддерживающий соответствующий уровень протокола. Маршрутизаторы уровня Layer 3 идентифицируют сегменты и координируют их с сетями VLAN. 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.

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 к VLAN), выберите Switch (Коммутатор) → VLAN → VLAN Membership (Принадлежность к VLAN) на панели дерева.

Рис. 7-102. 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).

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 7-64. Команды консоли для определения принадлежности VLAN

Команда консоли	Описание
<code>vlan database</code>	Включает режим настройки интерфейса (VLAN).
<code>vlan {диапазон_vlan}</code>	Создает VLAN.
<code>name строка</code>	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 принадлежности 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 7-65. Таблица принадлежности портов VLAN

Управление портом	Описание
T	Интерфейс входит в VLAN. Все пакеты, пересылаемые интерфейсом, помечаются. Пакеты содержат информацию о VLAN.
U	Интерфейс входит в VLAN. Пакеты, пересылаемые интерфейсом, не помечаются.
F	Интерфейсу отказано в принадлежности VLAN.
Пусто	Интерфейс не входит в VLAN. Пакеты, связанные с интерфейсом, не пересылаются.

 **ПРИМЕЧАНИЕ.** Порты, входящие в LAG, не отображаются в таблице принадлежности портов VLAN.

В VLAN Port Membership Table (Таблица принадлежности портов VLAN) отображаются порты и состояния портов, а также группы LAG.

Назначение портов в группу VLAN

1. Откройте страницу VLAN Membership (Принадлежность VLAN).
2. Нажмите кнопку **VLAN ID** (Идентификатор VLAN) или **VLAN Name** (Имя VLAN) и выберите VLAN в раскрывающемся меню.
3. Выберите порт в **Port Membership Table** (Таблица 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 7-66. Команды консоли для назначения портов в группы VLAN

Команда консоли	Описание
<code>switchport general acceptable-frame-types tagged-only</code>	Отбрасывает входящие непомеченные кадры.
<code>switchport forbidden vlan {add список_сетей_vlan remove список_сетей_vlan}</code>	Запрещает добавление указанных VLAN для порта.
<code>switchport mode {access trunk general}</code>	Настраивает режим принадлежности VLAN для порта.
<code>switchport access vlan vlan-id</code>	Настраивает идентификатор порта VLAN, если интерфейс работает в режиме доступа.
<code>switchport trunk allowed vlan {add vlan-list remove vlan-list}</code>	Добавляет или удаляет группы VLAN из порта, работающего в режиме транк.
<code>switchport trunk native vlan идентификатор_vlan</code>	Определяет принадлежность порт указанной группе VLAN, а идентификатор VLAN как «идентификатор VLAN по умолчанию для порта (PVID)».
<code>switchport general allowed vlan add список_vlan [tagged untagged]</code>	Добавляет или удаляет группы VLAN из порта, работающего в общем режиме.
<code>switchport general pvid идентификатор_vlan</code>	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)# switchport 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

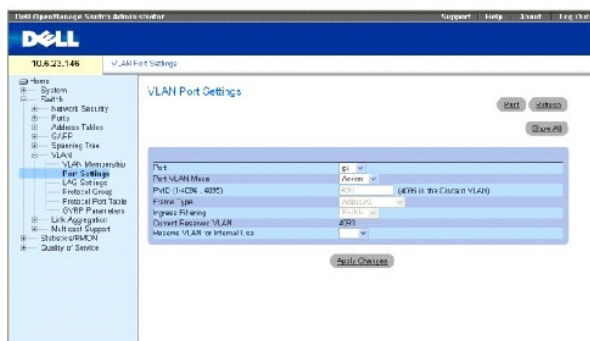
```

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 непоименованные пакеты, поступающие на устройство, маркируются идентификатором PVID портов.

Чтобы открыть страницу [VLAN Port Settings](#) (Параметры порта VLAN), выберите Switch (Коммутатор) → VLAN → Port Settings (Параметры порта) на панели дерева.

Рис. 7-103. 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).

PVID - 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).

Назначение портов в VLAN с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для назначения портов для групп VLAN.

Таблица 7-67. Команды консоли для назначения портов в группы VLAN

Команда консоли	Описание
switchport mode {access trunk general}	Настраивает режим принадлежности VLAN для порта.
switchport trunk native vlan <i>идентификатор_vlan</i>	Определяет принадлежность порт указанной группе VLAN, а идентификатор VLAN как «идентификатор VLAN по умолчанию для порта (PVID)».
switchport general pvid <i>идентификатор_vlan</i>	Настраивает идентификатор порта VLAN (PVID), если интерфейс работает в общем режиме.
switchport general allowed vlan add <i>список_vlan</i> [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 <i>интерфейс</i> port-channel <i>номер_канала_порта</i> }	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

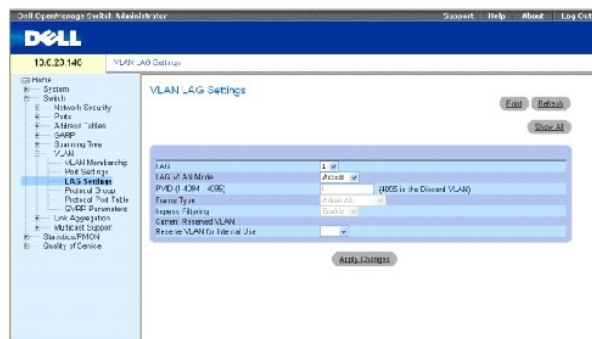
Console (config-if)# switchport general ingress-filtering disable

```

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. 7-104. 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 7-68. Команды консоли для назначения групп LAG VLAN

Команда консоли	Описание
switchport mode { access trunk general }	Настраивает режим принадлежности VLAN для порта.

<code>switchport trunk native vlan <i>идентификатор_vlan</i></code>	Определяет принадлежность порта указанной группе VLAN и идентификатор VLAN как «идентификатор порта по умолчанию VLAN (PVID)».
<code>switchport general pvid <i>идентификатор_vlan</i></code>	Настраивает идентификатор порта VLAN (PVID), если интерфейс работает в общем режиме.
<code>switchport general allowed vlan add <i>список_vlan</i> [tagged untagged]</code>	Добавляет или удаляет группы VLAN из порта, работающего в общем режиме.
<code>switchport general acceptable-frame-type tagged-only</code>	Отбрасывает непомеченные входящие пакеты.
<code>switchport general ingress-filtering disable</code>	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

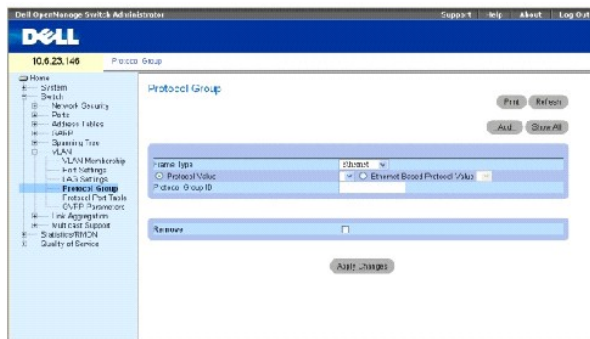
```

```
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. 7-105. Группа протоколов



Frame Type (Тип кадра) - тип пакетов. Возможные значения поля: **Ethernet**, **RFC1042** и **LLC Other**.

Protocol Value (Значение протокола) - определенное пользователем имя протокола.

Ethernet-Based Protocol Value - тип группы протокола Ethernet. 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 7-69. Команды консоли для определения групп протоколов VLAN

Команда консоли	Описание
<code>map protocol <i>протокол</i> [<i>encapsulation</i>] protocols-group <i>группа</i></code>	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»:

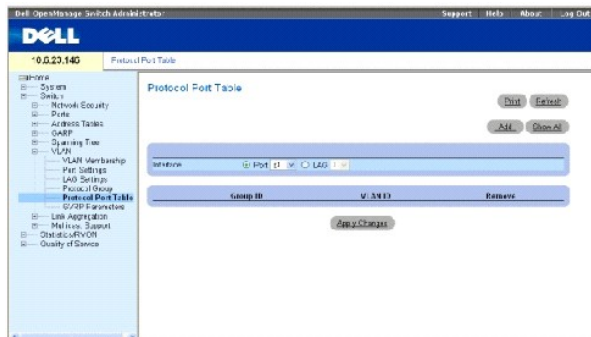
```
Console (config)# vlan
database

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. 7-106. 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 (1-4095)) - 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.

 **ПРИМЕЧАНИЕ.** VLAN 4095 - это игнорируемая сеть VLAN.

Добавление нового порта протокола

 **ПРИМЕЧАНИЕ.** 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 7-70. Команды консоли для определение портов протокола

Команда консоли	Описание
<code>switchport general map protocols-group группа vlan идентификатор_vlan</code>	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:

- 1 количества всех статических групп VLAN, настроенных на данный момент или ожидающих настройки;
- 1 количества всех динамических VLAN, входящих в протокол GVRP, настроенных на данный момент (начальное количество динамических сетей VLAN с протоколом GVRP равно 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. 7-107. 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 7-71. Команды консоли для настройки общих параметров протокола GVRP

Команда консоли	Описание
<code>gvrp enable (global)</code>	Включает протокол GVRP для системы в целом.
<code>gvrp enable (interface)</code>	Включает протокол GVRP для интерфейса.
<code>gvrp vlan-creation-forbid</code>	Включает или отключает динамическое создание VLAN.
<code>gvrp registration-forbid</code>	Отменяет регистрацию всех динамических сетей VLAN и предотвращает динамическую регистрацию VLAN для порта.
<code>show gvrp configuration [ethernet интерфейс port-channel порт-канал-номер]</code>	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.
<code>show gvrp error-statistics [ethernet интерфейс port-channel порт-канал-номер]</code>	Отображает статистику ошибок протокола GVRP.
<code>show gvrp statistics [ethernet интерфейс port-channel порт-канал-номер]</code>	Отображает статистику протокола GVRP.
<code>clear gvrp statistics [ethernet интерфейс port-channel порт-канал-номер]</code>	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

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:

- 1 Для порта не определен интерфейс уровня Layer 3.
- 1 Порт не принадлежит ни одной группе VLAN.
- 1 Порт не принадлежит ни одной другой группе LAG.
- 1 Порт не является дублированным портом.
- 1 Приоритет 802.1p порта равен приоритету 802.1p групп LAG.
- 1 Режим доверия QoS не отключен на этом порте.
- 1 Не включен протокол GVRP.



ПРИМЕЧАНИЕ. 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.

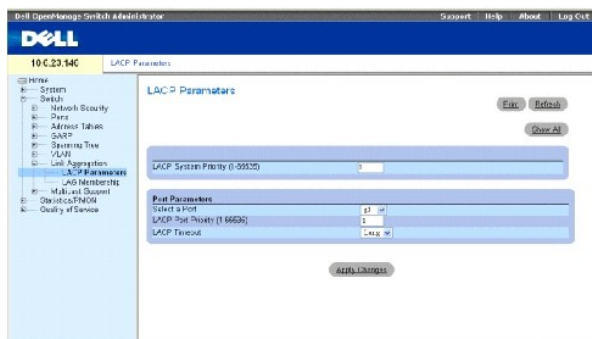
Каждый объединенный канал, включая порты Gigabit Ethernet, имеет тип порта объединенного канала. Порты могут быть добавлены в объединенный канал, только если они имеют одинаковый тип. Когда порты удаляются из объединенных портов, для них восстанавливаются первоначальные настройки. Чтобы открыть страницу **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. 7-108. 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 (Короткая) - определяет малое время ожидания.

Long (Длинная) - определяет большое время ожидания.

Определение общих параметров объединенных каналов

1. Откройте страницу [LACP Parameters](#) (Параметры LACP).
2. Укажите значение 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 7-72. Команды консоли для настройки параметров LACP

Команда консоли	Описание
<code>lACP system-priority значение</code>	Настраивает приоритет системы.
<code>lACP port-priority значение</code>	Настраивает приоритет физических портов.
<code>lACP timeout {long short}</code>	Задаёт административный тайм-аут LACP.
<code>show lACP ethernet интерфейс [parameters statistics protocol-state]</code>	Отображает информацию о протоколе LACP для 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

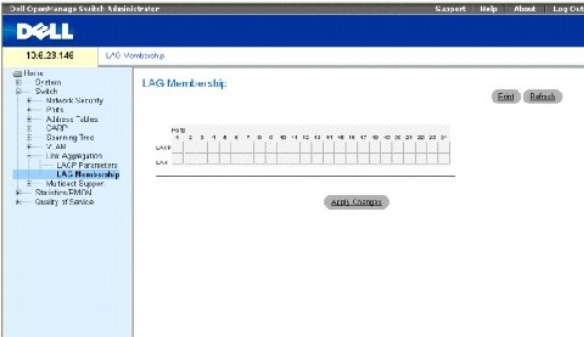
LACP PDUs received:2
```

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](#) (Членство в LAG), выберите **Switch** (Коммутатор) → **Link Aggregation** (Объединение каналов) → **LAG Membership** (Членство в LAG) на панели дерева.

Рис. 7-109. 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 в LAG).
2. В строке LAG (вторая) 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](#) (Членство в LAG).

Таблица 7-73. Команды консоли для определения принадлежности LAG

Команда консоли	Описание
<code>interface port-channel номер_канала_порта</code>	Включает режим настройки интерфейса для указанного канала-порта.
<code>channel-group номер_канала_порта mode {on auto}</code>	Связывает порт с каналом порта. Для удаления конфигурации группы канала из интерфейса используйте форму по этой команды.
<code>show interfaces port-channel [номер_канала_порта]</code>	Отображает информацию о канале порта.

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: chl


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:

- 1 Forwarding L2 Multicast Packets (Пересылка многоадресных пакетов L2) - включена по умолчанию и не настраивается.

 **ПРИМЕЧАНИЕ.** Система поддерживает фильтр многоадресной передачи для 63 групп многоадресной передачи.

- 1 Filtering L2 Multicast Packets (Фильтрация многоадресных пакетов L2) - включает пересылку пакетов Layer 2 на интерфейсы. Если фильтрация многоадресного трафика отключена, многоадресные пакеты «лавиной» рассылаются на все соответствующие порты.

Чтобы открыть страницу **Multicast Support** (Поддержка многоадресного трафика), выберите **Switch** (Коммутатор) → **Multicast Support** (Поддержка многоадресного трафика) на панели дерева.

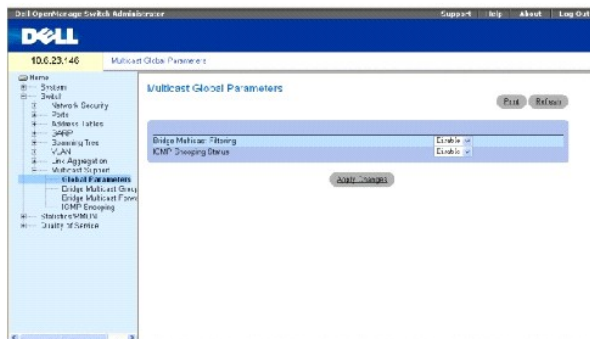
Определение общих параметров многоадресной передачи

Переключение Layer 2 пересылает многоадресные пакеты на все соответствующие порты VLAN по умолчанию, 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, выдают 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. 7-110. 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 включено 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 7-74. 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

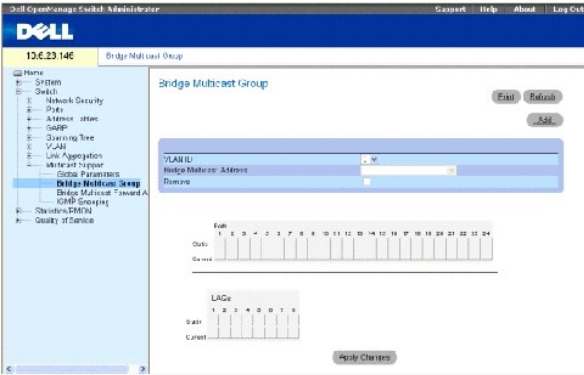
Console (config)# ip igmp
snooping
```

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. 7-111. Страница Bridge Multicast Group (Группа многоадресной передачи моста)



VLAN ID (Идентификатор VLAN) - определяет VLAN и содержит информацию об адресе группы многоадресной передачи.

Bridge Multicast Address (Адрес многоадресной передачи моста) - идентифицирует MAC/IP-адрес группы многоадресной передачи.

Remove (Удалить) - когда установлен этот флажок, адрес многоадресной передачи моста удаляется.

Ports (Порты) - порты, которые можно добавить в службу многоадресной передачи.

LAGs (Группы LAG) - группы LAG, которые можно добавить в службу многоадресной передачи.

В следующей таблице приведены параметры управления записями портов и групп LAG для IGMP:

Таблица 7-75. Параметры управления таблицей записей портов/LAG для IGMP

Управление портом	Описание
D	Показывает, что порт/группа LAG добавлена в группу многоадресной передачи динамически в строке <i>Current</i> (Текущий).
S	Связывает порт с многоадресной группой в качестве статического члена в строке <i>Static</i> (Статический). Порт/группа LAG присоединена к многоадресной группе статически в строке <i>Current</i> (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. 7-112. Страница Add Bridge Multicast Group (Добавление группы многоадресной передачи моста)

Add Bridge Multicast Group

Введите ID

Новый мост F Multicast: (XX:XX)

Новый мост Mac Multicast: (XX:XX:XX:XX:XX:XX)

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

Static: Current:

LAGs: 1 2 3 4 5 6 7 8

Static: Current:

Apply Changes

3. Определите поля **VLAN ID** (Идентификатор VLAN) и **New Bridge Multicast Address** (Новый адрес многоадресной передачи моста).
4. Переключите порт на значение **S**, чтобы добавить его в выбранную группу многоадресной передачи.
5. Переключите порт на значение **F**, чтобы запретить добавление определенных адресов многоадресной передачи для определенного порта.
6. Нажмите кнопку **Apply Changes** (Применить изменения).

Адрес многоадресной передачи моста будет добавлен в многоадресную группу, а устройство обновлено.

Определение портов для получения службы многоадресной пересылки

1. Откройте страницу [Bridge Multicast Group](#) (Группа многоадресной передачи моста).
2. Определите поля **VLAN ID** (Идентификатор VLAN) и **Bridge Multicast Address** (Адрес многоадресной передачи моста).
3. Переключите порт на значение **S**, чтобы добавить его в выбранную группу многоадресной передачи.
4. Переключите порт на значение **F**, чтобы запретить добавление определенных адресов многоадресной передачи для определенного порта.
5. Нажмите кнопку **Apply Changes** (Применить изменения).

Порт будет назначен в группу многоадресной передачи, а устройство обновлено.

Назначение групп LAG для получения службы многоадресной пересылки

1. Откройте страницу [Bridge Multicast Group](#) (Группа многоадресной передачи моста).
2. Определите поля **VLAN ID** (Идентификатор VLAN) и **Bridge Multicast Address** (Адрес многоадресной передачи моста).
3. Переключите LAG на значение **S**, чтобы добавить его в выбранную группу многоадресной передачи.
4. Переключите LAG на значение **F**, чтобы запретить добавление определенных адресов многоадресной передачи для определенной группы LAG.
5. Нажмите кнопку **Apply Changes** (Применить изменения).

Группа LAG будет назначена в группу многоадресной передачи, а устройство обновлено.

Управление записями службы многоадресной пересылки с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для управления записями службы многоадресной пересылки, как показано на странице [Bridge Multicast Group](#) (Группа многоадресной передачи моста).

Таблица 7-76. Команды консоли для управления записями службы многоадресной пересылки

Команда консоли	Описание
<code>bridge multicast address { mac_адрес_многоадресной_передачи ip_адрес_многоадресной_передачи }</code>	Регистрирует адреса для многоадресной передачи на уровне MAC-адресов для таблицы мостов и добавляет в группу статические порты.
<code>bridge multicast forbidden address { mac_адрес_многоадресной_передачи ip_адрес_многоадресной_передачи } [add remove] { ethernet список_интерфейсов </code>	Запрещает добавление определенного адреса многоадресной передачи для определенных портов. Для

<code>port-channel</code> <i>список_номеров_каналов_портов</i>)	возврата к значениям по умолчанию используйте форму по этой команды
<code>show bridge multicast address-table</code> [<i>vlan vlan-id</i>] [<i>address mac_адрес_многоадресной_передачи ip_адрес_многоадресной_передачи</i>] [<i>format ip mac</i>]	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

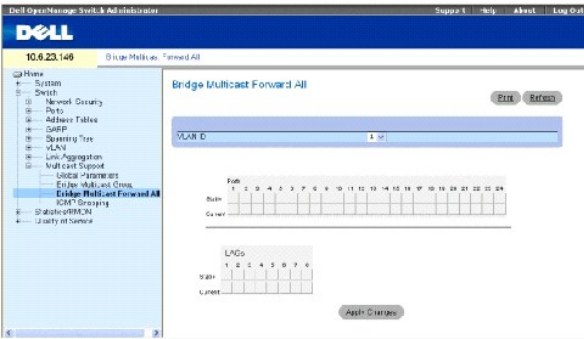
19	0100.5e02.0208	static	g1-8
19	0100.5e02.0208	dynamic	g9-11
Forbidden ports for multicast addresses:			
Vlan	MAC Address	Ports	
----	-----	-----	
1	0100.5e02.0203	g8	
19	0100.5e02.0208	g8	
Console # show bridge multicast address-table format ip			
Vlan	IP Address	Type	Ports
----	-----	-----	-----
1	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. 7-113. Страница Bridge Multicast Forward All (Мост для многоадресной пересылки 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 [Bridge Multicast Forward All Router/Port Control Settings Table](#) (Таблица параметров управления маршрутизатором/портами для многоадресной передачи моста всем) приведены параметры управления настройками маршрутизатора и портов.

Таблица 7-77. Таблица параметров управления маршрутизатором/портами для многоадресной передачи моста всем

Управление портом	Описание
D	Связывает порт с многоадресным маршрутизатором или коммутатором как динамический порт.
S	Связывает порт с многоадресным маршрутизатором или коммутатором как статический порт.
F	Запрещено.
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](#) (Мост для многоадресной пересылки 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](#) (Мост для многоадресной пересылки 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 7-78. Команды консоли для управления группами LAG и портами, привязанными к маршрутизаторам многоадресной передачи

Команда консоли	Описание
<code>show bridge multicast filtering <i>идентификатор_vlan</i></code>	Отображает настройку фильтра многоадресной передачи.
<code>no bridge multicast forbidden forward-all</code>	Запрещает пересылку многоадресных пакетов для порта.
<code>bridge multicast forward-all {add remove} {ethernet <i>список_интерфейсов</i> port-channel <i>список_номеров_каналов_портов</i>}</code>	Разрешает пересылку всех многоадресных пакетов для порта. Для возврата к значениям по умолчанию используйте форму по этой команды

Далее приведен пример команд консоли.

```

console(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

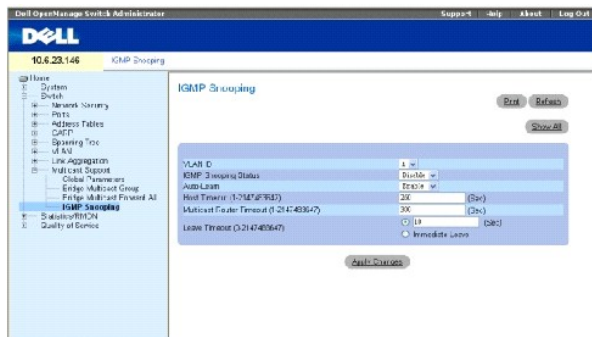
```

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. 7-114. Наблюдение по протоколу IGMP



VLAN ID (Идентификатор сети VLAN) - указывает идентификатор VLAN.

IGMP Snooping Status (Состояние наблюдения по протоколу IGMP) - включает или отключает наблюдение по протоколу IGMP для VLAN.

Auto Learn (Автоматическое распознавание) - включает или отключает автоматическое распознавание на устройстве.

Host Timeout (1-2147483647) (Время ожидания хоста (1-2147483647)) - время, по истечении которого запись наблюдения по протоколу IGMP устаревает. Значение по умолчанию: 260 секунд.

Multicast Router Timeout (1-2147483647) (Время ожидания многоадресного маршрутизатора (1-2147483647)) - время, по истечении которого запись многоадресного маршрутизатора устаревает. Значение по умолчанию: 300 секунд.

Leave Timeout (0-2147483647) (Время старения (0-2147483647)) - 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).

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 7-79. Команды консоли для настройки наблюдения по протоколу IGMP

Команда консоли	Описание
<code>ip igmp snooping</code>	Включает наблюдение по протоколу IGMP.
<code>ip igmp snooping mrouter learn-pim-dvmrp</code>	Включает автоматическое распознавание портов многоадресного маршрутизатора в контексте определенной VLAN.
<code>ip igmp snooping host-time-out количество_секунд</code>	Настраивает время ожидания хоста.
<code>ip igmp snooping mrouter-time-out количество_секунд</code>	Настраивает время ожидания маршрутизатора.
<code>ip igmp snooping leave-time-out {time-out immediate-leave}</code>	Настраивает время старения хоста.
<code>show ip igmp snooping groups [vlan идентификатор_vlan] [address ip_адрес_многоадресной_передачи]</code>	Отображает группы многоадресной передачи, полученные во время наблюдения по протоколу IGMP.
<code>show ip igmp snooping interface идентификатор_vlan</code>	Отображает конфигурацию наблюдения по протоколу IGMP
<code>show ip igmp snooping mrouter [interface идентификатор_vlan]</code>	Отображает информацию о динамически распознаваемых интерфейсах многоадресного маршрутизатора.

Далее приведен пример команд консоли.

```
Console> 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 1

IGMP Snooping is globally enabled

IGMP Snooping is enabled on VLAN 1

IGMP host timeout is 300 sec
```

IGMP Immediate leave is disabled. IGMP leave timeout is 60 sec

IGMP mrouter timeout is 200 sec

Automatic learning of multicast router ports is enabled

Console # **show ip igmp snooping mrouter**

VLAN	Ports
----	-----
1	g1

[Назад на страницу «Содержание»](#)

[Назад на страницу содержания](#)

Информация о настройке системы

Руководство пользователя системы Dell™ PowerConnect™ 5324

- [Определение общих сведений об устройстве](#)
- [Настройка параметров SNMP](#)
- [Управление журналами](#)
- [Определение IP-адресов устройств](#)
- [Запуск диагностики кабелей](#)
- [Управление безопасностью устройств](#)
- [Определение параметров SNMP](#)
- [Управление файлами](#)
- [Определение расширенных параметров](#)

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), выберите System (Система) на панели дерева.



Рис. 6-15. Страница System (Система)

Определение общих сведений об устройстве

Страница General (Общее) содержит ссылки на страницы, позволяющие настраивать параметры устройства.

Просмотр страницы Asset (Ресурсы)

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), выберите System (Система) → General (Общие) → Asset (Ресурсы) на панели дерева.



Рис. 6-16. Страница Asset (Ресурсы)

System Name (0-160 Characters) (Имя системы (от 0 до 160 символов)) - определенное пользователем имя устройства.

System Contact (0-160 Characters) (Контактное лицо системы (от 0 до 160 символов)) - определяет имя контактного лица.

System Location (0-160 Characters) (Местоположение системы (от 0 до 160 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/MM/YY) (Дата (ДД/ММ/ГГ)) - определяет системную дату. Формат этого поля: месяц, день, год. Например, 11/10/02 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. Щелкните **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).

Таблица 6-11. Команды консоли для настройки ресурсов

Команда консоли	Описание
hostname имя	Указывает или изменяет имя хоста устройства.
snmp-server contact текст	Задаёт контактные сведения для системы.
snmp-server location текст	Вводит сведения о местонахождении устройства.
show clock [detail]	Отображает системное время и дату.
show system id	Выводит информацию метки производителя
show system	Отображает информацию о системе.
asset-tag	Определяет метку 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 lqwepot

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:		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 5324		
Power Supply	Status	
-----	-----	
Main	OK	
Redundant	OK	
FAN	Status	
-----	-----	
1	OK	
2	OK	
DELL Switch#		

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:

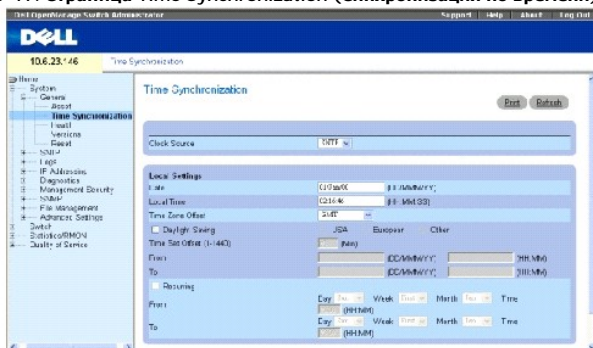
- 1 Австралия - с конца октября по конец марта.
- 1 Австралия - Тасмания - с начала октября по конец марта.
- 1 Австрия - с последних выходных марта по последние выходные октября.
- 1 Албания - с последних выходных марта по последние выходные октября.
- 1 Армения - с последних выходных марта по последние выходные октября.
- 1 Багамские о-ва - с апреля по октябрь, в сочетании с часами летнего времени США.
- 1 Белоруссия - с последних выходных марта по последние выходные октября.
- 1 Бельгия - с последних выходных марта по последние выходные октября.
- 1 Бразилия - с 3-его воскресенья октября по 3-его воскресенье марта. В течение периода перехода на летнее время часы в Бразилии переводятся на один час вперед в большинстве областей юго-востока Бразилии.
- 1 Великобритания - с последних выходных марта по последние выходные октября.
- 1 Венгрия - с последних выходных марта по последние выходные октября.

- 1 Германия - с последних выходных марта по последние выходные октября.
- 1 Греция - с последних выходных марта по последние выходные октября.
- 1 Дания - с последних выходных марта по последние выходные октября.
- 1 Египет - с последней пятницы апреля по последний четверг сентября.
- 1 Эстония - с последних выходных марта по последние выходные октября.
- 1 Израиль - в разные годы по-разному.
- 1 Индия - Индия не переходит на летнее время.
- 1 Иордания - с последних выходных марта по последние выходные октября.
- 1 Ирак - с 1-го апреля по 1-е октября.
- 1 Иран - с 21-го марта по 23-е сентября.
- 1 Ирландия - с последних выходных марта по последние выходные октября.
- 1 Испания - с последних выходных марта по последние выходные октября.
- 1 Италия - с последних выходных марта по последние выходные октября.
- 1 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.
- 1 Китай - Китай не переходит на летнее время.
- 1 Кипр - с последних выходных марта по последние выходные октября.
- 1 Куба - с последнего воскресенья марта по последнее воскресенье октября.
- 1 Латвия - с последних выходных марта по последние выходные октября.
- 1 Ливан - с последних выходных марта по последние выходные октября.
- 1 Литва - с последних выходных марта по последние выходные октября.
- 1 Люксембург - с последних выходных марта по последние выходные октября.
- 1 Македония - с последних выходных марта по последние выходные октября.
- 1 Мексика - с первого воскресенья апреля в 02:00 по последнее воскресенье октября в 02:00.
- 1 Молдавия - с последних выходных марта по последние выходные октября.
- 1 Нидерланды - с последних выходных марта по последние выходные октября.
- 1 Новая Зеландия - с первого воскресенья октября по первое воскресенье 15-го марта или после этой даты.
- 1 Норвегия - с последних выходных марта по последние выходные октября.
- 1 Финляндия - с последних выходных марта по последние выходные октября.
- 1 Франция - с последних выходных марта по последние выходные октября.
- 1 Парагвай - с 6-го апреля по 7-е сентября.
- 1 Польша - с последних выходных марта по последние выходные октября.
- 1 Португалия - с последних выходных марта по последние выходные октября.
- 1 Россия - с 29-го марта по 25-е октября.
- 1 Румыния - с последних выходных марта по последние выходные октября.
- 1 Сербия - с последних выходных марта по последние выходные октября.
- 1 Сирия - с 31-го марта по 30-ое октября.
- 1 Словацкая республика - с последних выходных марта по последние выходные октября.
- 1 США - с первого воскресенья апреля в 02:00 по последнее воскресенье октября в 02:00.
- 1 Тайвань - Тайвань не переходит на летнее время.
- 1 Турция - с последних выходных марта по последние выходные октября.
- 1 Черногория - с последних выходных марта по последние выходные октября.
- 1 Чили - о-в Пасхи с 9-го марта по 12-е октября. Первое воскресенье марта или после 9-го марта.
- 1 Швейцария - с последних выходных марта по последние выходные октября.
- 1 Швеция - с последних выходных марта по последние выходные октября.
- 1 ЮАР - ЮАР не переходит на летнее время.
- 1 Япония - Япония не переходит на летнее время.

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

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

Рис. 6-17. Страница Time Synchronization (Синхронизация по времени)



Clock Source (Источник синхронизации)

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

SNTP - определяет, что системное время будет установлено через сервер SNTP. Дополнительную информацию см. в разделе [«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 на основе местоположения устройства. Возможные значения:

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

European (Европейское) - устройство переключается на летнее время в 1:00 ночи в последнее воскресенье марта и переключается на стандартное время в 1:00 ночи в последнее воскресенье октября. 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: день, месяц, год, в одном поле и время в другом поле. Например, если действие летнего времени должно закончиться 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, 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, в которую каждый год выполняется переход на летнее время. Возможные значения поля: 1-5.

Month (Месяц) - месяц, в который 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 которую 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. Определите значение поля Clock Source (Источник синхронизации).
3. Нажмите кнопку Apply Changes (Применить изменения).

Будет выбран источник синхронизации, а устройство обновлено.

Определение параметров локальных часов

1. Откройте страницу [Time Synchronization](#) (Синхронизация по времени).
2. Определите поля 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. Определите поля.
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 6-12. Команды консоли для определения параметров часов

Команда консоли	Описание
clock source {sntp}	Определяет внешний источник времени для системных часов.
clock timezone <i>разница_в_часах</i> [<i>minutes разница_в_минутах</i>][<i>zone сокращение</i>]	Устанавливает часовой пояс для отображения.
clock summer-time	Настраивает в системе автоматическое переключение на летнее время.
clock summer-time recurring {usa eu { <i>день недели</i> <i>месяц</i> <i>чч:мм</i> <i>день недели</i> <i>месяц</i> <i>чч:мм</i> }} [<i>offset разница</i>][<i>zone сокращение</i>]	Настраивает систему для автоматического переключения на летнее время (в соответствии со стандартами США и европейскими стандартами).
clock summer-time date <i>дата</i> <i>месяц</i> <i>год</i> <i>чч:мм</i> <i>дата</i> <i>месяц</i> <i>год</i> <i>чч:мм</i> [<i>offset разница</i>][<i>zone сокращение</i>]	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), выберите System (Система)→ General (Общие)→ Health (Состояние) на панели дерева.

Рис. 6-18. Страница System Health (Состояние системы)




Power Supply Status (Состояние источника питания) - отображает 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 неправильно работают.

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 6-13. Команды консоли для просмотра состояния системы

Команда консоли	Описание
show system	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 5324		
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 используемых устройствах и версиях программного обеспечения. Чтобы открыть страницу [Versions](#) (Версии), выберите System (Система)→ General (Общие)→ Versions (Версии) на панели дерева.

Рис. 6-19. Страница Versions (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 6-14. Команды консоли для отображения версий

Команда консоли	Описание
show version	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)

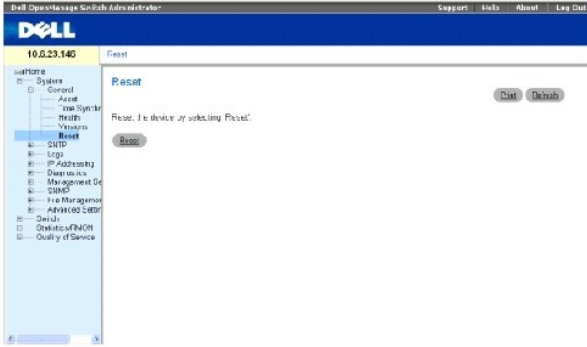
HW version x.x.x

```

Восстановление заводских параметров устройства

Страница [Reset](#) (Сброс) позволяет удаленно произвести сброс устройства и восстановить заводские параметры устройства. Чтобы открыть страницу [Reset](#) (Сброс), выберите System (Система) → General (Общие) → Reset (Сброс) на панели дерева.

Рис. 6-20. Страница Reset (Сброс)



ПРИМЕЧАНИЕ. Прежде чем выполнять сброс устройства, сохраните все изменения в файле Running Configuration (Рабочая конфигурация). Это позволит сохранить текущую конфигурацию устройства. Подробности о сохранении файлов конфигурации см. в разделе [«Управление файлами»](#).

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 команды консоли для восстановления параметров устройства с помощью команд консоли:

Таблица 6-15. Команды консоли для восстановления параметров устройства

Команда консоли	Описание
reload	Перезагружает операционную систему.

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 SNMP

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:

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

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

Далее приведен пример уровней:

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

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

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

- 1 **T1** - время, когда был послан исходный запрос клиентом.
- 1 **T2** - время, когда исходный запрос был получен сервером.
- 1 **T3** - время, когда сервер отправил ответ клиенту.
- 1 **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.

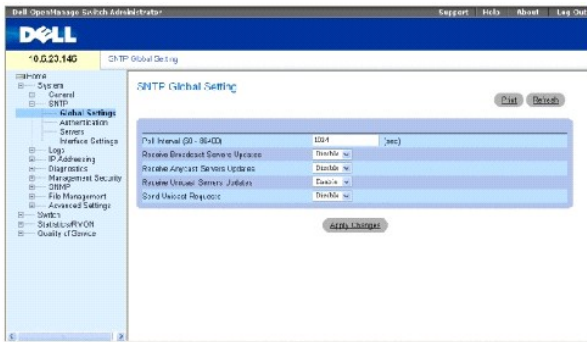
Проверка подлинности MD5 (Message Digest 5) обеспечивает синхронизацию линий связи коммутатора с серверами SNTP. MD5 - это алгоритм, создающий 128-разрядную хеш-строку. MD5 является разновидностью алгоритма MD4, который обеспечивает большую безопасность по сравнению с MD4. MD5 проверяет целостность передаваемых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

Щелкните **System** (Система)→ **SNTP** на панели дерева, 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), выберите System (Система) → SNTP → SNTP Global Settings (Общие параметры SNTP) на панели дерева.

Рис. 6-21. Страница SNTP Global Settings (Общие параметры SNTP)



Poll Interval (60-86400) (Интервал запроса (60-86400)) - 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 команды консоли для настройки полей, отображаемых на странице SNTP Global Settings (Общие параметры SNTP).

Таблица 6-16. Определение общих параметров SNTP с помощью команд консоли

Команда консоли	Описание
sntp broadcast client enable	Включает клиентов широковещательной передачи SNTP
sntp unicast client enable	Включает клиентов одноадресной передачи SNTP

Далее приведен пример команд консоли.

```
console> enable
```

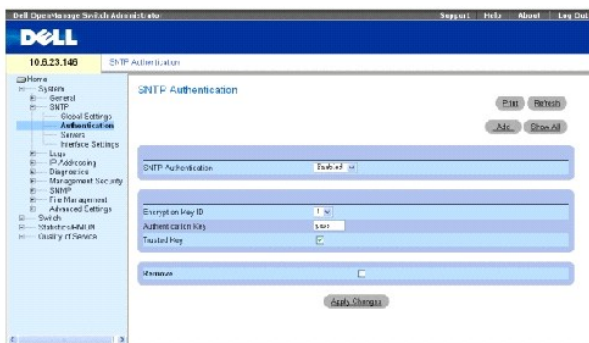
```
console# configure

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

Определение методов проверки подлинности SNMP

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

Рис. 6-22. Страница **SNTP Authentication** (Проверка подлинности SNMP)



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

Encryption Key ID (Идентификатор ключа шифрования) - определяет идентификатор ключа, который используется для проверки подлинности сервера SNMP 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 SNMP.

Remove (Удалить) - когда этот флажок установлен, выбранный ключ удаляется.

Добавление ключа проверки подлинности SNMP

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

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

Рис. 6-23. Страница **Add Authentication Key** (Добавление ключа проверки подлинности)

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

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

Отображение таблицы ключей проверки подлинности

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

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

Рис. 6-24. Страница Authentication Key Table (Таблица ключей проверки подлинности)

Encryption Key ID	Authentication Key	Trusted Key	Remove
1	1	md5	<input checked="" type="checkbox"/>

Удаление ключа проверки подлинности

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

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

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

Запись будет удалена, а устройство обновлено.

Определение параметров проверки подлинности SNMP с помощью команд консоли

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

Таблица 6-17. Команды консоли для проверки подлинности SNMP

Команда консоли	Описание
<code>sntp authenticate</code>	Определяет проверку подлинности для полученного трафика NTP (Network Time Protocol) от серверов.
<code>sntp authentication-key <i>число</i> <i>md5 значение</i></code>	Определяет ключ проверки подлинности для SNMP.

Далее приведен пример команд консоли.

```
console> enable
```

```

console# configure

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

Console(config)# snmp
trusted-key 8

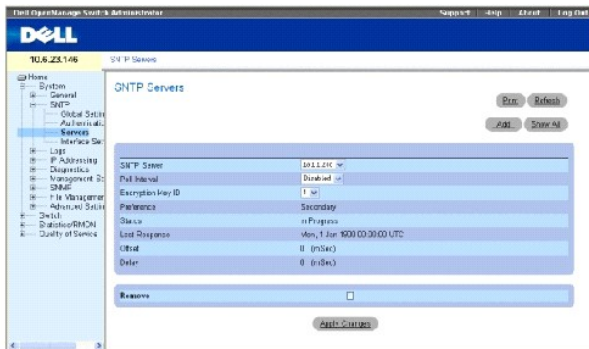
Console(config)# snmp
authenticate

```

Определение серверов SNMP

Страница [SNTP Servers](#) (Серверы SNMP) содержит информацию для выбора сервера SNMP, а также позволяет добавить новый сервер SNMP. Кроме того, на странице [SNTP Servers](#) (Серверы SNMP) можно разрешить устройству выполнять запросы и получать трафик от серверов SNMP. Чтобы открыть страницу [SNTP Servers](#) (Серверы SNMP), выберите System (Система) → SNMP → SNMP Servers (Серверы SNMP) на панели дерева.

Рис. 6-25. Страница SNMP Servers (Серверы SNMP)



SNTP Server (Сервер SNMP) - определяемый пользователем IP-адрес сервера SNMP или имя хоста. Можно определить до восьми серверов SNMP. Это поле может содержать от 1 до 158 символов.

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

Encryption Key ID (Идентификатор ключа шифрования) - определяет идентификатор ключа, который используется для обмена данными между сервером SNMP и устройством. Диапазон значений: 1 - 4294967295.

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

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

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

Status Up (Запуск) - Рабочее состояние сервера SNMP. 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 временем по часам локального 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** (Серверы SNTP), удаляется.

Добавление сервера SNTP

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

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

Рис. 6-26. Страница Add SNTP Server (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 6-18.

Команда консоли	Описание
sntp server ip-address hostname [poll] [key идентификатор_ключа]	Настраивает устройство для использования SNTP при запросе и принятии трафика NTP от сервера.

Команды консоли для сервера SNTP

Далее приведен пример команд консоли.

```
console> enable

console# configure

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


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. 6-27. Страница SNTP Servers Table (Таблица серверов SNTP)

SNTP Server	Poll Interval	Description	Preference	Status	Last Response	Offset	Delay	Remove
15.1.220	Disabled	1	Secondary	In Progress	Mon, 1 Jan '00 20:00:00 UTC	0	0	<input type="checkbox"/>

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).

Таблица 6-19. Команды консоли для сервера SNTP

Команда консоли	Описание
<code>sntp server ip-адрес имя_хоста [poll] [key идентификатор_ключа]</code>	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 [mSec]	Delay [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** (Таблица интерфейсов широковещательной передачи SNTP), 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 Server Updates (Принимать обновления сервера) - включает или отключает определенный интерфейс.

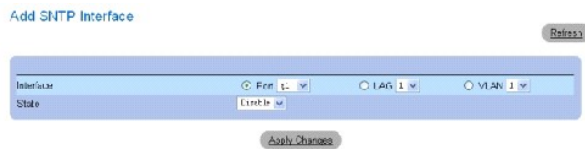
Remove (Удалить) - когда этот флажок установлен, протокол SNTP для указанного интерфейса будет отключен.

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. 6-28. Страница Add SNTP Interface (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).

Таблица 6-20. Команды консоли для 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 snmp 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), выберите System (Система) → Logs (Журналы) на панели дерева.

Страница **Logs** (Журналы) содержит ссылки на страницы разных журналов.

Определение общих параметров журналов

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

Сообщения событий имеют уникальный формат в соответствии с рекомендациями 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.

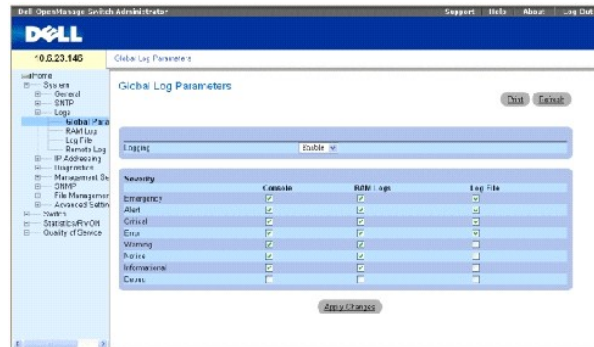
В следующей таблице приведены уровни важности ошибок журнала:

Таблица 6-21. Уровни важности журнала

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

Страница [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), выберите System (Система)→ Logs (Журналы)→ Global Parameters (Общие параметры) на панели дерева.

Рис. 6-29. Страница Global Log Parameters (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.

 **ПРИМЕЧАНИЕ.** 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 в раскрывающемся списке **Logging** (Протоколирование) значение **Enable** (Включить).
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).

Таблица 6-22. Команды консоли для общих параметров журналов

Команда консоли	Описание
logging on	Включает регистрацию сообщений об ошибках.
logging {ip-address hostname} [port port] [severity level] [facility facility] [description text]	Регистрирует сообщения на сервере системных журналов. Список уровней важности см. в разделе «Уровни важности журнала» .
logging console level	Ограничивает сообщения, фиксируемые в журнале консоли, в зависимости от их важности.
logging buffered level	Ограничивает вывод системных сообщений из внутреннего буфера (ОЗУ) в зависимости от их важности.
logging file level	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.

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

```

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 страницу [RAM Log Table](#) (Таблица журнала ОЗУ), выберите System (Система)→ Logs (Журналы)→ RAM Log (Таблица журнала ОЗУ) на панели дерева.

Рис. 6-30. Таблица журнала ОЗУ

Log Index	Log Time	Severity	Description
1	214743313	Warning	NLW-W Down: Vlan 1
2	214743314	Informational	NLW-W Up: Vlan 1
3	214743315	Warning	NLW-W Down: Vlan 1
4	214743316	Informational	NLW-W StartUp: Col. StartUp
5	214743317	Warning	NLW-W Down: g15
6	214743318	Warning	NLW-W Down: g23
7	214743319	Warning	NLW-W Down: g22
8	214743320	Warning	NLW-W Down: g24
9	214743321	Warning	NLW-W Down: g20
10	214743322	Warning	NLW-W Down: g14
11	214743323	Warning	NLW-W Down: g15
12	214743324	Informational	NLW-W Up: g17
13	214743325	Warning	NLW-W Down: g15
14	214743326	Informational	NLW-W Up: Vlan 1
15	214743327	Warning	NLW-W Down: g15
16	214743328	Warning	NLW-W Down: g14
17	214743329	Warning	NLW-W Down: g13
18	214743330	Warning	NLW-W Down: g12
19	214743331	Warning	NLW-W Down: g11
20	214743332	Warning	NLW-W Down: g10
21	214743333	Warning	NLW-W Down: g9
22	214743334	Warning	NLW-W Down: g8
23	214743335	Warning	NLW-W Down: g7
24	214743336	Warning	NLW-W Down: g6
25	214743337	Warning	NLW-W Down: g5
26	214743338	Warning	NLW-W Down: g4
27	214743339	Warning	NLW-W Down: g3
28	214743340	Warning	NLW-W Down: g2
29	214743341	Informational	NLW-W Up: g1
30	214743342	Informational	NLW-W Up: g1
31	214743343	Informational	NLW-W Up: g1
32	214743344	Informational	NLW-W Up: g1
33	214743345	Informational	NLW-W Up: g1
34	214743346	Informational	NLW-W Up: g1
35	214743347	Informational	NLW-W Up: g1

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).

Таблица 6-23. Команды консоли для просмотра таблицы 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
```

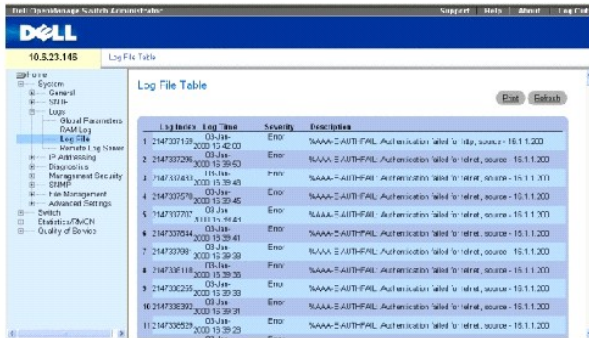


```
01-Jan-2000 01:01:36 :%  
LINK-W-Down: g22  
  
01-Jan-2000 01:01:36 :%  
LINK-W-Down: g21  
  
01-Jan-2000 01:01:36 :%  
LINK-W-Down: g20  
  
01-Jan-2000 01:01:36 :%  
LINK-W-Down: g19  
  
01-Jan-2000 01:01:36 :%  
LINK-W-Down: g18  
  
01-Jan-2000 01:01:36 :%  
LINK-W-Down: g17  
  
01-Jan-2000 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

[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 страницу [Log File Table](#) (Таблица файла журнала), выберите System (Система)→ Logs (Журналы)→ Log File (Файл журнала) на панели дерева.

Рис. 6-31. 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).

Таблица 6-24. Команды консоли для таблицы файла журналов

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

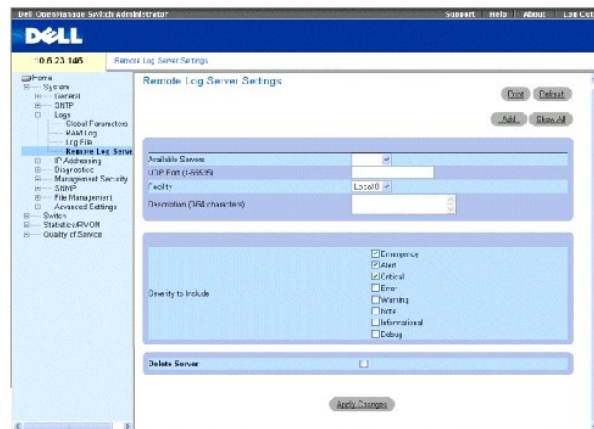
01-Jan-2000
01:11:34 :%LINK-W-
Down: g1

console#
```

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), выберите System (Система)→ Logs (Журналы)→ Remote Log Server (Удаленный сервер журналов) на панели дерева.

Рис. 6-32. Страница Remote Log Server Settings (Параметры удаленного сервера журналов)



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

UDP Port (1-65535) (Порт UDP (1-65535)) - 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.

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

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).

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** (Важность, включая).
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. 6-33. Страница Add a Log Server (Добавить сервер журналов)

The screenshot shows the 'Add a Log Server' configuration page. It features a blue header with the title 'Add a Log Server' and a 'Submit' button. The main form area contains several input fields: 'New Log Server IP Address' (text input), 'UDP Port (1-65535)' (text input with '514' entered), 'Facility' (dropdown menu with 'Local ?' selected), and 'Description (0-64 characters)' (text area). Below these fields is a 'Severity to include' section with a list of checkboxes: 'Emergency', 'Alert', 'Critical', 'Error', 'Warning', 'Notice', 'Information', and 'Debug'. The 'Emergency', 'Alert', and 'Critical' checkboxes are checked. At the bottom of the form is an 'Apply Changes' button.

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. 6-34. Таблица удаленных серверов журналов

Remote Log Servers Table

Refresh

Servers	UDP Port	Facility	Description	Minimum Severity	Remove
Apply Changes					

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](#) (Таблицы 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.

Таблица 6-25. Команды консоли для удаленного сервера журналов

Команда консоли	Описание
<code>logging (ip-адрес имя_хоста) [port порт] [severity уровень] [facility приложение] description текст</code>	Регистрирует сообщения на удаленном сервере.
<code>no logging</code>	Удаляет сервер syslog.
<code>show logging</code>	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. Чтобы открыть страницу IP Addressing (IP-адресация), выберите System (Система) → Addressing (IP-адресация) на панели дерева.

Определение шлюзов по умолчанию

Страница Default Gateway (Шлюз 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 Default Gateway (Шлюз по умолчанию), выберите System (Система) → IP Addressing (IP-адресация) → Default Gateway (Шлюз по умолчанию) на панели дерева.

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

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

Remove (Удалить) - когда этот флажок установлен, удаляются устройства шлюза из раскрывающегося списка **Default Gateway** (Шлюз по умолчанию)

Выбор устройства шлюза:

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

Устройство шлюза будет выбрано, а устройство обновлено.

Удаление шлюза по умолчанию:

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

Запись шлюза по умолчанию будет удалена, а устройство обновлено.

Определение устройств шлюза с помощью команд консоли

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

Таблица 6-26. Команды консоли для определения шлюза по умолчанию

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

Далее приведен пример команд консоли.

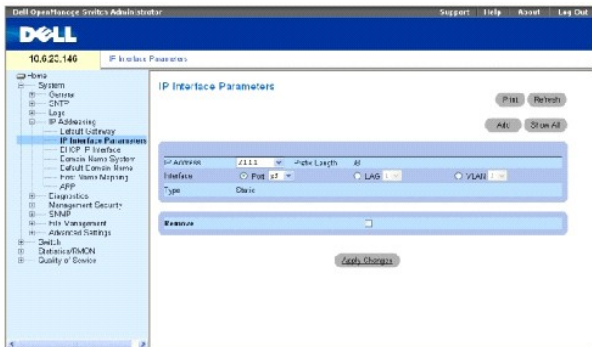
```
Console (config)# ip
default-gateway
196.210.10.1

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

Определение IP-интерфейсов

Страница [IP Interface Parameters](#) (Параметры IP-интерфейса) содержит поля для назначения IP-параметров для интерфейсов. Чтобы открыть страницу [IP Interface Parameters](#) (Параметры IP-интерфейса), выберите **System** (Система) → **IP-Addressing** (IP-адресация) → **Interface Parameters** (Параметры интерфейса) на панели дерева.

Рис. 6-35. Страница IP Interface Parameters (Параметры IP-интерфейса)



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.

Дополнительную информацию см. в разделе [«Настройка сетей VLAN»](#).

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

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

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

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

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

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

Добавление IP-интерфейса

1. Откройте страницу [IP Interface Parameters](#) (Параметры IP-интерфейса).
2. Нажмите кнопку Add (Добавить).

Откроется страница [Add a Static Interface](#) (Добавление статического интерфейса):

Рис. 6-36. Страница Add a Static Interface (Добавление статического интерфейса)



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

Параметры будут изменены, а устройство обновлено.

Удаление IP-адресов

1. Откройте страницу [IP Interface Parameters](#) (Параметры IP-интерфейса).
2. Нажмите кнопку **Show All** (Показать все).

Откроется страница **Interface Parameters Table** (Таблица параметров интерфейса):

Рис. 6-37. IP Interface Parameter Table (Таблица параметров IP-интерфейса)

IP Interface Parameter Table

IP Address	Prefix Length	Interface	Type	Remove
2 * 1.1	/8	g3	Static	<input type="checkbox"/>
10.0.255.46	/24	g1/	DHCP	<input type="checkbox"/>
16.1.1.3	/8	g1	Static	<input type="checkbox"/>

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 IP-интерфейсов с помощью команд консоли

В следующей таблице приведены команды консоли для настройки полей, отображаемых на странице [IP Interface Parameters](#) (Параметры IP-интерфейса).

Таблица 6-27. Команды консоли для определения параметров IP-интерфейса

Команда консоли	Описание
ip address ip-адрес { mask prefix-length }	Задаёт IP-адрес.
no ip address [ip-адрес]	Удаляет IP-адрес.
show ip interface [ethernet номер_интерфейса vlan идентификатор_vlan port-channel номер]	Отображает состояние готовности настроенных IP-интерфейсов.

Далее приведен пример команд консоли.

```


```

```

Console (config)#
interface vlan 1

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)#
exitconsole# 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 IP-интерфейса DHCP

```

console# show ip interface vlan 1

```

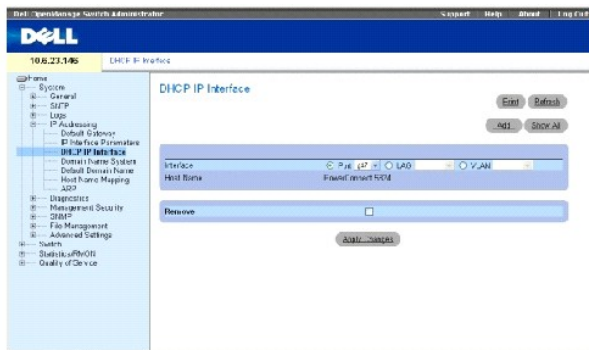
Отображаемая информация

Gateway IP Address	Activity status	
-----	-----	

192.168.1.1	Active	
IP address	Interface	Type
-----	-----	-----
192.168.1.123 /24	VLAN 1	Static

Страница [DHCP IP Interface](#) (IP-интерфейс DHCP) содержит поля для определения клиентов DHCP, подключенных к устройству. Выберите **System** (Система) → **IP Addressing** (IP-адресация) → **DHCP IP Interface** (IP-интерфейс DHCP) на панели дерева. Чтобы открыть [страницу DHCP IP Interface](#) (IP-интерфейс DHCP).

Рис. 6-38. Страница DHCP IP Interface (IP-интерфейс DHCP)



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

Host Name (Имя хоста) - имя системы. Это поле может содержать до 20 символов.

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

Добавление клиента DHCP

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

Откроется страница **Add DHCP IP Interface** (Добавить IP-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 IP-интерфейса DHCP

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

Запись будет изменена, а устройство обновлено.

Удаление IP-интерфейса DHCP

1. Откройте страницу [DSCP IP Interface](#) (IP-интерфейс DHCP).
2. Нажмите кнопку **Show All** (Показать все).

Откроется **DHCP Client Table** (Таблица клиентов DHCP).

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 IP-интерфейсов DHCP с помощью команд консоли

В следующей таблице приведены эквивалентные команды консоли для определения клиентов DHCP.

Таблица 6-28. Команды консоли для определения IP-интерфейсов DHCP

Команда консоли	Описание
<code>ip address dhcp [hostname ИМЯ_ХОСТА]</code>	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

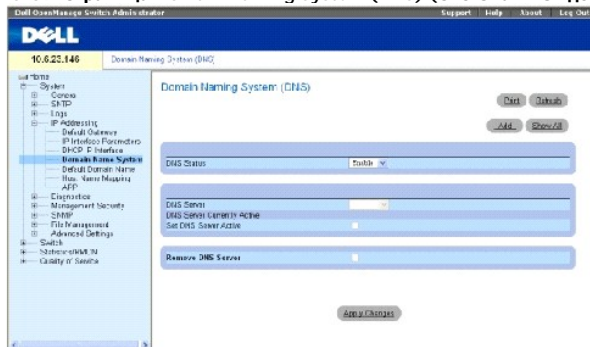
console (config-if)# ip
address dhcp 10.0.0.1 /8
```

Настройка системы имен доменов

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

Страница Domain Naming System (DNS) (Система имен доменов) содержит поля для включения и активизации определенных серверов DNS. Чтобы открыть страницу Domain Naming System (DNS) (Система имен доменов), выберите System (Система) → IP Addressing (IP-адресация) → Domain Name System (Система имен доменов) на панели дерева.

Рис. 6-39. Страница Domain Naming System (DNS) (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).

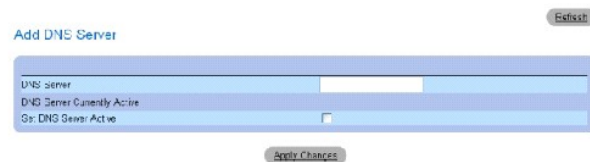
Remove DNS Server (Удалить сервер DNS) - когда выбран этот параметр, серверы DNS удаляются.

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. 6-40. Страница Add DNS Server (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. 6-41. Таблица DNS Server Table (Таблица серверов DNS)

Удаление серверов DNS

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

Выбранный сервер DNS будет удален, а устройство обновлено.

Настройка серверов DNS с помощью команд консоли

В следующей таблице приведены команды консоли для настройки системной информации устройства.

Таблица 6-29. Команды консоли для сервера DNS

Команда консоли	Описание
<code>ip name-server <i>адрес_сервера</i></code>	Задаёт доступные имена серверов. Можно определить до восьми имен серверов.
<code>no ip name-server <i>адрес_сервера</i></code>	Удаляет имя сервера.
<code>ip domain-name <i>имя</i></code>	Определяет имя домена по умолчанию, которое используется программой, если имена хоста указаны неправильно.
<code>clear host { <i>name</i> * }</code>	Удаляет записи из кэша имя хоста-адрес.
<code>show hosts [<i>имя</i>]</code>	Отображает имя домена по умолчанию, список хостов сервера имен, статические имена и адреса, а также список имен и адресов из кэша.

Далее приведен пример команд консоли.

```
console> enable

Console# configure

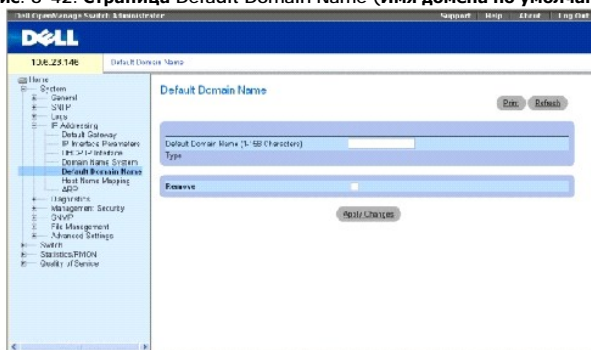
console (config)# ip name-
server 176.16.1.18
```

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), выберите System (Система)→ IP Addressing (IP-адресация)→ Default Domain Name (Имя домена по умолчанию) на панели дерева.

Рис. 6-42. Страница Default Domain Name (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 удалится.

Определение имен доменов DNS с помощью команд консоли

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

Таблица 6-30. Команды консоли имен доменов DNS

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

Далее приведен пример команд консоли.

```
console> enable

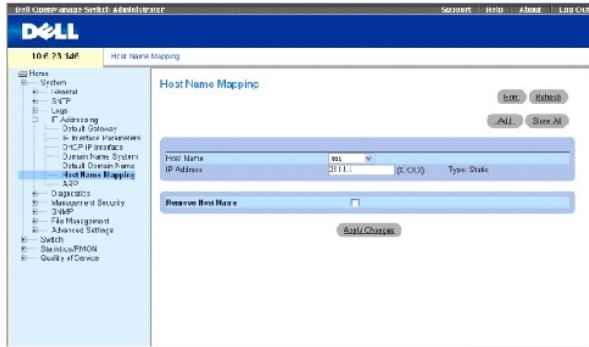
console# configure

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

Отображение хоста домена

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. 6-43. Страница Host Name Mapping (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 (X.X.X.X)) - предоставляет до восьми IP-адресов, которые назначаются для определенного имени хоста.

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

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

Static (Статический) - статический IP-адрес.

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

Добавление имен домена хоста

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

Откроется страница **Add Host Name Mapping** (Добавление отображения имени хоста):

Рис. 6-44. Страница Add Host Name Mapping (Добавление отображения имени хоста)



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

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

Отображение таблицы отображения имен хостов

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

Откроется страница **Hosts Name Mapping Table** (Таблица отображения имен хостов):

Рис. 6-45. Hosts Name Mapping Table (Таблица отображения имен хостов)

Hosts Name Mapping Table

Host Name	IP Address	Remove Select All
1 asa	193.11.1	<input type="checkbox"/>
2 www.com	193.11.1	<input type="checkbox"/>

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 таблицы Host Mapping Table (Таблица отображения хостов) будет удалена, а устройство обновлено.

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

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

Таблица 6-31. Команды консоли имен хостов домена

Команда консоли	Описание
ip host name address1 [address2 ... address8]	Определяет соответствие статических имен хостов адресам в кэше хоста
no ip host name	Удаляет соответствие имен хостов адресам.
clear host {name *}	Удаляет записи из кэша имя хоста-адрес.
show hosts [name]	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
```

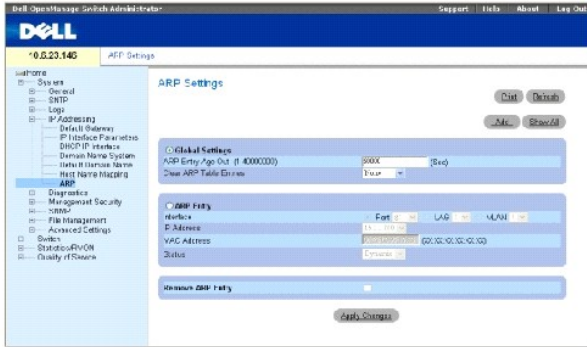
```
console# configure
```

```
console (config)# ip 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), выберите System (Система) → IP Addressing (IP-адресация) → ARP на панели дерева.

Рис. 6-46. Страница ARP Settings (Параметры ARP)



Global Settings (Общие параметры) - выберите этот параметр, чтобы активизировать поля общих параметров ARP.

ARP Entry Age Out (1-4000000) (Срок хранения записи ARP (1-4000000)) - 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 в таблице ARP с IP-адресом.

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. 6-47. Страница Add ARP Entry (Добавление записи ARP)

The screenshot shows the 'Add ARP Entry' configuration page. At the top right is a 'Refresh' button. Below it is a form with three rows: 'Interface' with a dropdown menu showing 'g1', 'IP Address' with a text input '0.0.0.0' and a '(P.S. K3)' button, and 'MAC Address' with a text input '00:00:00:00:00:00'. At the bottom center is an 'Apply Changes' button.

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

Запись **ARP Table** (Таблицы 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. 6-48. Страница ARP Table (Таблица ARP)

The screenshot shows the 'ARP Table' page with a 'Refresh' button at the top right. Below it is a table with the following data:

	Interface	IP Address	MAC Address	Status	Remove
1	g1	15.1.1.200	00:0b:35:17:8b	Dynamic	<input type="checkbox"/>
2	g7	10.6.23.129	00:05:00:0f:0d	Dynamic	<input type="checkbox"/>

At the bottom center is an 'Apply Changes' button.

Удаление записи таблицы ARP

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

Откроется страница **ARP Table** (Таблица ARP).

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

Выбранная запись таблицы **ARP Table** будет удалена, а устройство обновлено.

Настройка ARP с помощью команд консоли

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

Таблица 6-32. Команды консоли для настройки 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

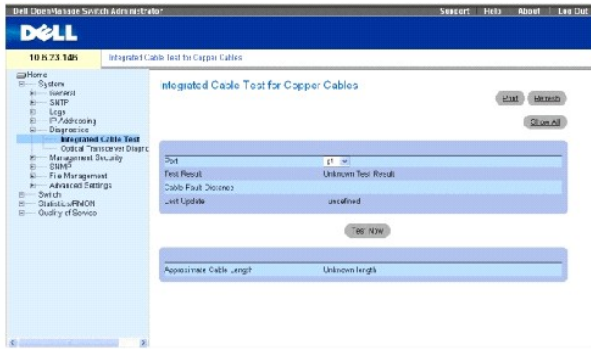
Страница **Diagnostics** (Диагностика) содержит ссылки на страницы, которые используются для виртуального тестирования медных и оптоволоконных кабелей. Чтобы открыть страницу **Diagnostics** (Диагностика), выберите **System** (Система) → **Diagnostics** (Диагностика) на панели дерева.

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 выполняется при отключенных портах. Исключение составляет тест примерной длины кабеля (Approximated Cable Length).

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

Рис. 6-49. Страница **Integrated Cable Test for Copper Cables** (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 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.

Таблица 6-3 3. Команды консоли для выполнения тестирования медных кабелей

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

Далее приведен пример команд консоли.


```
console> 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
g5	Fiber	-	-

 **ПРИМЕЧАНИЕ.** 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.

Просмотр диагностики оптического трансивера

Страница [Optical Transceiver Diagnostics](#) содержит поля для выполнения тестов оптоволоконных кабелей. Чтобы открыть страницу [Optical Transceiver Diagnostics](#) (Диагностика оптического трансивера), выберите **System (Система) → Diagnostics (Диагностика) → Optical Transceiver Diagnostics** (Диагностика оптического трансивера) на панели дерева.


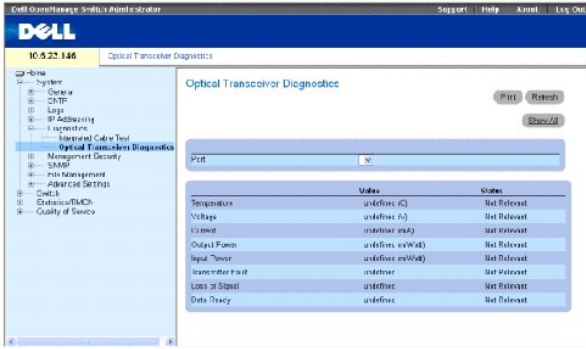
 **ПРИМЕЧАНИЕ.** Диагностика оптического трансивера может быть выполнена только в том случае, если установлено соединение.

Рис. 6-50. 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).

Выполнение тестирования оптоволоконных кабелей с помощью команд консоли

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

Таблица 6-34. 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
```

Port	Temp	Voltage	Current	Power		TX	LOS
				Output	Input		
	(C)	(Volt)	(mA)	(mWatt)	(mWatt)	Fault	
g1	W	OK	E	OK	OK	OK	OK
g2	OK	OK	OK	OK	OK	E	OK
g3	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


Таблица **Optical Transceiver Diagnostics Table** (Таблица диагностики оптического трансивера) содержит следующие столбцы:

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

 **ПРИМЕЧАНИЕ.** Трансиверы Finisar не поддерживают диагностический тест неисправности.

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

1 N/A - недоступно, N/S - не поддерживается, W - предупреждение, E - ошибка.

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

Управление безопасностью устройств

Страница **Management Security** (Безопасность управления) предоставляет 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), выберите **System** (Система)→**Management Security** (Безопасность управления) на панели дерева.

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.

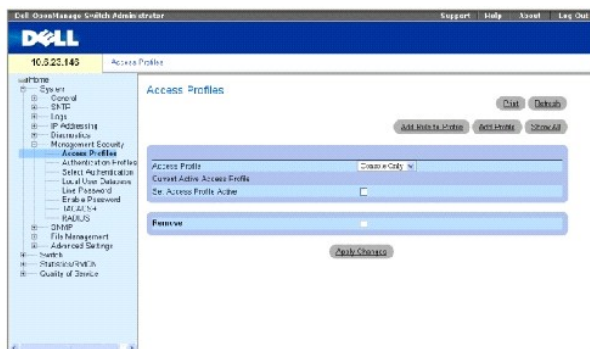
Доступ к управлению может быть отдельно определен для каждого метода доступа для управления, включая Web (HTTP), безопасный web (HTTPS), Telnet, безопасный Telnet и SNMP.

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

Рис. 6-51. 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** (Профиля доступа), сеанс будет прерван, а затем разрешен доступ к устройству только с консоли.

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

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

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

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. 6-52. Страница Add An Access Profile (Добавление профиля доступа)

Access Profile Name (1-32 Characters) (Имя профиля доступа (1-32 Символов)) - определенное пользователем имя профиля доступа.

Rule Priority (1-65535) (Приоритет правила (1-65535)) - 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.

ПРИМЕЧАНИЕ. Назначение профиля доступа для интерфейса означает запрет доступа через другие интерфейсы. Если профиль доступа не назначен ни для одного интерфейса, устройство будет доступно для всех интерфейсов.

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

ПРИМЕЧАНИЕ. 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** (Добавление правила профиля доступа):

Рис. 6-53. Добавление правила профиля доступа

Скриншот экрана конфигурации "Add an Access Profile Rule". Вверху заголовок "Add an Access Profile Rule" и кнопка "Cancel". Основная форма имеет заголовок "Access Profile Name" со значением "Console Only". Поля для настройки: "Priority (1-65535)" (текстовое поле), "Management Method" (выпадающий список со значением "All"), "Interface" (checkbox и выпадающие списки "Port", "LAG", "VLAN"), "Exclude IP Address" (checkbox и текстовое поле), "Network Mask" (текстовое поле), "Prefix Length" (текстовое поле), "Action" (выпадающий список со значением "Permit"). Внизу кнопки "Apply Changes".

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

Правило будет добавлено в профиль доступа, а устройство обновлено.

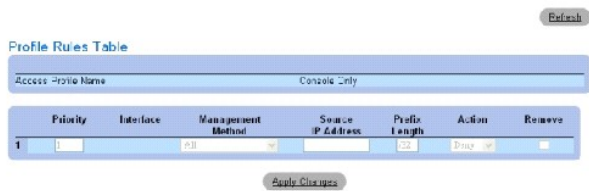
Просмотр таблицы правил профиля:

ПРИМЕЧАНИЕ. Порядок, в котором правила отображаются в **Profile Rules Table** (Таблице правил профиля), имеет значение. Пакеты сравниваются с первым правилом, которое отвечает критериям правила.

1. Откройте страницу [Access Profiles](#) (Профили доступа).
2. Нажмите кнопку **Show All** (Показать все).

Откроется страница **Profile Rules Table** (Таблица правил профиля):

Рис. 6-54. Страница Profile Rules Table (Таблица правил профиля)



Удаление правила

1. Откройте *страницу* AccessProfiles (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).

Таблица 6-35. Команды консоли для профилей 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]	Задаёт разрешающие условия для списка доступа для управления для порта
permit ip-source ip_адрес [mask маска длина_префикса] [ethernet номер_интерфейса vlan идентификатор_vlan port-channel номер] [service служба]	Задаёт для порта разрешающие условия списка доступа для управления и выбранный метод управления.
deny [ethernet номер_интерфейса vlan идентификатор_vlan port-channel номер] [service служба]	Задаёт для порта запрещающие условия списка доступа для управления и выбранный метод управления.
deny ip-source ip_адрес [mask маска длина_префикса] [ethernet номер_интерфейса vlan идентификатор_vlan port-channel номер] [service служба]	Задаёт 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
m1ist

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
m1ist

Console (config)# exit

Console# show management
access-list

m1ist

-----

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
m1ist
```

Определение профилей проверки подлинности

Страница [Authentication Profiles](#) (Профили проверки подлинности) содержит поля для выбора метода проверки подлинности пользователя на устройстве. Идентификация пользователя происходит:

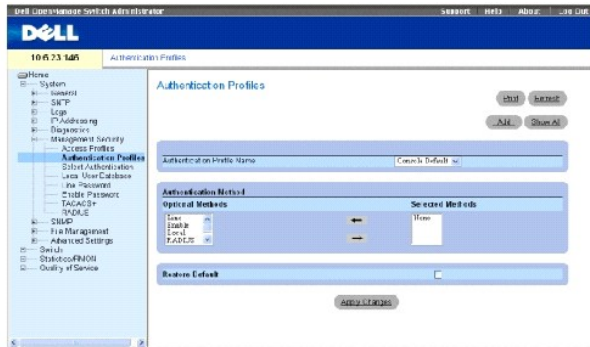
- 1 Локально
- 1 Через внешний сервер

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. 6-55. Страница 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 [«Настройка общих параметров 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 клавишей 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. 6-56.

Страница 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. 6-57. Страница Authentication Profiles (Профили проверки подлинности)

Profile Name	Methods	Remove
1 create Default	None	<input type="checkbox"/>
2 network Default	Local	<input type="checkbox"/>

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).

Таблица 6-36. Команды консоли для профилей проверки подлинности

Команда консоли	Описание
aaa authentication login {default имя_списка} метод1 [метод2]	Настраивает проверку подлинности при входе в систему.
no aaa authentication login {default имя_списка}	Удаляет профиль проверки подлинности при входе в систему.

Далее приведен пример команд консоли.

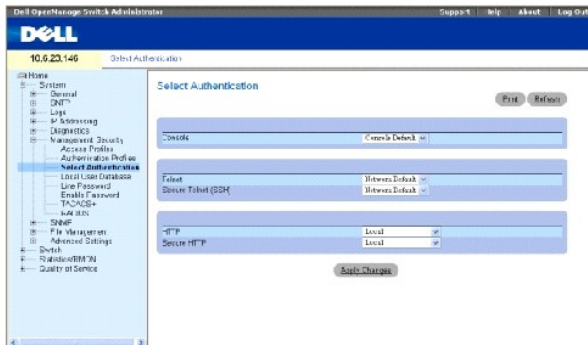
```
Console (config)# aaa
authentication login
default radius local
enable none

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

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 выполняется по списку методов проверки подлинности 2. Чтобы открыть страницу [Select Authentication](#) (Выбор проверки подлинности), выберите System (Система)→ Management Security (Безопасность управления)→ Select Authentication (Выбор проверки подлинности) на панели дерева.

Рис. 6-58. Страница 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 зашифрованные удаленные соединения с устройством.

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

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

Local (Локально) - проверка подлинности выполняется локально.

RADIUS - проверка подлинности выполняется на сервере RADIUS.

TACACS+ - проверка подлинности выполняется на сервере TACACS+.

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 проверки подлинности в поле Secure HTTP (Безопасный 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).

Таблица 6-37. Команды консоли для выбора 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

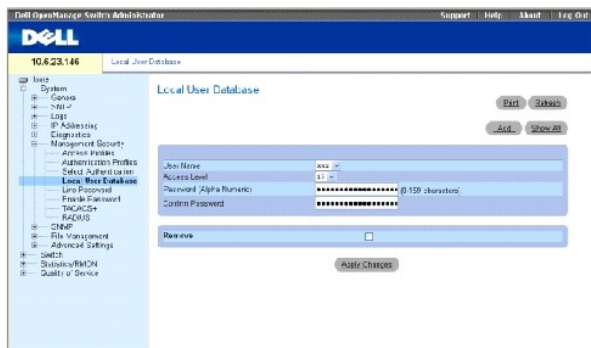
HTTPS: Radius, local

Dot1x: Radius
```

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. Страница Local User Database (Локальная база данных пользователей)



User Name (Имя пользователя) - список пользователей.

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

Password (0-159 Characters) (Пароль от 0 до 159 символов) - задаваемый пользователем пароль. Длина паролей локальной базы данных не должна превышать 159 символов.

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

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

Назначение прав доступа пользователю:

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

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

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. Страница Add User (Добавление пользователя)

Add a User Name Refresh

Attribute	Value	
User Name (Alpha Numeric)	<input type="text"/>	(1-23 characters)
Access Level (1-16)	1	
Password (Alpha Numeric)	<input type="password"/>	(0-159 characters)
Confirm Password	<input type="password"/>	

Apply Changes

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. Страница Local User Table (Локальная пользовательская таблица)



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).

Таблица 6-38. Команды консоли для локальной базы данных пользователей

Команда консоли	Описание
username name [password password] [level level] [encrypted]	Устанавливает проверку подлинности по имени пользователя.

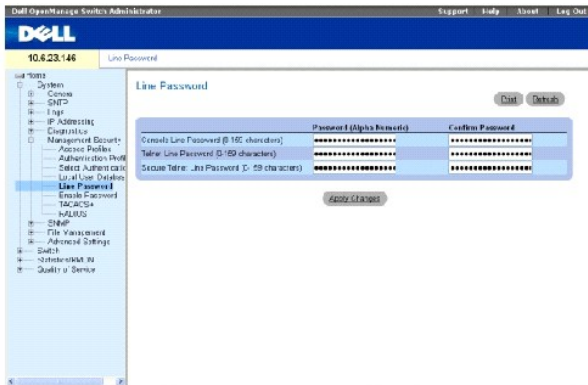
Далее приведен пример команд консоли.

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

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. Страница Line Password (Пароль канала)



Line Password for Console/Telnet/Secure Telnet (0-159 Characters) (Пароль канала для консоли/Telnet/Secure Telnet (0-159 Characters)) - пароль канала для доступа к устройству через сеанс консоли, Telnet или Secure Telnet. Пароли могут содержать не более 159 символов.

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

Определение паролей каналов связи для сеансов консоли

1. Откройте страницу [Line Password](#) (Пароль канала).
2. Определите поле Line Password for Console (Пароль линии для консоли).
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Пароль линии для сеансов консоли будет определен, а устройство обновлено.

Определение паролей каналов связи для сеансов Telnet

1. Откройте страницу [Line Password](#) (Пароль канала).
2. Определите поле Line Password for Telnet (Пароль линии 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. Определите поле Line Password for Secure Telnet (Пароль линии для безопасной связи Telnet).
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Пароль линии для сеансов Secure Telnet будет определен, а устройство обновлено.

Назначение паролей каналов с помощью команд консоли

В следующей таблице приведены команды консоли для настройки полей, отображаемых на странице [Line Password](#) (Пароль канала).

Таблица 6-39. Команды консоли для пароля канала

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

password пароль [encrypted]	Задаёт пароль линии.
-----------------------------	----------------------

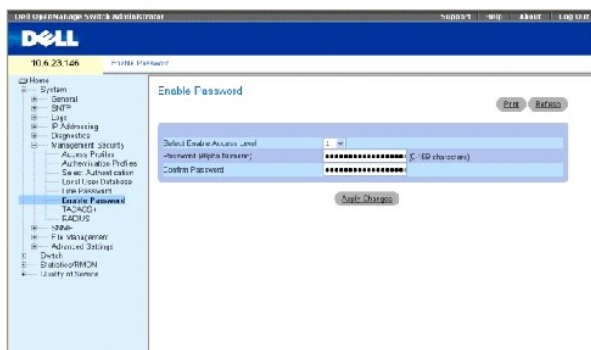
Далее приведен пример команд консоли.

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

Определение пароля включения

Страница [Modify Enable Password](#) (Изменение пароля включения) задает локальный пароль для управления доступом для конфигураций Normal (Обычная), Privilege (С привилегиями) и Global (Общая). Чтобы открыть страницу [Modify Enable Password](#) (Изменение пароля включения), выберите System (Система) → Management Security (Безопасность управления) → Enable Passwords (Пароли включения) на панели дерева.

Рис. 6-63. Страница Modify Enable Password (Изменение пароля включения)



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 настроенный пароль включения. Пароли включения могут содержать не более 159 символов.

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

Определение нового пароля включения:

1. Откройте страницу [Modify Enable Password](#) (Изменение пароля включения).
2. Определите соответствующие поля.
3. Нажмите кнопку Apply Changes (Применить изменения).

Новый пароль включения будет определен, а устройство обновлено.

Назначение паролей включения с помощью команд консоли

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

Таблица 6-40. Команды консоли для изменения пароля включения

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

enable password [level уровень] пароль [encrypted]	Задаёт локальный пароль для управления доступом для уровней пользователей и привилегий.
show users accounts	Отображает сведения о локальной базе данных пользователей.

Далее приведен пример команд консоли.

```

Console (config)# enable
password level 15 secret

Console# show users
accounts

Username Privilege
-----
secret 15

```

Определение параметров TACACS+

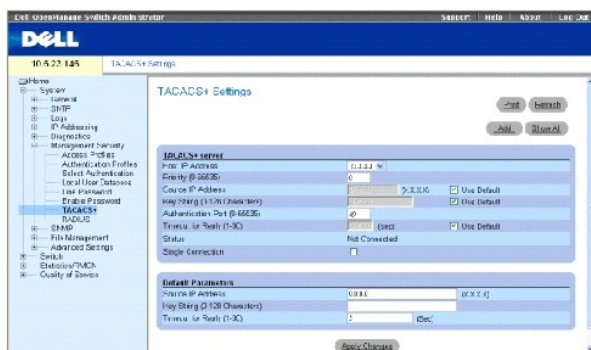
Устройство предоставляет поддержку для клиентов TACACS+ (Terminal Access Controller Access Control System). TACACS+ обеспечивает централизованную систему безопасности для проверки пользователей, получающих доступ к устройству.

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

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

Протокол TACACS+ обеспечивает целостность сети благодаря обмену зашифрованными 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. Параметры TACACS+



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

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

Reply Timeout (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) - когда выбран этот параметр, поддерживается одно открытое соединение между устройством и сервером TACACS+.

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

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

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

Timeout for Reply (1-30) (Время для ответа (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. Страница Add TACACS+ Host (Добавление хоста TACACS+)

Add TACACS+ Host

Return

Host IP Address	<input type="text"/>	(x.x.x.x)
Priority (0-65535)	<input type="text"/>	
Source IP Address	<input type="text"/>	(x.x.x.x) <input type="checkbox"/> Use Default
Key String (0-128 Characters)	<input type="text"/>	<input type="checkbox"/> Use Default
Authentication Port (0-65535)	<input type="text"/>	<input type="checkbox"/> Use Default
Timeout for Reply (1-30)	<input type="text"/>	<input type="checkbox"/> Use Default
Single Connection	<input type="checkbox"/>	

Apply Changes

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+)

Host IP Address	Priority	Source IP Address	Authentication Prot.	Timeout for Reply	Single Connection	Status	Remove
1 23.1.1.1	0	Default	49	Default	<input type="checkbox"/>	Not Connected	<input type="checkbox"/>

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+).

Таблица 6-41. Команды консоли для TACACS+

Команда консоли	Описание
<code>TACACS-server host (ip-адрес имя_хоста) [single-connection] [port номер_порта] [timeout тайм-аут] [key строка_ключа] [source источник] [priority приоритет]</code>	Определяет хост TACACS+.
<code>no TACACS-server host (ip-адрес имя_хоста)</code>	Удаляет хост TACACS+.
<code>tacacs-server key key-string</code>	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.)
<code>tacacs-server timeout timeout</code>	Указывает значение тайм-аута в секундах. (Диапазон: 1 - 30.)
<code>tacacs-server source-ip source</code>	Определяет IP-адрес источника. (Диапазон: допустимый IP-адрес.)
<code>show TACACS [ip-адрес]</code>	Отображает настройку и статистику для сервера TACACS+.

Далее приведен пример команд консоли.

Console# show tacacs						
Router Configuration						
-----	-----	---	-----	-----	-----	-----
-		-		-	-	-
IP address	Status	Port	Single Connection	TimeOut	Source IP	Priority
-----	-----	---	-----	-----	-----	-----
-		-		-	-	-
12.1.1.2	Not Connected	49	Yes	1	12.1.1.1	1
Global values						

TimeOut :						
5						
Router Configuration						

Source IP : 0.0.0.0						
console#						

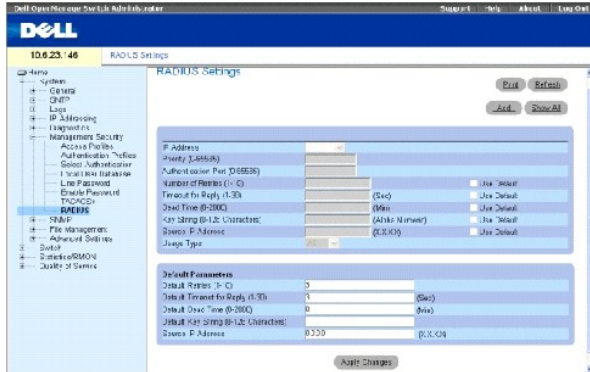
Настройка общих параметров RADIUS

Серверы RADIUS (RADIUS - Remote Authorization Dial-In User Service) обеспечивают дополнительную защиту сетей. Серверы RADIUS обеспечивают централизованный метод проверки подлинности:

- 1 для доступа Telnet
- 1 для доступа по Интернету
- 1 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. Страница RADIUS Settings (Параметры RADIUS)



IP Address (IP-адрес) - список IP-адресов серверов для проверки подлинности.

Priority (1-65535) (Приоритет (1-65535)) - 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) - порт проверки подлинности. Порт проверки подлинности используется для проверки подлинности сервера RADIUS.

Number of Retries (1-10) (Число повторных попыток (1-10)) - 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 (1-30)) - 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 (0-2000)) - 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.

Следующие поля задают значения по умолчанию для RADIUS:

Default Timeout for Reply (1-30) (Время для ответа по умолчанию (1-30)) - время по умолчанию (в секундах), в течение которого устройство ожидает ответа от сервера RADIUS.

 **ПРИМЕЧАНИЕ.** Если не указаны значения времени ожидания, числа попыток или времени отключения для конкретного хоста, для каждого хоста используются общие значения (по умолчанию).

Default Retries (1-10) (Число повторных попыток по умолчанию (1-10)) - число запросов по умолчанию, передаваемых серверу RADIUS, прежде чем отображается ошибка.

Default Dead time (0-2000) (Время отключения по умолчанию (0-2000)) - 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 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).

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. Страница Add RADIUS Server (Добавление сервера RADIUS)

IP Address	<input type="text"/>	(X.X.X.X)
Priority ID (0-65535)	<input type="text"/>	0
Authentication Port (0-65535)	<input type="text"/>	1812
Number of Retries (1-10)	<input type="text"/>	3 <input type="checkbox"/> Use Default
Timeout for Reply (1-30)	<input type="text"/>	30 <input type="checkbox"/> Use Default
Dead Interval (0-2000)	<input type="text"/>	300 <input type="checkbox"/> Use Default
Key String (0-120 Characters)	<input type="text"/>	(Alpha numeric) <input type="checkbox"/> Use Default
Source IP Address	<input type="text"/>	(X.X.X.X) <input type="checkbox"/> Use Default
Usage Type	<input type="text"/>	All

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

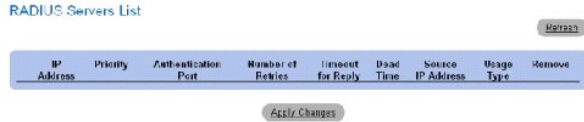
Новый сервер RADIUS будет добавлен, а устройство обновлено.

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. Страница 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).

Таблица 6-42. Команды консоли для настройки серверов RADIUS

Команда консоли	Описание
radius-server timeout количество_секунд	Задаёт стандартный интервал для каждого устройства, ожидающего ответа сервера.
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]	Задаёт 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)# radius-
server timeout 5
```

```
Console (config)# radius-  
server retransmit 5
```

```
Console (config)# radius-  
server deadtime 10
```

```
Console (config)# radius-  
server key dell-server
```

```
Console (config)# radius-  
server host 196.210.100.1  
auth-port 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

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.

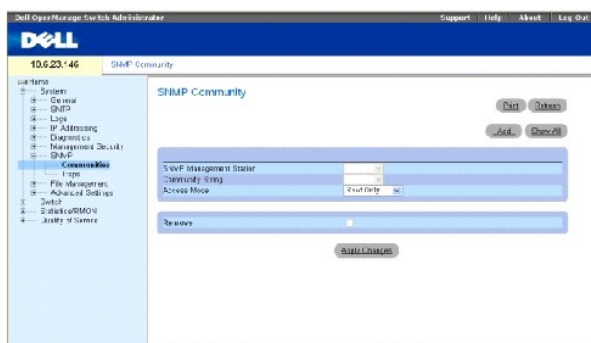
Управление правами доступа к агенту SNMP осуществляется с помощью строк доступа. Для установки связи с коммутатором встроенный веб-сервер предлагает правильную строку сообщества для идентификации. Чтобы открыть страницу SNMP, выберите System (Система) → SNMP на панели дерева.

В этом разделе содержится информация по управлению настройкой SNMP.

Определение сообщества

Управление правами доступа осуществляется путем определения сообществ в Community Table (Таблице сообществ). При изменении имен сообществ изменяются также и права доступа. Чтобы открыть страницу [SNMP Community](#) (Сообщество SNMP), выберите System (Система) → SNMP → Communities (Сообщества) на панели дерева.

Рис. 6-70. Страница 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.

Access Mode (Режим доступа) - определяет права доступа для сообщества. 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 (Администрирование) - доступ управления предоставляется с возможностью чтения и записи. Это справедливо для всех баз MIB, включая таблицу сообществ.

Remove (Удалить) - когда установлен этот флажок, сообщество удаляется.

Определение нового сообщества

1. Откройте страницу [SNMP Community](#) (Сообщество SNMP).
2. Нажмите кнопку Add (Добавить).

Откроется страница **Add SNMP Community** (Добавление сообщества SNMP):

Рис. 6-71. Страница Add SNMP Community (Добавление сообщества SNMP)
[Add SNMP Community](#)

SNMP Management

Management Station (XXXXX) All (0.0.0.0)

Community String (1-20 Characters)

Access Mode: Read Only

Refresh

Apply Changes

3. Выберите одно из следующих значений:

Management Station (Станция управления) - 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 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. 6-72. Страница Community Table (Таблица сообществ)

Community Table

Management Station	Community String	Access Mode	Remove
--------------------	------------------	-------------	--------

Refresh

Apply Changes

Удаление сообществ

1. Откройте страницу [SNMP Community](#) (Сообщество SNMP).
2. Нажмите кнопку Show All (Показать все).

Откроется страница [Community Table](#) (Таблица сообществ).

3. Выберите сообщество в **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 [SNMP Community](#) (Сообщество SNMP).

Таблица 6-43. Команды консоли для сообщества SNMP

Команда консоли	Описание
snmp-server community строка [ro rw su] [ip_адрес]	Задаёт строку доступа к сообществу для разрешения доступа по протоколу SNMP.
snmp-server host {ip-адрес имя_хоста} строка_сообщества [1 2]	Определяет тип системных прерываний, отправляемых выбранному получателю.
show snmp	Отображает состояние соединений по протоколу SNMP.

Далее приведен пример команд консоли.

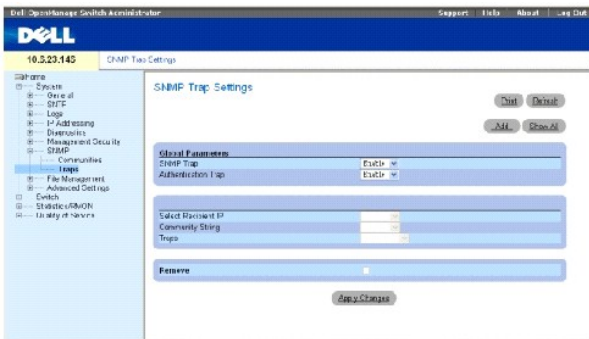
console(config)# snmp-server community public_1 su 1.1.1.1		
console(config)# snmp-server community public_2 rw 2.2.2.2		
console(config)# snmp-server community public_3 ro 3.3.3.3		
console(config)# snmp-server host 1.1.1.1 public_1 1		
console(config)# snmp-server host 2.2.2.2 public_2 2		
console(config)#		
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

-----	-----	-----
1.1.1.1	public_1	1
2.2.2.2	public_2	2
System Contact: 345 6789		
System Location: 1234 5678		
console#		

Определение системные прерывания

На странице [SNMP Trap Settings](#) (Параметры системных прерываний SNMP) пользователь может включить или выключить для устройства функцию отправки системных прерываний SNMP или уведомлений. Чтобы открыть страницу [SNMP Trap Settings](#) (Параметры системных прерываний SNMP), выберите System (Система)→ SNMP→ Traps (Прерывания) на панели дерева.

Рис. 6-73. Страница SNMP Trap Settings (Параметры системных прерываний SNMP)



SNMP Trap (Системное прерывание SNMP) - включает системных прерываний SNMP или уведомлений SNMP с устройства определенному получателю системных прерываний.

Authentication Trap (Системное прерывание проверки подлинности) - включает отправку системных прерываний SNMP при ошибке проверки подлинности для определенных получателей.

Select Recipient IP (Выбор IP-адреса получателя) - IP-адрес, по которому отправляются системные прерывания.

Community String (Строка сообщества) - строка сообщества менеджера системных прерываний.

Traps (Прерывания) - определяет тип системных прерываний, отправляемых выбранному получателю. Возможные значения:

SNMP V1 - отправляются системные прерывания SNMP версии 1.

SNMP V2c - отправляются системные прерывания SNMP версии 2.

Remove (Удалить) - когда этот флажок установлен, запись удаляется из таблицы **Trap Manager Table** (Таблица менеджеров системных прерываний).

Включение прерываний SNMP на устройстве

1. Откройте страницу [SNMP Trap Settings](#) (Параметры системных прерываний SNMP).
2. Выберите **Enable** (Включить) в раскрывающемся списке **SNMP Trap** (Системное прерывание SNMP).
3. Определите поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Системные прерывания SNMP будут включены на устройстве.

Включение прерываний проверки подлинности на устройстве

1. Откройте страницу [SNMP Trap Settings](#) (Параметры системных прерываний SNMP).
2. Выберите в раскрывающемся списке **Authentication Trap** (Системное прерывание идентификации) значение **Enable** (Включить).
3. Определите поля.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Системные прерывания идентификации будут включены на устройстве.

Добавление нового получателя системного прерывания:

1. Откройте страницу [SNMP Trap Settings](#) (Параметры системных прерываний SNMP).
2. Нажмите кнопку **Add** (Добавить).

Откроется страница [Add Trap Receiver/Manager](#) (Добавление менеджера/получателя системных прерываний):

Рис. 6-74. Страница Add Trap Receiver/Manager (Добавление менеджера/получателя системных прерываний)

The screenshot shows a web form titled "Add Trap Recipient". At the top right is a "Back" button. The form has three input fields: "Recipient IP Address" with a placeholder "(XXX.X)", "Community String (1-20 Characters)", and "Traps Enable" with a dropdown menu showing "SNMPV". Below the form is an "Apply Changes" button.

3. Определите поля. Настройка 0.0.0.0 означает «All» (Все), и системные прерывания передаются.
4. Нажмите кнопку **Apply Changes** (Применить изменения).

Менеджер или получатель системных прерываний будет добавлен, а устройство обновлено.

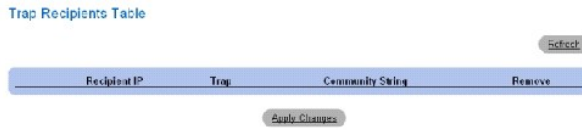
Отображение таблицы менеджеров системных прерываний

Trap Managers Table (Таблица менеджеров системных прерываний) содержит поля для настройки типов системных прерываний.

1. Откройте страницу [SNMP Trap Settings](#) (Параметры системных прерываний SNMP).
2. Нажмите кнопку **Show All** (Показать все).

Откроется страница [Trap Managers Table](#) (Таблица менеджеров системных прерываний):

Рис. 6-75. Страница Trap Managers Table (Таблица менеджеров системных прерываний)



Удаление записи из таблицы менеджеров системных прерываний

1. Откройте страницу [SNMP Trap Settings](#) (Параметры системных прерываний SNMP).
2. Нажмите кнопку Show All (Показать все).

Откроется страница [Trap Managers Table](#) (Таблица менеджеров системных прерываний).

3. Выберите запись в таблице Trap Managers Table (Таблица менеджеров системных прерываний).
4. Установите флажок Remove (Удалить).
5. Нажмите кнопку Apply Changes (Применить изменения).

Выбранный менеджер системных прерываний будет удален, а устройство обновлено.

Настройка системных прерываний с помощью команд консоли

В следующей таблице приведены команды консоли для настройки полей, отображаемых на странице [SNMP Trap Settings](#) (Параметры системных прерываний SNMP).

Таблица 6-44. Команды консоли для настройки параметров системных прерываний SNMP.

Команда консоли	Описание
snmp-server enable traps	Разрешает устройству отправлять системные прерывания SNMP или уведомления SNMP.
snmp-server trap authentication	Разрешает устройству отправлять системные прерывания SNMP при ошибке проверки подлинности.
snmp-server host адрес_хоста строка_сообщества [1 2]	Определяет тип системных прерываний, отправляемых выбранному получателю.
show snmp	Отображает состояние соединения 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)# snmp-server enable traps		
console(config)# snmp-server trap authentication		
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
-----	-----	-----
1.1.1.1	public_1	1
2.2.2.2	public_2	2
System Contact: 345 6789		
System Location: 1234 5678		
console#		

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:

- 1 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 или резервного файла настройки.
- 1 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.
- 1 Backup Configuration File (Резервный файл настройки) - содержит резервную копию настройки устройства. Резервный файл настройки изменяется, когда в него копируется файл рабочей настройки или файл для запуска. Копируемые в файл команды заменяют существующие команды, сохраненные в резервном файле. Содержимое резервного файла можно скопировать либо в файл рабочей настройки, либо в файл настройки запуска.
- 1 Файлы образа - системные образы сохраняются в двух файлах Flash, называемых образами (Image 1 и Image 2). Активный образ хранит 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.

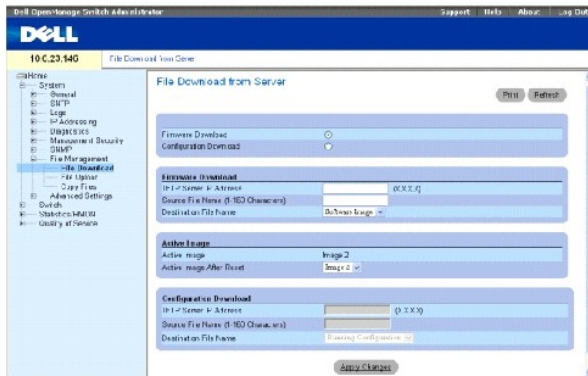
Чтобы открыть страницу File Management (Управление файлами), выберите System (Система)→ File Management (Управление файлами) на панели дерева. Страница File Management (Управление файлами) содержит следующие ссылки:

- 1 File Download (Загрузка файлов)
- 1 File Upload (Передача файлов)
- 1 Copy Files (Копирование файлов)

Загрузка файлов

Страница [File Download From Server](#) (Загрузка файлов с сервера) содержит поля для загрузки системного образа и файлов настройки с сервера TFTP 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. 6-76. Страница File Download from Server (Загрузка файлов с сервера)



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.

Firmware Download TFTP Server IP Address (IP-адрес сервера TFTP для загрузки микропрограмм) - IP-адрес сервера TFTP, с которого загружаются файлы.

Firmware Download Source File Name (Имя исходного файла микропрограммы для загрузки) - файл микропрограммы для загрузки.

Firmware Download Destination File (Целевой файл микропрограммы для загрузки) - тип файла, в который будет загружен файл. Возможные значения:

Software Image (Образ программы) - загружает файл образа.

Boot Code (Код загрузки) - загружает загрузочный файл.

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 File TFTP Server IP Address (IP-адрес сервера TFTP для загрузки файла настройки) - IP-адрес сервера TFTP, с которого загружаются файлы настройки.

Configuration Download File Source File Name (Имя исходного файла для загрузки конфигурации) - показывает файлы настройки, доступные для загрузки.

Configuration Download File Destination (Целевой файл настройки) - файл, в который загружается 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.

Backup Configuration (Резервная настройка) - загружается и переписывается файл резервной настройки.

Загрузка файлов с сервера:

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.



ПРИМЕЧАНИЕ. Для активизации выбранного файла образа перезагрузите устройство. Подробнее о перезагрузке устройства см. в разделе [«Восстановление заводских параметров устройства»](#).

Загрузка файлов с сервера с помощью команд консоли

В следующей таблице приведены команды консоли для настройки полей, отображаемых на странице [File Download From Server](#) (Загрузка файлов с сервера).

Таблица 6-45. Команды консоли для загрузки файлов

Команда консоли	Описание
copy url_источника url_назначения [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

■ ПРИМЕЧАНИЕ. Каждый знак «!» свидетельствует об успешной передаче десяти пакетов.

Accessing file 'file1' on 172.16.101.101.

Loading file1 from 172.16.101.101: !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

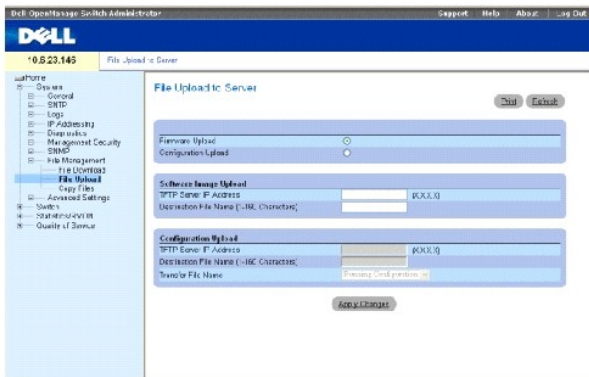
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK]

Copy took 0:01:11 [hh:mm:ss]
```

Передача файлов на сервер

Страница [File Upload to Server](#) (Загрузка файла на сервер) содержит поля для загрузки программного обеспечения с сервера TFTP на устройство. Файл образа также можно передать со страницы [File Upload to Server](#) (Передача файлов на сервер). Чтобы открыть страницу [File Upload to Server](#) (Передача файлов на сервер), выберите System (Система) → File Management (Управление файлами) → File Upload (Передача файла) на панели дерева.

Рис. 6-77. Страница File Upload to Server (Передача файлов на сервер)



Firmware Upload (Передача микропрограммы) - передается файл микропрограммы. Если выбран параметр **Firmware Upload** (Передача микропрограммы), поля **Configuration Upload** (Передача настройки) недоступны.

Configuration Upload (Передача настройки) - передается файл настройки. Если выделено поле **Configuration Upload**, то поля **Software Image Upload** (Загрузка образа с сервера) недоступны.

Software Image Upload TFTP Server IP Address (IP-адрес сервера TFTP для передачи образа программы) - IP-адрес сервера TFTP, на который передается образ программы.

Software Image Upload Destination (Место назначения передачи образа программы) - путь к файлу образа программы, из которого передается файл.

Configuration Upload TFTP Server IP Address (IP-адрес сервера TFTP для передачи настройки) - IP-адрес сервера TFTP, на который передается файл настройки.

Configuration Upload Destination (Место назначения передачи настройки) - определяет путь, по которому выполняется передача файла настройки.

Configuration Upload Transfer file name (Имя передаваемого файла настройки) - программный файл, в который выполняется передача настройки.
Возможные значения:

Running Configuration (Рабочая настройка) - передает текущий файл настройки.

Startup Configuration (Настройка для запуска) - передает файл настройки для запуска.

Backup Configuration (Резервная настройка) - передает файл резервной настройки.

Передача файлов

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).

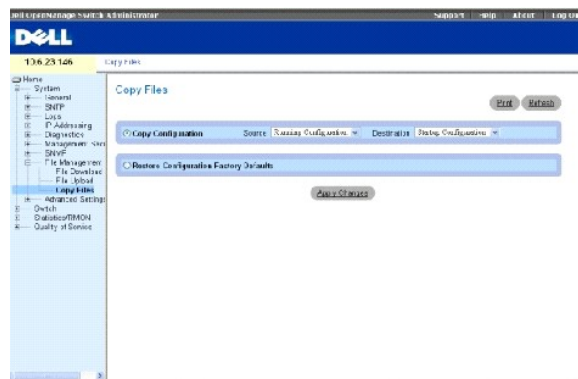
Таблица 6-46. Команды консоли для передачи файлов

Команда консоли	Описание
copy url_источника url_назначения [snmp]	Копирует файл из исходного местоположения в место назначения.

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. 6-78. Страница Copy Files (Копирование файлов)



Copy Configuration (Копировать настройку) - когда установлен этот флажок, выполняется копирование файлов рабочей настройки, настройки запуска или резервной настройки. Возможные значения:

Source (Источник) - выполняется копирование файлов рабочей настройки, настройки запуска или резервной настройки.

Destination (Назначение) - файл, в который копируется файл рабочей настройки, настройки для запуска или резервной 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. Определите поля **Source** (Источник) и **Destination** (Назначение).
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Файл будет скопирован, а устройство обновлено.

Восстановление заводских настроек по умолчанию

1. Откройте страницу [Copy Files](#) (Копирование файлов).
2. Выберите **Restore Company Factory Defaults** (Восстановить заводские файлы настройки).
3. Нажмите кнопку **Apply Changes** (Применить изменения).

Заводские настройки по умолчанию будут восстановлены, а устройство обновлено.

Копирование и удаление файлов с помощью команд консоли

В следующей таблице приведены команды консоли для настройки полей, отображаемых на странице [Copy Files](#) (Копирование файлов).

Таблица 6-47. Команды консоли для копирования файлов

Команда консоли	Описание
copy url_источника url_приемника [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
```

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) содержит 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. 6-79. Страница 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 (20-400)) - 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.

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).

Таблица 6-48. Команды консоли для общих параметров

Команда консоли	Описание
logging buffered size число	Задаёт число системных сообщений, хранящихся во внутреннем буфере (ОЗУ).
port jumbo-frame	Включает поддержку больших кадров для устройства.

Далее приведен пример команд консоли.

```
Console (config)# logging  
buffered size 300
```

[Назад на страницу «Содержание»](#)

[Назад на страницу «Содержание»](#)

Руководство пользователя системы Dell™ PowerConnect™ 5324



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



ЗАМЕЧАНИЕ. ЗАМЕЧАНИЕ указывает на потенциальную опасность повреждения оборудования или потери данных и объясняет, как этого избежать.



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

Информация, включенная в состав данного документа, может быть изменена без уведомления.
© Dell Inc., 2003 - 2004. Все права защищены.

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

Товарные знаки, использованные в этом документе: *Dell*, *Dell OpenManage*, логотип *DELL*, *Inspiron*, *Dell Precision*, *Dimension*, *OptiPlex*, *PowerConnect*, *PowerApp*, *PowerVault*, *Axim*, *DellNet* и *Latitude* являются товарными знаками корпорации Dell Inc. *Microsoft* и *Windows* являются охраняемыми товарными знаками корпорации Майкрософт.

В данном документе могут быть упомянуты также другие товарные знаки и торговые наименования для ссылок на организации, обладающие этими товарными знаками или наименованиями, либо на их изделия. Корпорация Dell Inc. отказывается от всех прав собственности на любые товарные знаки и названия, кроме своих собственных.

Апрель 2004 Ред. А00

[Назад на страницу «Содержание»](#)

[Назад на страницу содержания](#)

Использование Dell OpenManage Switch Administrator

Руководство пользователя системы Dell™ PowerConnect™ 5324

- [Элементы интерфейса](#)
- [Использование кнопок программы Switch Administrator](#)
- [Запуск приложения](#)
- [Доступ к устройству с помощью команд консоли](#)
- [Использование режима командной строки](#)

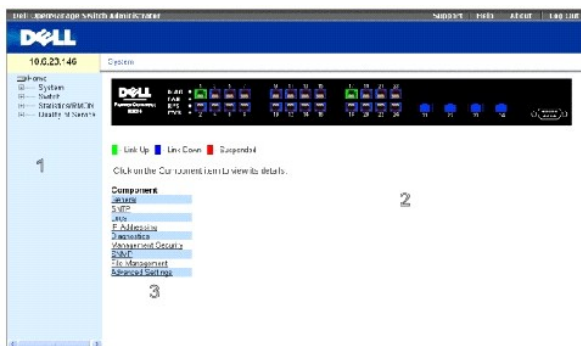
В этом разделе представлено описание интерфейса пользователя.

Элементы интерфейса

Домашняя страница содержит следующие панели:

- 1 Панель дерева — расположена в левой части домашней страницы и представляет собой развертываемое дерево параметров и их компонентов.
- 1 Панель устройства — расположена с правой стороны домашней страницы и отображает вид устройства, информационную или табличную область и инструкции по настройке.

Рис. 5-13. Компоненты программы Switch Administrator



В [таблице 5-7](#) приведен список компонентов интерфейса с соответствующими номерами.

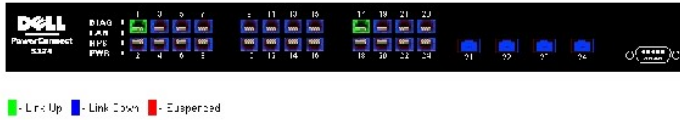
Таблица 5- 7. Компоненты интерфейса

Компонент	Название
1	Панель дерева содержит список различных параметров устройства. Ветви дерева можно раскрывать для просмотра всех компонентов параметра или сворачивать, скрывая эти компоненты. Чтобы расширить панель дерева для просмотра полного названия компонента, перетащите вертикальную полосу вправо.
2	На панели устройства приведены сведения о портах устройства, текущей настройке и состоянии устройства, табличная информация и компоненты параметров. 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. 5-14. Индикаторы портов



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

Таблица 5-8. 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 [«Определения 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 справке, а также к информации об интерфейсах OpenManage Switch Administrator.

Таблица 5-9. 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.
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 5-10. Кнопки управления устройством

Кнопка	Описание
--------	----------


Apply Changes (Применить изменения)	Применяет заданные изменения для устройства.
Add (Добавить)	Добавляет информацию в таблицы или диалоговые окна.
Telnet	Запускает сеанс Telnet.
Query (Запрос)	Запрашивает таблицы.
Show All (Показать все)	Отображает таблицы устройств.
Стрелка влево и стрелка вправо	Перемещает информацию между списками.
Refresh (Обновить)	Обновляет информацию об устройстве.
Reset All Counters (Сбросить все счетчики)	Сбрасывает статистические счетчики.
Print (Печать)	Распечатывает страницу Network Management System (Система сетевого управления) и табличную информацию.
Show 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. Щелкните на кнопке ОК.

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 **ОК**, чтобы начать сеанс Telnet.

Использование режима командной строки

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:

```
Порт консоли>
```

 **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 «m1ist», настройки двух интерфейсов управления (ethernet g1 и ethernet g9), а также активации списка доступа:

```
Console (config)# management access-list m1ist
```

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

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

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

```
Console (config)# management access-class m1ist
```

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 «Содержание»](#)


[Назад на страницу Содержание](#)

Просмотр статистики

Руководство пользователя системы Dell™ PowerConnect™ 5324

- [Просмотр таблиц](#)
- [Просмотр статистики удаленного мониторинга RMON](#)
- [Просмотр диаграмм](#)

На страницах **статистики** приведена информация для интерфейса, GVRP, Etherlike, RMON и использования устройства. Чтобы открыть страницу **статистики**, щелкните Statistics (Статистика) на панели дерева.

 **ПРИМЕЧАНИЕ.** Команды консоли доступны не для всех страниц статистики.

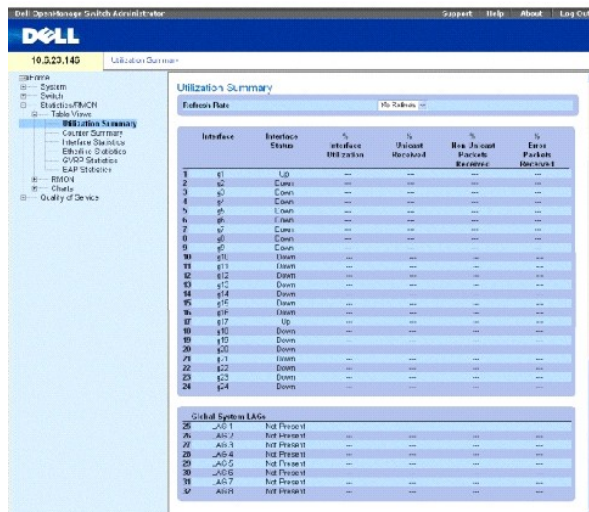
Просмотр таблиц

Страница Table Views (Просмотр в виде таблиц) содержит ссылки для отображения статистики в графическом виде. Чтобы открыть страницу, 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. 8-115. Utilization Summary (Общие сведения по использованию)



Refresh Rate	Interface	Interface Status	% Interface Utilization	% Packet Received	% Packets Discarded	% Error Packets Discarded
1	E1	Up	---	---	---	---
2	E2	Down	---	---	---	---
3	E3	Down	---	---	---	---
4	E4	Down	---	---	---	---
5	E5	Down	---	---	---	---
6	E6	Down	---	---	---	---
7	E7	Down	---	---	---	---
8	E8	Down	---	---	---	---
9	E9	Down	---	---	---	---
10	E10	Down	---	---	---	---
11	E11	Down	---	---	---	---
12	E12	Down	---	---	---	---
13	E13	Down	---	---	---	---
14	E14	Down	---	---	---	---
15	E15	Down	---	---	---	---
16	E16	Down	---	---	---	---
17	E17	Up	---	---	---	---
18	E18	Down	---	---	---	---
19	E19	Down	---	---	---	---
20	E20	Down	---	---	---	---
21	E21	Down	---	---	---	---
22	E22	Down	---	---	---	---
23	E23	Down	---	---	---	---
24	E24	Down	---	---	---	---

Global System LAGs	LAG ID	LAG Status	% Utilization	% Packet Received	% Packets Discarded	% Error Packets Discarded
25	LAG1	Not Present	---	---	---	---
26	LAG2	Not Present	---	---	---	---
27	LAG3	Not Present	---	---	---	---
28	LAG4	Not Present	---	---	---	---
29	LAG5	Not Present	---	---	---	---
30	LAG6	Not Present	---	---	---	---
31	LAG7	Not Present	---	---	---	---
32	LAG8	Not Present	---	---	---	---

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), щелкните **Statistics/RMON** (Статистика/RMON) → **Table Views** (Просмотр в виде таблиц) → **Counter Summary** (Сводка по счетчикам) на панели дерева.

Рис. 8-116. Counter Summary (Сводка по счетчикам)

Interface	Interface Status	Received Packets	Transmitted Packets	Received Bytes	Transmitted Bytes	Received Errors	Transmitted Errors
0	Up	1175	262	0	136	0	0
1	Down	0	0	0	0	0	0
2	Down	0	0	0	0	0	0
3	Down	0	0	0	0	0	0
4	Down	0	0	0	0	0	0
5	Down	0	0	0	0	0	0
6	Down	0	0	0	0	0	0
7	Down	0	0	0	0	0	0
8	Down	0	0	0	0	0	0
9	Down	0	0	0	0	0	0
10	Down	0	0	0	0	0	0
11	Down	0	0	0	0	0	0
12	Down	0	0	0	0	0	0
13	Down	0	0	0	0	0	0
14	Down	0	0	0	0	0	0
15	Down	0	0	0	0	0	0
16	Down	0	0	0	0	0	0
17	Up	6220	636	33600	6	0	0
18	Down	0	0	0	0	0	0
19	Down	0	0	0	0	0	0
20	Down	0	0	0	0	0	0
21	Down	0	0	0	0	0	0
22	Down	0	0	0	0	0	0
23	Down	0	0	0	0	0	0
24	Down	0	0	0	0	0	0

LAG ID	LAG Name	Received Packets
0	LAG0	0
1	LAG1	0
2	LAG2	0
3	LAG3	0
4	LAG4	0
5	LAG5	0
6	LAG6	0
7	LAG7	0
8	LAG8	0

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.

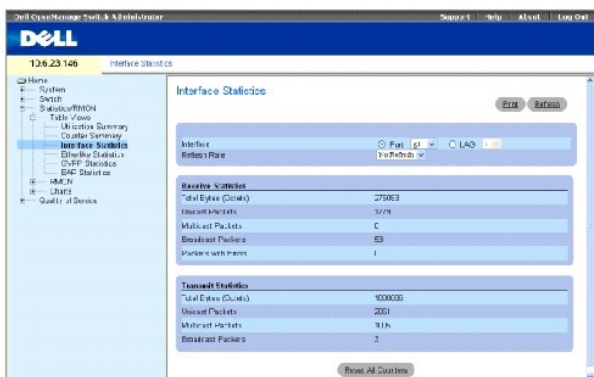
Received Errors (Получено пакетов с ошибками) - число пакетов с ошибками, полученных на интерфейс.

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 таблицы) → [Interface Statistics](#) (Статистика интерфейса) на панели дерева.

Рис. 8-117. 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 ошибок, 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 8-80. Команды консоли для статистики интерфейса

Команда консоли	Описание
<code>show interfaces counters [ethernet <i>интерфейс</i> port-channel <i>порт-канал-номер</i>]</code>	Отображает трафик, видимый физическим интерфейсом.

Далее приведен пример команд консоли.

```
Console> enable
Console# show interfaces counters
```

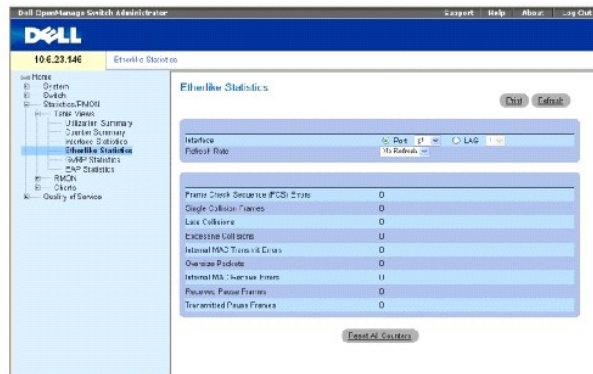
Port	InOctets	InUcastPkts	InMcastPkts	InBcastPkts
---	-----	-----	-----	-----
---	---	---	---	---
-				
g1	183892	1289	987	8
g2	0	0	0	0

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. 8-118. 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.

Multiple Collision Frames (Кадры с множественными коллизиями) - число множественных коллизий в кадрах, полученных на выбранный интерфейс.

Single Quality Error (SQE) Test Errors (Ошибки проверки SQE) - число ошибок проверки SQE, полученных на выбранный интерфейс.

Deferred Transmissions (Отвергнутые передачи) - число отсроченных передач на выбранный интерфейс.

Late Collisions (Последние коллизии) - число последних коллизий, полученных на выбранный интерфейс. **Excessive Collisions** (Чрезмерные коллизии) - число чрезмерных коллизий, полученных на выбранный интерфейс.

Internal MAC Transmit Errors (Внутренние ошибки передачи MAC) - число внутренних ошибок управления доступом к среде передачи (Internal MAC Transmit), полученных на выбранный интерфейс.

Carrier Sense Errors (Ошибки контроля несущей) - число ошибок контроля несущей, полученных на выбранный интерфейс.

Oversize Packets (Превышение размера пакетов) - число ошибок слишком больших пакетов, полученных на выбранный интерфейс.

Internal MAC Receive Errors (Внутренние ошибки приема MAC) - число внутренних ошибок MAC-сигнала, полученных на выбранный интерфейс.

Single Quality Errors (SQE) Test Errors (Ошибки проверки SQE) - число ошибок проверки SQE, 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 8-81. Команды консоли статистики Etherlike

Команда консоли	Описание
<code>show interfaces counters [ethernet интерфейс port-channel порт-канал-номер]</code>	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

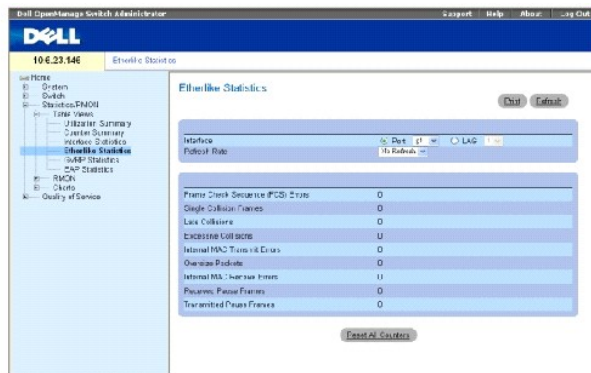
Received Pause Frames: 0

Transmitted Pause Frames: 0

Просмотр статистики протокола GVRP

На странице [GVRP Statistics](#) (Статистика GVRP) показана статистика для протокола GVRP. Чтобы открыть эту таблицу, щелкните [Statistics/RMON](#) (Статистика/RMON) → [Table Views](#) (Просмотр в виде таблиц) → [GVRP Statistics](#) (Статистика интерфейса).

Рис. 8-119. GVRP Statistics (Статистика GVRP)



The screenshot shows the Dell OpenManage Switch Administrator interface. The main content area displays the 'Filterable Statistics' table for the selected interface. The table lists various statistics and their values, all of which are 0.

Interface	Port of Role
Frame Check Sequence (FCS) Errors	0
Single Collision Frames	0
Late Collisions	0
Excessive Collisions	0
Internal MAC Tx Errors	0
Oversize Packets	0
Internal MAC Rx Errors	0
Received Pause Frames	0
Transmitted Pause Frames	0

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 8-82. Команды консоли для просмотра статистики GVRP

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

Console# show gvrp error-statistics					
GVRP error statistics:					

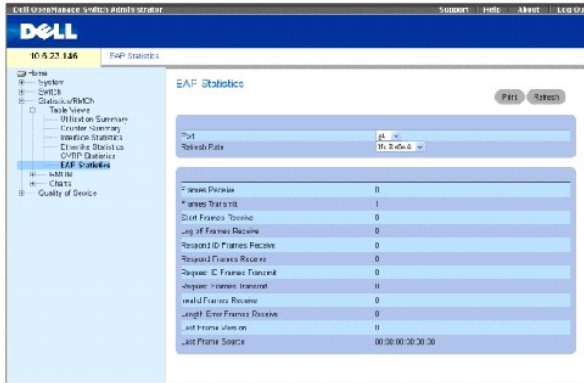
Legend:					
INVPROT : Invalid Protocol ID			INVPLEN : Invalid PDU Length		
INVATYP : Invalid Attribute Type			INVALEN : Invalid Attribute Length		
INVAVAL : Invalid Attribute Value			INVEVENT : Invalid Event		
Port	INVPROT	INVATYP	INVAVAL	INVALEN	INVEVENT

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. 8-120. 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 разрегистрации) - число кадров Log off по протоколу EAPOL, полученных на порте.

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 (Получено неверный кадр) - 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 8-83. Команды консоли для просмотра статистики GVRP

Команда консоли	Описание
<code>show dot1x statistics ethernet <i>интерфейс</i></code>	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

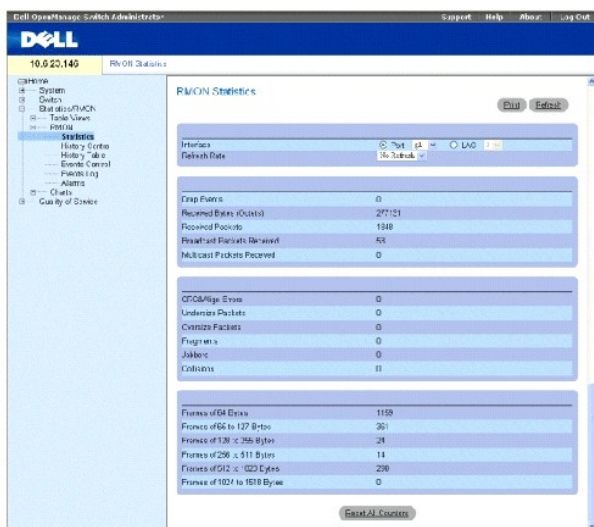
Просмотр статистики удаленного мониторинга RMON

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 (Статистика RMON) содержит поля для просмотра информации по использованию устройства и возникающие на нем ошибки. Чтобы открыть страницу RMON Statistics (Статистика RMON), щелкните Statistics/RMON (Статистика/RMON) → RMON → Statistics (Статистика) на панели дерева.

Рис. 8-121. Статистика 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 длинее 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 - Number of xx (Кадры из xx байт) - число xx-байтовых кадров, полученных на интерфейс с момента последнего обновления устройства.

Просмотр статистики интерфейса

1. Откройте страницу [RMON Statistics](#) (Статистика RMON).
2. Выберите тип и номер интерфейса в поле **Interface** (Интерфейс).

Отобразится статистика интерфейса.

Просмотр статистики удаленного мониторинга с помощью команд консоли

В следующей таблице приведены команды консоли для просмотра статистики интерфейса RMON.

Таблица 8-84. Команды консоли для просмотра статистики RMON

Команда консоли	Описание
<code>show rmon statistics {ethernet интерфейс port-channel порт-канал-номер}</code>	Отображает статистику удаленного мониторинга по Ethernet.

Далее приведен пример команд консоли.

```
console> enable
```

```
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

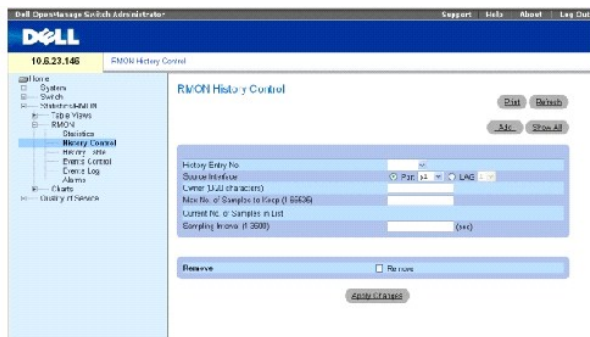
512 to 1023 Octets: 491 1024 to 1518 Octets: 389

```

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. 8-122. 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 RMON.

Max No. of Samples to Keep (1-65535) (Максимальное число выборок для хранения (1-65535)) - число сохраняемых выборок. Значение по умолчанию: 50.

Current No. of Samples in List (Текущее число выборок) - текущее количество полученных выборок.

Sampling Interval (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** (таблицы управления журналом).

Добавление записи управления журналом

1. Откройте страницу [RMON History Control](#) (Управление журналом удаленного мониторинга).
2. Щелкните на кнопке **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 таблицы 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 таблицы 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 8-85. Команды консоли журнала удаленного мониторинга

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

<code>rmon collection history</code> <i>индекс</i> [<i>owner имя владельца</i> <i>buckets номер_блока</i>] [<i>interval секунды</i>]	Включает и настраивает удаленный мониторинг на интерфейсе.
<code>show rmon collection history</code> [<i>ethernet интерфейс</i> <i>port-channel порт-канал-номер</i>]	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

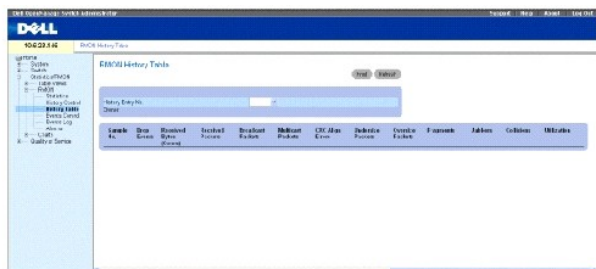
Console(config)# exit

```

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. 8-123. Журнал 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 длиной 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 больше допустимого) - число пакетов, полученных во время сеанса выборки, с длиной больше 1518 октетов.

Fragments (Фрагменты) - число пакетов, полученных во время сеанса выборки, с длиной меньше 64 октетов и содержащих контрольную последовательность кадра.

Jabbers (Сбойные пакеты) - число пакетов, полученных во время сеанса выборки, с длиной больше 1518 октетов и содержащих контрольную последовательность кадра.

Collisions (Коллизии) - оценка общего количества коллизий пакетов, имевших место во время сеанса выборки. Коллизии обнаруживаются, когда порты повторителя 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 таблицы 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 8-86. 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
```

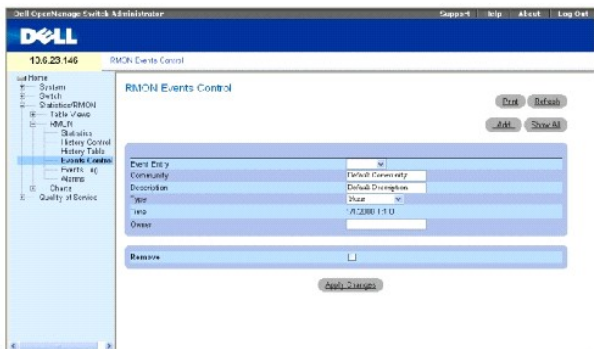
Sample Set: 1	Owner: CLI
Interface: g1	Interval: 1800
Requested samples: 50	Granted samples: 50
Maximum table size: 500	

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. 8-124. 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.

Типе (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. Щелкните на кнопке **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 событий **Event Table**.
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 8-87. Команды консоли для определения событий устройств

Команда консоли	Описание
<code>gmon event тип индекса [community текст сообщества] [description текст описания] [owner имя владельца]</code>	Настраивает события удаленного мониторинга.
<code>show gmon events</code>	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

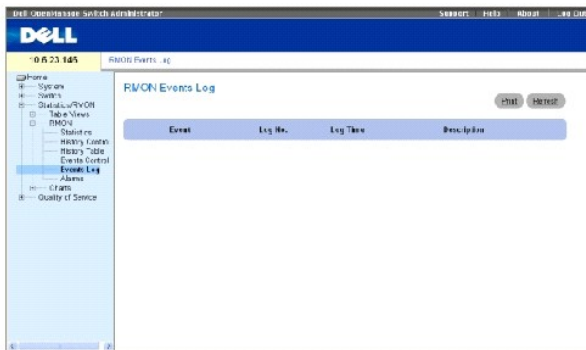
```

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. 8-125. 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 8-88. 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

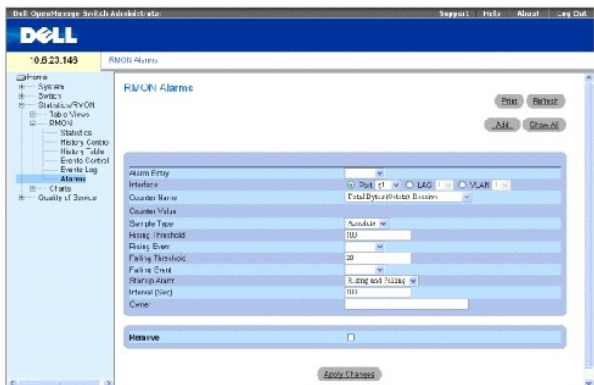
```
Console# show rmon log
```

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. 8-126. RMON Alarms (Сигналы удаленного мониторинга)



Alarm Entry (Запись сигнала) - показывает определенный сигнал.

Interface (Интерфейс) - указывает порт, для которого отображается статистика RMON.

Counter Name (Имя счетчика) - показывает выбранную переменную MIB.

Counter Value (Значение счетчика) - значение выбранной переменной MIB.

Sample Type (Тип выборки) - определяет метод выборки для выбранной переменной и сравнивает значение с пороговыми величинами. Возможные значения:

Delta (Разность) - вычитается последнее значение выборки из текущего значения. Разница значений сравнивается с пороговой величиной.

Absolute (Абсолютное значение) - сравнивает значения с пороговыми величинами в конце интервала выборки.

Rising Threshold (Превышение порога) - значение счетчика превышения, активирующее 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, активирующее 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, активирующий 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. Щелкните на кнопке **Add** (Добавить).

Откроется страница **Add an Alarm Entry** (Добавление записи журнала):

Рис. 8-127. Страница Add an Alarm Entry (Добавление записи журнала)

Alarm Entry	1
Interface	Port 1
Counter Name	Total Bytes (Cores) Receive
Sample Type	Absolute
Rising Threshold	100
Rising Event	
Falling Threshold	20
Falling Event	
Startup Alarm	Rising and Falling
Interval	100
Owner	

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 8-89. Команды консоли для сигналов устройств

Команда консоли	Описание
<code>rmon alarm индекс переменная интервал порог_верх порог_нижн верх_событие нижн_событие [type тип] [startup направление] [owner имя]</code>	Настраивает условия выдачи сигналов удаленного мониторинга.
<code>show rmon alarm-table</code>	Отображает сводную таблицу сигналов.
<code>show rmon alarm</code>	Отображает конфигурацию сигналов удаленного мониторинга.

Далее приведен пример команд консоли.

```

console> enable

console# config

Console (config)# rmon alarm 1000 dell 360000 1000000 1000000 10 20

Console# show rmon alarm-table

```

Index	OID	Owner
-----	-----	-----

1	1.3.6.1.2.1.2.2.1.1 0.1	CLI
2	1.3.6.1.2.1.2.2.1.1 0.1	Manager
3	1.3.6.1.2.1.2.2.1.1 0.9	CLI

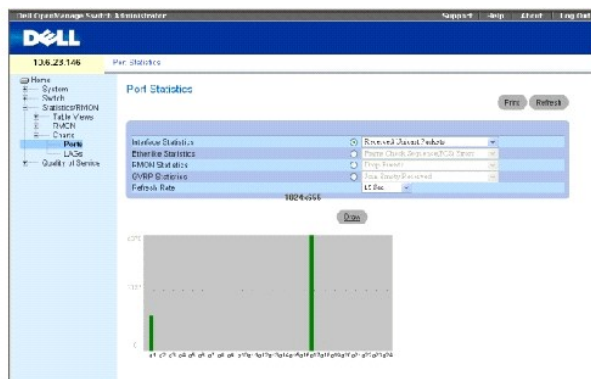
Просмотр диаграмм

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](#), щелкните [Statistics](#) (Статистика) → [Charts](#) (Диаграммы) → [Ports](#) (Порты) на панели дерева.

Рис. 8-128. Статистика порта



Interface Statistics (Статистика интерфейса) - выбор типа статистики интерфейса для открытия.

Etherlike Statistics (Статистика интерфейса) - выбор типа статистики Etherlike для открытия.

RMON Statistics (Статистика интерфейса) - выбор типа статистики RMON для открытия.

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 8-90. Команды консоли статистики портов

Команда консоли	Описание
show interfaces counters [ethernet интерфейс port-channel порт-канал-номер]	Отображает трафик, видимый физическим интерфейсом.
show rmon statistics { ethernet интерфейс port-channel порт-канал-номер }	Отображает статистику удаленного мониторинга по Ethernet.
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.

```

Console# show interfaces
description ethernet g1

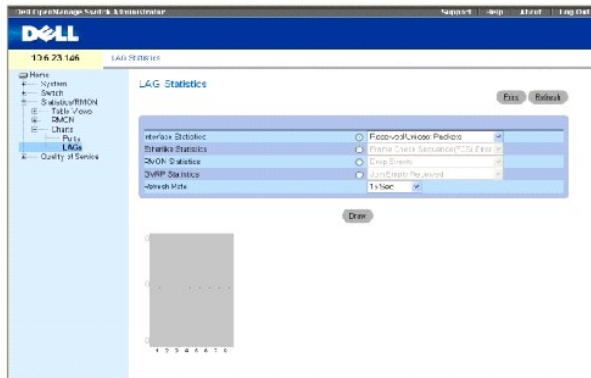
```

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. 8-129. LAG Statistics (Статистика LAG)



Interface Statistics (Статистика интерфейса) - выбор типа статистики интерфейса для открытия.

Etherlike Statistics (Статистика интерфейса) - выбор типа статистики Etherlike для открытия.

RMON Statistics (Статистика интерфейса) - выбор типа статистики RMON для открытия.

GVRP Statistics (Статистика) - 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 8-91. Команды консоли для статистики LAG

Команда консоли	Описание
show interfaces counters {ethernet <i>интерфейс</i> port-channel <i>порт-канал-номер</i> }	Отображает трафик, видимый физическим интерфейсом.
show rmon statistics {ethernet <i>интерфейс</i> port-channel <i>порт-канал-номер</i> }	Отображает статистику удаленного мониторинга по Ethernet.
show gvrp statistics {ethernet <i>интерфейс</i> port-channel <i>порт-канал-номер</i> }	Отображает статистику протокола GVRP.
show gvrp error-statistics {ethernet <i>интерфейс</i> port-channel <i>порт-канал-номер</i> }	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	0
g2	0	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	0
g4	0	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	0
g6	0	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	0
g8	0	0	0	0	0	0	0	0	0	0	0	0	0