Интерфейсные платы Cisco EtherSwitch HWIC-4ESW и HWIC-D-9ESW

Содержание

Объединение в стек в одном корпусе

Мостовое соединение при отказе

Настройка интерфейсных плат EtherSwitch HWIC

Настройка VLAN

Настройка протокола VLAN Trunking Protocol

Настройка интерфейсов уровня 2

Настройка параметров аутентификации 802.1x

Настройка протокола Spanning Tree

Настройка обработки таблицы MAC-адресов

Настройка протокола Cisco Discovery Protocol

Настройка анализатора коммутируемых портов (SPAN)

Настройка управления электропитанием на интерфейсе

Настройка коммутации с мультиадресной IP-рассылкой уровня 3

Настройка функции IGMP Snooping

Настройка контроля шторма по портам

Настройка стеков

Настройка мостового соединения при отказе

Настройка отдельных подсетей для голоса и данных

Интерфейсные платы Cisco EtherSwitch HWIC-4ESW и HWIC-D-9ESW

В данном документе описаны действия по настройке аппаратных функций высокоскоростной 4-портовой интерфейсной платы Cisco HWIC-4ESW и высокоскоростной 9-портовой интерфейсной платы Cisco HWIC-D-9ESW EtherSwitch для сетей WAN (HWIC), поддерживаемых на маршрутизаторах Cisco 1800 (модульный), Cisco 2800 и Cisco 3800 Series Integrated Services Routers.

Интерфейсные платы Cisco EtherSwitch представляют собой коммутаторы Ethernet 10/100BaseT уровня 2 с поддержкой маршрутизации уровня 3. (Маршрутизация уровня 3 переадресуется на сетевой узел и непосредственно на коммутаторе не выполняется.) Трафик между различными сетями VLAN на коммутаторе осуществляется на платформе маршрутизатора. Любой порт интерфейсной платы Cisco EtherSwitch HWIC можно настроить для использования в качестве объединительного порта связи с другой интерфейсной платой Cisco EtherSwitch HWIC или сетевым модулем EtherSwitch в этой же системе. Для обеспечения питания от линии для IP-телефона можно подключить дополнительный модуль питания. Интерфейсная плата HWIC-D-9ESW устанавливается в слот для сдвоенных плат.

Для этого оборудования не используются новые или измененные команды IOS.

История функциональных возможностей интерфейсных плат Cisco EtherSwitch HWIC-4ESW и HWIC-D-9ESW

Версия	Изменение
12.3(8)T4	Функция впервые появилась

Получение информации о поддержке платформ и образов программного обеспечения Cisco IOS

Для поиска информации о поддержке платформ и образов программного обеспечения Cisco IOS воспользуйтесь инструментом Cisco Feature Navigator. Доступ к инструменту Cisco Feature Navigator можно получить по адресу http://www.cisco.com/go/fn. Необходимо наличие учетной записи на веб-сайте cisco.com. Если у вас нет учетной записи, вы забыли имя пользователя или пароль, то в диалоговом окне входа в систему нажмите кнопку **Cancel** (Отмена) и следуйте дальнейшим указаниям.

Содержание

Информация об интерфейсных платах Cisco EtherSwitch HWIC приводится в следующих разделах:

Предварительные требования для интерфейсных плат EtherSwitch HWIC

Ниже приведены предварительные требования для настройки интерфейсных плат EtherSwitch HWIC.

- Настройка IP-маршрутизации. (См. *Руководство по настройке IP для Cisco IOS*.)

- Для поддержки интерфейсных плат Cisco HWIC-4ESW и Cisco HWIC-D-9ESW необходимо использовать программное обеспечение Cisco IOS версии T (12.3(8)T4 и выше). (См. документацию к Cisco IOS.)

Ограничения для интерфейсных плат EtherSwitch HWIC

К интерфейсным платам Cisco EtherSwitch HWIC-4ESW и Cisco HWIC-D-9ESW применяются следующие ограничения.

- В маршрутизаторе допускается установка не более двух интерфейсных плат Ethernet Switch HWIC или сетевых модулей.

При установке нескольких интерфейсных плат коммутаторов Ethernet или сетевых модулей в маршрутизатор их независимая работа невозможна. Модули необходимо объединить в стек, в противном случае они не будут работать.

- Порты интерфейсной платы Cisco EtherSwitch ЗАПРЕЩАЕТСЯ подключать к встроенным портам Fast Ethernet/Gigabit маршрутизатора.

- На девятом порте (порт 8) интерфейсной платы HWIC-D-9ESW питание от линии отсутствует.

- Если для одного из параметров **speed** или **duplex** не установлено значение **auto**, на девятом порте (порт 8) интерфейсной платы HWIC-D-9ESW поддержка Auto MDIX отключается.

- Вставка и удаление интерфейсных плат EtherSwitch HWIC в процессе работы не поддерживается.

- После установки и настройки коммутаторов Ethernet на маршрутизаторе сетевого узла запрещается производить вставку и удаление в процессе работы карт памяти CompactFlash. После выполнения такой вставки/удаления карт памяти CompactFlash конфигурация коммутаторов Ethernet может быть нарушена.

- Отсечение по протоколу VTP не поддерживается.

- Интерфейсная плата EtherSwitch HWIC поддерживает до 200 защищенных MAC-адресов.

Информация об интерфейсных платах EtherSwitch HWIC

Для настройки интерфейсных плат Cisco EtherSwitch HWIC-4ESW и HWIC-D-9ESW необходимо ознакомиться со следующими понятиями:

- Виртуальные локальные сети (VLAN)

- Питание от линии для IP-телефонов Cisco

- Коммутация Ethernet уровня 2

- Аутентификация 802.1x

- Протокол Spanning Tree Protocol

- Протокол Cisco Discovery Protocol
- Анализатор коммутируемых портов
- Функция IGMP Snooping
- Контроль шторма
- Объединение в стек в одном корпусе
- Мостовое соединение при отказе

Виртуальные локальные сети (VLAN)

Для получения информации о сетях VLAN перейдите по следующему адресу:

/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00801d2d60.html#1047027

Питание от линии для IP-телефонов Cisco

Для получения информации о питании от линии для IP-телефонов Cisco перейдите по следующему адресу:

/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00801d2d60.html#1048439

Коммутация Ethernet уровня 2

Для получения информации о коммутации Ethernet уровня 2 перейдите по следующему адресу:

/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00801d2d60.html#1048478

Аутентификация 802.1x

Для получения информации об аутентификации 802.1x перейдите по следующему адресу:

/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00801d2d60.html#1051006

Протокол Spanning Tree Protocol

Для получения информации о протоколе STP перейдите по следующему адресу:

/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00801d2d60.html#1048458

Протокол Cisco Discovery Protocol

Для получения информации о протоколе Cisco Discovery Protocol перейдите по следующему адресу:

/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00801d2d60.html#1048498

Анализатор коммутируемых портов

Для получения информации об анализаторе коммутируемых портов перейдите по следующему адресу:

/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00801d2d60.html#1053663

Функция IGMP Snooping

Для получения информации о функции IGMP Snooping перейдите по следующему адресу:

/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00801d2d60.html#1053727

Контроль шторма

Для получения информации о контроле шторма перейдите по следующему адресу:

/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00801d2d60.html#1051018

Объединение в стек в одном корпусе

Для получения информации об объединении в стек в одном корпусе перейдите по следующему адресу:

/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00801d2d60.html#1051061

Мостовое соединение при отказе

Для получения информации о мостовом соединении при отказе перейдите по следующему адресу:

/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00801d2d60.html#1054833

Настройка интерфейсных плат EtherSwitch HWIC

Задачи по настройке интерфейсных плат EtherSwitch HWIC см. в следующих разделах.

- Настройка VLAN
- Настройка протокола VLAN Trunking Protocol
- Настройка интерфейсов уровня 2
- Настройка параметров аутентификации 802.1x
- Настройка протокола Spanning Tree
- Настройка обработки таблицы MAC-адресов
- Настройка протокола Cisco Discovery Protocol

- Настройка анализатора коммутируемых портов (SPAN)
- Настройка управления электропитанием на интерфейсе
- Настройка коммутации с мультиадресной IP-рассылкой уровня 3
- Настройка функции IGMP Snooping
- Настройка контроля шторма по портам
- Настройка стеков
- Настройка мостового соединения при отказе
- Настройка отдельных подсетей для голоса и данных
- Управление интерфейсными платами EtherSwitch HWIC

Настройка VLAN

В данном разделе содержится информация по настройке сетей VLAN на коммутаторе. В него включены следующие подразделы:

- Добавление экземпляров сетей VLAN
- Удаление экземпляра сети VLAN из базы данных

Добавление экземпляров сетей VLAN

Интерфейсная плата EtherSwitch HWIC поддерживает до 15 сетей VLAN.

Войдите в привилегированный режим EXEC и выполните следующие действия для настройки интерфейса Fast Ethernet с доступом уровня 2.

СВОДКА ШАГОВ

1. vlan database

2. vlan *vlan_id*

3. exit

ПОДРОБНОЕ ОПИСАНИЕ ШАГОВ

	Команда	Назначение
Шаг 1	`Router#vlan database`	Вход в режим настройки сети VLAN.

Шаг 2	`Router(vlan)#vlan vlan_id`	Добавление Ethernet VLAN.
Шаг 3	`Router(vlan)#exit`	Обновление базы данных сетей VLAN, распространение новых данных в административном домене и возврат в привилегированный режим EXEC.

Проверка конфигурации сети VLAN

Для проверки конфигурации сети VLAN можно использовать режим базы данных VLAN.

Для проверки конфигурации сети VLAN в режиме базы данных VLAN используйте команду **show**, как показано ниже.

```
Router(vlan)#show

 VLAN ISL Id: 1

 Name: default

 Media Type: Ethernet

 VLAN 802.10 Id: 100001

 State: Operational

 MTU: 1500

 Translational Bridged VLAN: 1002

 Translational Bridged VLAN: 1003



 VLAN ISL Id: 2

 Name: VLAN0002

 Media Type: Ethernet

 VLAN 802.10 Id: 100002

 State: Operational

 MTU: 1500



 VLAN ISL Id: 3

 Name: Red_VLAN

 Media Type: Ethernet

 VLAN 802.10 Id: 100003
```

State: Operational

MTU: 1500

VLAN ISL Id: 1002

Name: fddi-default

Media Type: FDDI

VLAN 802.10 Id: 101002

State: Operational

MTU: 1500

Bridge Type: SRB

Translational Bridged VLAN: 1

Translational Bridged VLAN: 1003

VLAN ISL Id: 1003

Name: token-ring-default

Media Type: Token Ring

VLAN 802.10 Id: 101003

State: Operational

MTU: 1500

Bridge Type: SRB

Ring Number: 0

Bridge Number: 1

Parent VLAN: 1005

Maximum ARE Hop Count: 7

Maximum STE Hop Count: 7

Backup CRF Mode: Disabled

Translational Bridged VLAN: 1

Translational Bridged VLAN: 1002

```
 VLAN ISL Id: 1004

  Name: fddinet-default

 Media Type: FDDI Net

 VLAN 802.10 Id: 101004

 State: Operational

 MTU: 1500

 Bridge Type: SRB

 Bridge Number: 1

 STP Type: IBM


 VLAN ISL Id: 1005

 Name: trnet-default

 Media Type: Token Ring Net

 VLAN 802.10 Id: 101005

 State: Operational

 MTU: 1500

 Bridge Type: SRB

 Bridge Number: 1

 STP Type: IBM


router(vlan)# exit

APPLY completed.

Exiting....

router#

router#
```

В привилегированном режиме EXEC при помощи интерфейса командной строки Cisco IOS введите команду **show vlan-switch** для проверки конфигурации сети VLAN, как показано ниже.

```
router#show vlan-switch

VLAN Name                             Status    Ports
```

```
---- -------------------------------- --------- -------------------------------

1    default                          active    Fa0/1/1, Fa0/1/2, Fa0/1/3, Fa0/1/4

                                                Fa0/1/5, Fa0/1/6, Fa0/1/7, Fa0/1/8

                                                Fa0/3/0, Fa0/3/2, Fa0/3/3, Fa0/3/4

                                                Fa0/3/5, Fa0/3/6, Fa0/3/7, Fa0/3/8

2    VLAN0002                         active    Fa0/1/0

3    Red_VLAN                         active

1002 fddi-default                     active

1003 token-ring-default               active

1004 fddinet-default                  active

1005 trnet-default                    active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2

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

1    enet  100001     1500  -      -      -        -    -        1002   1003

2    enet  100002     1500  -      -      -        -    -        0      0

3    enet  100003     1500  -      -      -        -    -        0      0

1002 fddi  101002     1500  -      -      -        -    -        1      1003

1003 tr    101003     1500  1005   0      -        -    srb      1      1002

1004 fdnet 101004     1500  -      -      1        ibm  -        0      0

1005 trnet 101005     1500  -      -      1        ibm  -        0      0

router#
```

Удаление экземпляра сети VLAN из базы данных

Невозможно удалить сети VLAN по умолчанию для различных типов сред, а именно: Ethernet VLAN 1, FDDI, Token Ring VLAN 1002 —1005.

Войдите в привилегированный режим EXEC и выполните следующие действия для удаления сети VLAN из базы данных.

СВОДКА ШАГОВ

1. vlan database

2. no vlan *vlan_id*

3. exit

ПОДРОБНОЕ ОПИСАНИЕ ШАГОВ

	Команда	Назначение
Шаг 1	`Router#vlan database`	Вход в режим настройки сети VLAN.
Шаг 2	`Router(vlan)#no vlan` *`vlan_id`*	Удаление сети VLAN.
Шаг 3	`Router(vlan)#exit`	Обновление базы данных сетей VLAN, распространение новых данных в административном домене и возврат в привилегированный режим EXEC.

Проверка удаления сети VLAN

Можно подтвердить факт удаления сети VLAN из коммутатора в режиме базы данных VLAN.

Для подтверждения удаления сети VLAN в режиме базы данных VLAN из коммутатора используйте команду **show**, как показано ниже.

```
Router(vlan)#show

 VLAN ISL Id: 1

   Name: default

   Media Type: Ethernet

   VLAN 802.10 Id: 100001

   State: Operational

   MTU: 1500

   Translational Bridged VLAN: 1002

   Translational Bridged VLAN: 1003


 VLAN ISL Id: 1002

   Name: fddi-default

   Media Type: FDDI

   VLAN 802.10 Id: 101002
```

```
   State: Operational

   MTU: 1500

   Bridge Type: SRB

   Translational Bridged VLAN: 1

   Translational Bridged VLAN: 1003

<output truncated>



Router(vlan)#
```

В привилегированном режиме EXEC при помощи интерфейса командной строки Cisco IOS введите команду **show vlan-switch brief** для подтверждения удаления сети VLAN из коммутатора, как показано в следующем примере выходных данных команды.

```
Router#show vlan-switch brief



VLAN Name                             Status    Ports

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

1    default                          active    Fa0/1/0, Fa0/1/1, Fa0/1/2

                                                Fa0/1/3, Fa0/1/4, Fa0/1/5

                                                Fa0/1/6, Fa0/1/7, Fa0/1/8

300  VLAN0300                         active

1002 fddi-default                     active

1003 token-ring-default               active

1004 fddinet-default                  active

1005 trnet-default                    active

Router#
```

Настройка протокола VLAN Trunking Protocol

В данном разделе приведена информация по настройке протокола VTP (VLAN Trunking Protocol) на интерфейсной плате EtherSwitch HWIC. Он содержит следующие подразделы.

- Настройка VTP-сервера
- Настройка VTP-клиента

- Отключение протокола VTP (прозрачный режим VTP)
- Проверка протокола VTP

Примечание. Отсечение по протоколу VTP не поддерживается интерфейсными платами EtherSwitch HWIC.

Настройка VTP-сервера

Если коммутатор работает в режиме VTP-сервера, можно изменить настройку сети VLAN и распространить эти данные по всей сети.

Войдите в привилегированный режим EXEC и выполните следующие действия для настройки коммутатора в качестве VTP-сервера.

СВОДКА ШАГОВ

1. vlan database
2. vtp server
3. **vtp domain** domain_*name*
4. **vtp password** password_*value*
5. exit

ПОДРОБНОЕ ОПИСАНИЕ ШАГОВ

	Команда	Назначение
Шаг 1	`Router# vlan database`	Вход в режим настройки сети VLAN.
Шаг 2	`Router(vlan)# vtp server`	Настройка коммутатора в качестве VTP-сервера.
Шаг 3	`Router(vlan)# vtp domain domain_`*`name`*	Задание имени домена VTP, которое может содержать до 32 символов.
Шаг 4	`Router(vlan)# vtp password password_`*`value`*	Задание пароля домена VTP, который может содержать от 8 до 64 символов (необязательно).
Шаг 5	`Router(vlan)# exit`	Выход из режима настройки сети VLAN.

Настройка VTP-клиента

Если коммутатор работает в режиме VTP-клиента, настройку сети VLAN на коммутаторе изменить невозможно. Коммутатор в режиме клиента получает обновления по протоколу VTP от VTP-сервера в административном домене и соответствующим образом изменяет собственные настройки.

СВОДКА ШАГОВ

1. vlan database
2. vtp client
3. exit

ПОДРОБНОЕ ОПИСАНИЕ ШАГОВ

	Команда	Назначение
Шаг 1	`Router# vlan database`	Вход в режим настройки сети VLAN.
Шаг 2	`Router(vlan)# vtp client`	Настройка коммутатора в качестве VTP-клиента.
Шаг 3	`Router(vlan)# exit`	Выход из режима настройки сети VLAN.

Отключение протокола VTP (прозрачный режим VTP)

При настройке на коммутаторе прозрачного режима VTP протокол VTP на коммутаторе отключается. Коммутатор в прозрачном режиме VTP не отправляет обновления VTP и не выполняет других действий при получении обновлений VTP от других коммутаторов.

Войдите в привилегированный режим EXEC и выполните следующие действия для отключения протокола VTP на коммутаторе.

СВОДКА ШАГОВ

1. vlan database
2. vtp transparent
3. exit

ПОДРОБНОЕ ОПИСАНИЕ ШАГОВ

	Команда	Назначение
Шаг 1	`Router# vlan database`	Вход в режим настройки сети VLAN.

Шаг 2	`Router(vlan)# vtp transparent`	Настройка прозрачного режима VTP.
Шаг 3	`Router(vlan)# exit`	Выход из режима настройки сети VLAN.

Проверка протокола VTP

Для проверки состояния VTP используйте команду **show vtp status**.

```
Router# show vtp status



VTP Version                     : 2

Configuration Revision          : 0

Maximum VLANs supported locally : 256

Number of existing VLANs        : 5

VTP Operating Mode              : Server

VTP Domain Name                 :

VTP Pruning Mode                : Disabled

VTP V2 Mode                     : Disabled

VTP Traps Generation            : Disabled

MD5 digest                      : 0xBF 0x86 0x94 0x45 0xFC 0xDF 0xB5 0x70

Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00

Local updater ID is 1.3.214.25 on interface Fa0/0 (first interface found)

Router#
```

Настройка интерфейсов уровня 2

В данном разделе приведена следующая информация по настройке:

- Настройка диапазона интерфейсов (обязательно)
- Создание макроса для диапазона (необязательно)
- Настройка дополнительных функций интерфейса уровня 2 (необязательно)

Настройка диапазона интерфейсов

Для настройки диапазона интерфейсов в режиме глобальной конфигурации используйте команду **interface range**.

Команда	Назначение
Router(config)#**interface range** {**macro** macro_name | **FastEthernet** *interface-id* [**-** *interface-id*] | **vlan** vlan_ID} [**, FastEthernet** *interface-id* [**-** *interface-id*] | **vlan** vlan_ID]	Выберите диапазон интерфейсов, которые необходимо настроить. • Перед символом «тире» необходимо оставлять пробел. Например, команда **interface range fastethernet** 0/<*slot*>/**0 -** 0/<*slot*>/**3** является действительной; команда **interface range fastethernet** 0/<*slot*>/**0-**0/<*slot*>/**3** недопустима. • Можно ввести один макрос или до пяти значений диапазонов, разделенных запятыми. • Значения диапазонов, разделенные запятыми, могут включать в себя сети VLAN и физические интерфейсы. • До и после запятой пробелы оставлять необязательно. • Команда **interface range** поддерживается только на интерфейсах VLAN, настроенных при помощи команды **interface vlan**.

Создание макроса для диапазона

Для создания макроса для диапазона в режиме глобальной конфигурации используйте команду **define interface-range**.

Команда	Назначение
Router(config)#**define interface-range** *macro_name* {**FastEthernet** *interface-id* [- *interface-id*] | {**vlan** *vlan_ID* - *vlan_ID*} | **[, FastEthernet** *interface-id* [- *interface-id*]	Задание макроса для диапазона интерфейсов и сохранение его в памяти NVRAM.

Проверка конфигурации макроса диапазона интерфейсов

Для отображения конфигурации макроса для диапазона интерфейсов используйте команду **show running-configuration**, как показано ниже.

```
Router#show running-configuration | include define

define interface-range first_three FastEthernet0/1/0 - 2
```

Настройка дополнительных функций интерфейса уровня 2

- Инструкции по настройке скорости интерфейса и дуплексного режима
- Настройка скорости интерфейса
- Настройка дуплексного режима интерфейса
- Проверка настройки скорости интерфейса и дуплексного режима
- Настройка описания интерфейса
- Настройка интерфейса Fast Ethernet в качестве магистрального канала уровня 2
- Настройка интерфейса Fast Ethernet с доступом уровня 2

Инструкции по настройке скорости интерфейса и дуплексного режима

В ходе настройки скорости и дуплексного режима интерфейса примите во внимание следующие инструкции.

- Если автосогласование поддерживается на обоих концах линии, компания Cisco рекомендует установить для параметров автосогласования значения по умолчанию.
- Если автосогласование поддерживается на одном конце линии, а на другом не поддерживается, настройте скорость и дуплексный режим на обоих интерфейсах; не используйте на стороне, поддерживающей автосогласование, параметр **auto**.
- Значения параметров на обоих концах линии должны быть одинаковыми. Например, на обоих концах может быть установлено значение «hard-set» «auto-negotiate». Разные значения не поддерживаются.

⚠

Внимание Изменение скорости и дуплексного режима интерфейса может привести к отключению и повторному включению интерфейса в ходе повторной настройки.

Настройка скорости интерфейса

Войдите в режим глобальной конфигурации и выполните следующие действия для настройки скорости интерфейса.

СВОДКА ШАГОВ

1. **interface fastethernet** *interface-id*
2. speed [10 | 100 | auto]

ПОДРОБНОЕ ОПИСАНИЕ ШАГОВ

	Команда	Назначение
Шаг 1	`Router(config)#interface fastethernet interface-id`	Выбор интерфейса, который необходимо настроить.

Шаг 2	`Router(config-if)#speed [10 | 100 | auto]`	Установка скорости интерфейса на интерфейсе.

Примечание. Если на интерфейсе Ethernet, поддерживающем скорость передачи 10/100 Мбит/с, а для скорости установлено значение «auto», автоматическое согласование будет осуществляться для скорости и дуплексного режима.

Настройка дуплексного режима интерфейса

Войдите в режим глобальной конфигурации и выполните следующие действия для настройки дуплексного режима интерфейса Fast Ethernet.

СВОДКА ШАГОВ

1. **interface fastethernet** *interface-id*
2. **duplex [auto | full | half]**

ПОДРОБНОЕ ОПИСАНИЕ ШАГОВ

	Команда	Назначение
Шаг 1	`Router(config)#`**`interface fastethernet`** *`interface-id`*	Выбор интерфейса, который необходимо настроить.
Шаг 2	`Router(config-if)#`**`duplex [auto | full | half]`**	Задание дуплексного режима интерфейса.

Примечание. Если на интерфейсе Ethernet, поддерживающем скорость передачи 10/100 Мбит/с, для скорости порта установлено значение «auto», автоматическое согласование будет осуществляться для скорости и дуплексного режима. Дуплексный режим интерфейсов с автосогласованием изменить невозможно.

В следующем примере показан интерфейс Fast Ethernet interface 3, на котором для дуплексного режима установлено значение «auto».

```
Router(config)#interface fastethernet 0/1/0

router(config-if)#speed 100

Router(config-if)#duplex auto

Router(config-if)#end
```

Проверка настройки скорости интерфейса и дуплексного режима

Для проверки настройки скорости интерфейса и дуплексного режима используется команда **show interfaces**, как показано в следующем примере.

```
Router#show interfaces fastethernet 0/1/0



FastEthernet0/1/0 is up, line protocol is up

 Hardware is Fast Ethernet, address is 000f.f70a.f272 (bia 000f.f70a.f272)

 MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,

   reliability 255/255, txload 1/255, rxload 1/255

 Encapsulation ARPA, loopback not set

 Keepalive set (10 sec)

 Auto-duplex, Auto-speed

 ARP type: ARPA, ARP Timeout 04:00:00

 Last input 00:00:11, output never, output hang never

 Last clearing of "show interface" counters never

 Queueing strategy: fifo

 Output queue 0/40, (size/max)

 5 minute input rate 0 bits/sec, 0 packets/sec

 5 minute output rate 0 bits/sec, 0 packets/sec

   4 packets input, 1073 bytes, 0 no buffer

   Received 0 broadcasts, 0 runts, 0 giants, 0 throttles

   0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored

   0 input packets with dribble condition detected

   6 packets output, 664 bytes, 0 underruns(0/0/0)

   0 output errors, 0 collisions, 3 interface resets

   0 babbles, 0 late collision, 0 deferred

   0 lost carrier, 0 no carrier

   0 output buffer failures, 0 output buffers swapped out

Router#
```

Настройка описания интерфейса

Для интерфейса можно создать описание, которое поможет запомнить его функцию. Описание отображается в выходных данных следующих команд: **show configuration**, **show running-config** и **show interfaces**.

Для добавления описания интерфейса в режиме настройки интерфейса введите команду **description**.

Команда	Назначение
`Router(config-if)#`**`description`** `string`	Добавление описания для интерфейса.

Настройка интерфейса Fast Ethernet в качестве магистрального канала уровня 2

Войдите в режим глобальной конфигурации и выполните следующие действия для настройки интерфейса Fast Ethernet в качестве магистрального канала уровня 2.

СВОДКА ШАГОВ

1. interface fastethernet *interface-id*
2. shutdown
3. **switchport** mode trunk
4. **switchport** trunk native vlan *vlan-num*
5. **switchport** trunk allowed vlan {add | except | none | remove} *vlan1*[**,**vlan[**,**vlan[**,**...]]
6. no shutdown
7. end

ПОДРОБНОЕ ОПИСАНИЕ ШАГОВ

	Команда	Назначение
Шаг 1	`Router(config)# interface fastethernet` *`interface-id`*	Выбор интерфейса, который необходимо настроить.
Шаг 2	`Router(config-if)# shutdown`	Отключение интерфейса для остановки трафика до момента завершения настройки (необязательно).
Шаг 3	`Router(config-if)#` **`switchport`** `mode trunk`	Настройка интерфейса в качестве магистрального канала уровня 2. **Примечание.** Параметр инкапсуляции всегда принимает

		значение dot1q.
Шаг 4	`Router(config-if)# switchport trunk native vlan vlan-num`	Для магистральных каналов 802.1Q — задание стандартной сети VLAN (необязательно).
Шаг 5	`Router(config-if)# switchport trunk allowed vlan {add | except | none | remove} vlan1[,vlan[,vlan[,...]]]`	Настройка списка сетей VLAN, допустимых к использованию на магистральном канале (необязательно). По умолчанию разрешено использование всех сетей VLAN. Удаление из магистрального канала сетей VLAN, заданных по умолчанию, невозможно.
Шаг 6	`Router(config-if)# no shutdown`	Активация интерфейса. Используется только в том случае, если интерфейс был отключен.
Шаг 7	`Router(config-if)# end`	Выход из режима настройки.

Примечание. Порты не поддерживают протокол DTP. Убедитесь, что для соседнего коммутатора включен режим, в котором не отправляются данные DTP.

Проверка настройки интерфейса Fast Ethernet в качестве магистрального канала уровня 2

Для проверки настройки интерфейса Fast Ethernet в качестве магистрального канала уровня 2 используйте следующие команды **show**.

```
router#show running-config interfaces fastEthernet 0/3/1

Building configuration...

Current configuration: 71 bytes

!

interface FastEthernet0/3/1

 switchport mode trunk

 no ip address

end

router#
```

```
router#show interfaces trunk
```

```
Port  Mode  Encapsulation  Status  Native vlan

Fa0/3/1  on     802.1q      trunking     1


Port  Vlans allowed on trunk

Fa0/3/1    1-1005


Port  Vlans allowed and active in management domain

Fa0/3/1    1


Port  Vlans in spanning tree forwarding state and not pruned

Fa0/3/1    1


router#
```

Настройка интерфейса Fast Ethernet с доступом уровня 2

Войдите в режим глобальной конфигурации и выполните следующие действия для настройки интерфейса Fast Ethernet с доступом уровня 2.

СВОДКА ШАГОВ

1. interface fastethernet *interface-id*

2. shutdown

3. switchport mode access

4. switchport access vlan *vlan_num*

5. no shutdown

6. end

ПОДРОБНОЕ ОПИСАНИЕ ШАГОВ

	Команда	Назначение
Шаг 1	`Router(config)#interface fastethernet` *`interface-id`*	Выбор интерфейса, который необходимо настроить.
Шаг 2	`Router(config-if)#shutdown`	Отключение интерфейса для остановки

		трафика до момента завершения настройки (необязательно).
Шаг 3	`Router(config-if)#switchport mode access`	Настройка интерфейса для доступа уровня 2.
Шаг 4	`Router(config-if)#switchport access vlan` *`vlan_num`*	Указание сети Vlan для портов доступа.
Шаг 5	`Router(config-if)#no shutdown`	Активация интерфейса. Используется только в том случае, если интерфейс был отключен.
Шаг 6	`Router(config-if)#end`	Выход из режима настройки.

Проверка настройки интерфейса Fast Ethernet с доступом уровня 2

Для проверки настройки интерфейса используйте команду **show running-config interface**, как показано ниже:

```
Router#show running-config interface fastethernet 0/1/2

Building configuration...

Current configuration: 76 bytes

!

interface FastEthernet0/1/2

 switchport access vlan 3

 no ip address

end
```

Для проверки конфигурации коммутируемого порта интерфейса используйте команду **show interfaces**, как показано ниже.

```
Router#show interfaces f0/1/0 switchport

Name: Fa0/1/0

Switchport: Enabled

Administrative Mode: static access

Operational Mode: static access

Administrative Trunking Encapsulation: dot1q

Operational Trunking Encapsulation: native

Negotiation of Trunking: Disabled
```

```
Access Mode VLAN: 1 (default)

Trunking Native Mode VLAN: 1 (default)

Trunking VLANs Enabled: ALL

Trunking VLANs Active: 1

Priority for untagged frames: 0

Override vlan tag priority: FALSE

Voice VLAN: none

Appliance trust: none

router#
```

Настройка параметров аутентификации 802.1x

В данном разделе приведено описание настройки аутентификации 802.1x на основе портов на интерфейсной плате EtherSwitch HWIC.

- Настройки параметров аутентификации 802.1x по умолчанию
- Включение аутентификации 802.1x
- Настройка соединения коммутатора с сервером RADIUS
- Включение периодической повторной аутентификации
- Изменение тихого периода
- Изменение времени повторной передачи данных от коммутатора клиенту
- Задание числа повторных передач кадров от коммутатора к клиенту
- Включение поддержки нескольких узлов сети
- Сброс значений параметров аутентификации 802.1x на значения по умолчанию
- Отображение статистики и состояния аутентификации 802.1x

Настройки параметров аутентификации 802.1x по умолчанию

В таблице 1 показана конфигурация 802.1x по умолчанию.

Функция	Значение по умолчанию
Authentication, authorization, and accounting	Отключено.

(AAA) (Аутентификация, авторизация и учет (AAA))	
RADIUS server (Сервер RADIUS) • IP address (IP-адрес) • UDP authentication port (Порт аутентификации UDP) • Key (Ключ)	• Не задано. • 1645. • Не задано.
Per-interface 802.1x enable state (Включение аутентификации 802.1x для каждого интерфейса)	Отключено (включается принудительно). Порт используется для отправки и получения трафика без необходимости прохождения аутентификации 802.1x клиентом.
Periodic reauthentication (Периодическая повторная аутентификация)	Отключено.
Number of seconds between reauthentication attempts (Время в секундах между попытками повторной аутентификации)	3600 секунд.
Quiet period (Тихий период)	60 секунд (время в секундах, в течение которого коммутатор остается в неактивном состоянии после сбоя во время аутентификации клиента).
Retransmission time (Время повторной передачи)	30 секунд (время в секундах, в течение которого коммутатор ожидает ответа на запрос EAP/кадра идентификации от клиента перед повторной передачей запроса).
Maximum retransmission number (Максимальное количество повторных передач)	2 раза (количество отправок коммутатором запросов EAP/кадров идентификации перед повторным началом процесса аутентификации).
Multiple host support (Поддержка нескольких сетевых узлов)	Отключено.
Client timeout period (Период ожидания клиента)	30 секунд (время ожидания коммутатором ответа на запрос, отправленный сервером аутентификации, до повторной отправки этого запроса клиенту). Настройка данного значения невозможна.
Authentication server timeout period (Период ожидания сервера аутентификации)	30 секунд (время ожидания коммутатором ответа на запрос, который должен быть передан серверу аутентификации, до повторной отправки ответа на запрос серверу). Настройка данного значения невозможна.

Ниже приведены инструкции по настройке параметров аутентификации 802.1x.

• Если протокол 802.1x включен, перед включением любой другой функции уровня 2 осуществляется аутентификация портов.

• Протокол 802.1x поддерживается портами статического доступа уровня 2 и не поддерживается портами следующих типов:

– Порт магистрального канала — при попытке включения протокола 802.1x для этого порта отображается сообщение об ошибке, а протокол 802.1x не включается. При попытке изменения на магистральный режима порта, поддерживающего протокол 802.1x, режим не изменяется.

– Порт назначения анализатора коммутируемого порта (SPAN) — протокол 802.1x можно включить для порта, являющегося портом назначения SPAN. Однако при удалении атрибута порта назначения SPAN протокол 802.1x выключается. Протокол 802.1x можно включить на порте источника SPAN.

Включение аутентификации 802.1x

Для включения аутентификации на базе порта протокола 802.1x необходимо включить функцию AAA и настроить список способов аутентификации. В списке способов указываются способы аутентификации пользователей и последовательность их применения.

Для аутентификации пользователей программное обеспечение сначала использует первый способ аутентификации; если этот способ не срабатывает, программа переходит к следующему способу в списке. Этот процесс продолжается до тех пор, пока посредством указанного в списке способа не будет установлено соединение или пока не будет осуществлена попытка подключения всеми указанными способами. Если в любой момент времени в ходе цикла аутентификации происходит сбой, процесс аутентификации останавливается, а другие способы аутентификации не используются.

Войдите в привилегированный режим EXEC и выполните следующие действия для настройки аутентификации на базе порта протокола 802.1x. Эта процедура является обязательной.

СВОДКА ШАГОВ

1. **configure terminal**
2. **configure terminal**
3. **aaa authentication** dot1x {default | *listname*} *method1* [*method2*...]
4. **interface** *interface-id*
5. **dot1x port-control auto**
6. **end**
7. **show dot1x**
8. **copy running-config startup-config**

ПОДРОБНОЕ ОПИСАНИЕ ШАГОВ

	Команда	Назначение
Шаг 1	**configure terminal**	Вход в режим глобальной конфигурации.
Шаг 2	**aaa new-model**	Включение AAA.
Шаг 3	**aaa authentication** dot1x {default | *listname*} *method1* [*method2*...]	Создание списка способов аутентификации 802.1x. Если список с именем *не указан* в команде **authentication**, для создания списка по умолчанию следует использовать ключевое слово **default**, после которого указываются способы, используемые в указанных ситуациях по умолчанию. Список методов, используемых по умолчанию, автоматически применяется ко всем интерфейсам. Необходимо ввести хотя бы одно из следующих ключевых слов: • **group radius** — использование для аутентификации списка всех серверов RADIUS. • **none** — аутентификация не выполняется. Аутентификация клиента осуществляется автоматически с использованием информации, предоставляемой клиентом, минуя коммутатор.
Шаг 4	**interface** *interface-id*	Вход в режим настройки интерфейса и выбор интерфейса, для которого необходимо включить аутентификацию 802.1x.
Шаг 5	**dot1x port-control auto**	Включение аутентификации 802.1x на интерфейсе. Информацию по взаимодействию функции с портами магистральных каналов, динамическими портами, портами динамического доступа, портами EtherChannel, безопасными портами и портами SPAN см. в разделе «Инструкции по настройке параметров аутентификации 802.1x».
Шаг 6	**end**	Возврат к привилегированному режиму EXEC.
Шаг 7	**show dot1x**	Проверка введенных пользователем данных. См. столбец Status (Состояние) области 802.1x Port Summary (Краткие сведения о портах 802.1x) дисплея. Состояние *enabled* (включено) означает, что для параметра контроля порта установлено значение **auto (авто)** или **force-unauthorized (принудительное отключение авторизации)**.
Шаг 8	**copy running-config startup-config**	Сохранение записей в файл конфигурации (необязательно).

Для отключения функции AAA используйте команду **no aaa new-model** в режиме глобальной конфигурации. Для отключения аутентификации 802.1x AAA используйте команду **no aaa authentication dot1x** {**default** | *list-name*} *method1* [*method2...*]. Для отключения протокола 802.1x используйте команду **dot1x port-control force-authorized** или **no dot1x port-control** в режиме настройки интерфейса.

Настройка соединения коммутатора с сервером RADIUS

Идентификация серверов безопасности RADIUS осуществляется посредством имени узла сети или IP-адресу, имени узла сети и указанных номеров портов UDP или IP-адреса и указанных номеров портов UDP. Сочетание IP-адреса номера порта UDP представляет собой уникальный идентификатор, который позволяет осуществлять отправку запросов RADIUS на несколько портов UDP на сервере с одним IP-адресом. Если на одном сервере RADIUS для одной службы (например, аутентификация) настроены записи двух различных узлов сети, запись второго узла выступает в качестве резервной на случай переключения в результате сбоя. Обращение к записям сетевых узлов RADIUS осуществляется в той же последовательности, что и их настройка.

Войдите в привилегированный режим EXEC и выполните следующие действия для настройки параметров сервера RADIUS на коммутаторе. Эта процедура является обязательной.

СВОДКА ШАГОВ

1. **configure terminal**
2. **radius-server host** {*hostname* | *ip-address*} **auth-port** *port-number* **key** *string*
3. **end**
4. **show running-config**
5. **copy running-config startup-config**

ПОДРОБНОЕ ОПИСАНИЕ ШАГОВ

	Команда	Назначение
Шаг 1	**configure terminal**	Вход в режим глобальной конфигурации.
Шаг 2	**radius-server host** {*hostname* | *ip-address*} **auth-port** *port-number* **key** *string*	Настройка параметров сервера RADIUS на коммутаторе. Для параметров *hostname* | *ip-address* , укажите имя узла сети IP-адрес удаленного сервера RADIUS. Для параметров **auth-port** *port-number* укажите порт назначения UDP для запросов на аутентификацию. Значение по умолчанию — 1645. Для параметров **key** *string* укажите ключи аутентификации и шифрования, используемые между коммутатором и демоном RADIUS, запущенным на удаленном сервере RADIUS. Ключ - текстовая строка, соответствующая ключу шифрования, используемому на сервере RADIUS.

		Примечание. Ключ следует конфигурировать в качестве последнего параметра при использовании в команде **radius-server host**, так как пробелы непосредственно перед ключом не учитываются (пробелы внутри строки ключа и пробелы после строки ключа учитываются). Если пробел используется непосредственно в ключе, не следует заключать его в кавычки, если кавычки не являются частью строки ключа. Данный ключ должен соответствовать шифрованию на демоне RADIUS. При использовании нескольких серверов RADIUS данную команду следует ввести повторно.
Шаг 3	**end**	Возврат к привилегированному режиму EXEC.
Шаг 4	**show running-config**	Проверка введенных пользователем данных.
Шаг 5	**copy running-config startup-config**	Сохранение записей в файл конфигурации (необязательно).

Для удаления указанного сервера RADIUS используйте команду **no radius-server host** {*hostname* | *ip-address*} в режиме глобальной конфигурации.

В режиме глобальной конфигурации можно изменить значения времени ожидания, повторной передачи и ключа шифрования для всех серверов RADIUS посредством использования команды **radius-server host**. Для настройки этих параметров на каждом сервере по отдельности используйте команды **radius-server timeout**, **radius-server retransmit** и **radius-server key** в режиме глобальной конфигурации.

Необходимо также настроить несколько параметров на сервере RADIUS. Эти параметры включают в себя IP-адрес коммутатора и строку ключа, которая используется как на сервере, так и на коммутаторе. Дополнительную информацию см. в документации к серверу RADIUS.

Включение периодической повторной аутентификации

Можно включить периодическую повторную аутентификацию 802.1x для клиента и указать периодичность отправки запросов на ввод данных аутентификации. Если перед включением повторной аутентификации не указан временной интервал, время между попытками повторной аутентификации будет составлять 3600 секунд.

Автоматическая повторная аутентификация клиента по протоколу 802.1x является глобальным параметром и не может быть изменена для клиентов, подключенных к отдельным портам.

Войдите в привилегированный режим EXEC и выполните следующие действия для включения периодической повторной аутентификации и установки времени ожидания (в секундах) между попытками повторной аутентификации.

СВОДКА ШАГОВ

1. **configure terminal**

2. **dot1x re-authentication**

3. **dot1x timeout re-authperiod** *seconds*

4. **end**

5. **show dot1x**

6. **copy running-config startup-config**

ПОДРОБНОЕ ОПИСАНИЕ ШАГОВ

	Команда	Назначение
Шаг 1	**configure terminal**	Вход в режим глобальной конфигурации.
Шаг 2	**dot1x re-authentication**	Включение периодической повторной аутентификации клиента, которая по умолчанию отключена.
Шаг 3	**dot1x timeout re-authperiod** *seconds*	Задание времени ожидания (в секундах) между попытками повторной аутентификации. Допустимый диапазон составляет от 1 до 4294967295 секунд; значение по умолчанию — 3600 секунд. Данная команда влияет на работу коммутатора только в том случае, если повторная аутентификация включена.
Шаг 4	**end**	Возврат к привилегированному режиму EXEC.
Шаг 5	**show dot1x**	Проверка введенных пользователем данных.
Шаг 6	**copy running-config startup-config**	Сохранение записей в файл конфигурации (необязательно).

Для отключения периодической аутентификации используйте команду **no dot1x re-authentication** в режиме глобальной конфигурации. Для восстановления времени ожидания между попытками повторной аутентификации по умолчанию используйте команду **no dot1x timeout re-authperiod** в режиме глобальной конфигурации.

Изменение тихого периода

Если коммутатору не удается выполнить аутентификацию пользователя, он осуществляет следующую попытку через определенный интервал. Этот интервал определяется значением параметра quiet-period (тихий период). Причиной сбоя аутентификации клиента может быть ввод клиентом неверного пароля. Пользователю можно предоставить возможность вводить данные повторно через меньший временной интервал. Для этого нужно указать время ожидания, которое меньше значения по умолчанию.

Войдите в привилегированный режим EXEC и выполните следующие действия для изменения значения тихого периода.

СВОДКА ШАГОВ

1. **configure terminal**
2. **dot1x timeout quiet-period** *seconds*
3. **end**
4. **show dot1x**
5. **copy running-config startup-config**

ПОДРОБНОЕ ОПИСАНИЕ ШАГОВ

	Команда	Назначение
Шаг 1	**configure terminal**	Вход в режим глобальной конфигурации.
Шаг 2	**dot1x timeout quiet-period** *seconds*	Задание времени в секундах, в течение которого коммутатор остается в неактивном состоянии после неудавшейся аутентификации клиента. Диапазон составляет от 0 до 65535 секунд; значение по умолчанию — 60 секунд.
Шаг 3	**end**	Возврат к привилегированному режиму EXEC.
Шаг 4	**show dot1x**	Проверка введенных пользователем данных.
Шаг 5	**copy running-config startup-config**	Сохранение записей в файл конфигурации (необязательно).

Для возврата к значению тихого периода по умолчанию используйте команду **no dot1x timeout quiet-period** в режиме глобальной конфигурации.

Изменение времени повторной передачи данных от коммутатора к клиенту

После получения запроса EAP/кадра идентификации от коммутатора клиент отправляет ответ EAP/кадр идентификации. Если коммутатор не получает ответа, он осуществляет следующую попытку через определенный интервал (время повторной передачи).

Примечание. Значение данной команды по умолчанию следует изменять только в крайних случаях, например при ненадежных каналах связи или других проблемах при взаимодействии с определенными клиентами и серверами аутентификации.

Войдите в привилегированный режим EXEC и выполните следующие действия для изменения временного интервала

ожидания коммутатором повторного уведомления клиента.

СВОДКА ШАГОВ

1. **configure terminal**
2. **dot1x timeout tx-period** *seconds*
3. **end**
4. **show dot1x**
5. **copy running-config startup-config**

ПОДРОБНОЕ ОПИСАНИЕ ШАГОВ

	Команда	Назначение
Шаг 1	**configure terminal**	Вход в режим глобальной конфигурации.
Шаг 2	**dot1x timeout tx-period** *seconds*	Задание времени в секундах, в течение которого коммутатор ожидает ответа на запрос EAP/кадра идентификации от клиента перед повторной передачей запроса. Диапазон составляет от 1 до 65535 секунд; значение по умолчанию — 30 секунд.
Шаг 3	**end**	Возврат к привилегированному режиму EXEC.
Шаг 4	**show dot1x**	Проверка введенных пользователем данных.
Шаг 5	**copy running-config startup-config**	Сохранение записей в файл конфигурации (необязательно).

Для возврата к значению времени повторной отправки по умолчанию используйте команду **no dot1x timeout tx-period** в режиме глобальной конфигурации.

Задание числа повторных передач кадров от коммутатора к клиенту

Помимо изменения временного интервала между повторными передачами кадров от коммутатора клиенту, можно также изменять количество попыток отправки коммутатором запросов EAP/кадров идентификации (при условии отсутствия ответа) клиенту перед началом процесса аутентификации заново.

Примечание. Значение данной команды по умолчанию следует изменять только в крайних случаях, например при ненадежных каналах связи или других проблемах при взаимодействии с определенными клиентами и серверами аутентификации.

Войдите в привилегированный режим EXEC и выполните следующие действия для задания количества попыток отправки коммутатором кадров идентификации клиенту.

СВОДКА ШАГОВ

1. **configure terminal**
2. **dot1x max-req** *count*
3. **end**
4. **show dot1x**
5. **copy running-config startup-config**

ПОДРОБНОЕ ОПИСАНИЕ ШАГОВ

	Команда	Назначение
Шаг 1	**configure terminal**	Вход в режим глобальной конфигурации.
Шаг 2	**dot1x max-req** *count*	Задание количества отправок коммутатором запросов EAP/кадров идентификации клиенту перед повторным началом процесса аутентификации. Диапазон составляет от 1 до 10; значение по умолчанию — 2.
Шаг 3	**end**	Возврат к привилегированному режиму EXEC.
Шаг 4	**show dot1x**	Проверка введенных пользователем данных.
Шаг 5	**copy running-config startup-config**	Сохранение записей в файл конфигурации (необязательно).

Для возврата к значению количества попыток повторной отправки по умолчанию используйте команду **no dot1x max-req** в режиме глобальной конфигурации.

Включение поддержки нескольких узлов сети

Одному порту, поддерживающему 802.1x, можно назначить несколько сетевых узлов. В этом режиме для получения доступа к сети всеми сетевыми узлами достаточно получения доступа одним из назначенных сетевых узлов. Если порт становится неавторизованным (сбой во время повторной аутентификации и получение сообщения EAPOL о выходе из системы), доступ к сети закрывается для всех назначенных клиентов.

Войдите в привилегированный режим EXEC и выполните следующие действия для доступа нескольких сетевых узлов (клиентов) к порту с поддержкой 802.1x, для которого команда **dot1x port-control** режима настройки интерфейса имеет значение **auto**.

СВОДКА ШАГОВ

1. **configure terminal**
2. **interface** interface-id
3. **dot1x multiple-hosts**
4. **end**
5. **show dot1x interface** *interface-id*
6. **copy running-config startup-config**

ПОДРОБНОЕ ОПИСАНИЕ ШАГОВ

	Команда	Назначение
Шаг 1	**configure terminal**	Вход в режим глобальной конфигурации.
Шаг 2	**interface** *interface-id*	Вход в режим настройки интерфейса и выбор интерфейса, которому будут косвенно назначаться узлы сети.
Шаг 3	**dot1x multiple-hosts**	Позволяет подключить несколько узлов сети (клиентов) к порту с поддержкой 802.1x. Убедитесь, что для команды **dot1x port-control** режима настройки интерфейса установлено значение **auto** для указанного интерфейса.
Шаг 4	**end**	Возврат к привилегированному режиму EXEC.
Шаг 5	**show dot1x interface** *interface-id*	Проверка введенных пользователем данных.
Шаг 6	**copy running-config startup-config**	Сохранение записей в файл конфигурации (необязательно).

Для отключения поддержки нескольких сетевых узлов на одном порте используйте команду **no dot1x multiple-hosts** в режиме настройки интерфейса.

Сброс значений параметров аутентификации 802.1x на значения по умолчанию

Для параметров аутентификации 802.1x установите значения по умолчанию с помощью одной команды.

Войдите в привилегированный режим EXEC и выполните следующие действия для установки параметров аутентификации 802.1x на значения по умолчанию.

СВОДКА ШАГОВ

1. **configure terminal**
2. **dot1x default**
3. **end**
4. **show dot1x**
5. **copy running-config startup-config**

ПОДРОБНОЕ ОПИСАНИЕ ШАГОВ

	Команда	Назначение
Шаг 1	`configure terminal`	Вход в режим глобальной конфигурации.
Шаг 2	`dot1x default`	Возврат параметров аутентификации 802.1x к значениям по умолчанию.
Шаг 3	`end`	Возврат к привилегированному режиму EXEC.
Шаг 4	`show dot1x`	Проверка введенных пользователем данных.
Шаг 5	`copy running-config startup-config`	Сохранение записей в файл конфигурации (необязательно).

Отображение статистики и состояния аутентификации 802.1x

Для отображения статистики аутентификации 802.1x для всех интерфейсов используйте команду **show dot1x statistics** в привилегированном режиме EXEC. Для отображения статистики аутентификации 802.1x для заданного интерфейса используйте команду **show dot1x statistics interface** *interface-id* в привилегированном режиме EXEC.

Для отображения административного и рабочего состояния аутентификации 802.1x коммутатора используйте команду **show dot1x** в привилегированном режиме EXEC. Для отображения административного и рабочего состояния аутентификации 802.1x для заданного интерфейса используйте команду **show dot1x interface** *interface-id* в привилегированном режиме EXEC.

Настройка протокола Spanning Tree

- Включение протокола Spanning Tree
- Настройка приоритета портов протокола Spanning Tree
- Настройка стоимости порта протокола Spanning Tree

- Настройка приоритета моста сети VLAN
- Настройка параметра Hello Time (времени приветствия)
- Настройка параметра Forward-Delay Time (времени задержки пересылки) для сети VLAN
- Настройка параметра Maximum Aging Time (максимального времени устаревания) для сети VLAN
- Отключение протокола Spanning Tree

Включение протокола Spanning Tree

Можно активировать протокол Spanning Tree для отдельных сетей VLAN. Коммутатор поддерживает отдельные экземпляры протокола Spanning Tree для каждой сети VLAN (за исключением сетей VLAN, в которых протокол Spanning Tree отключен).

Команда	Назначение
`Router(config)# spanning-tree vlan vlan_ID`	

Проверка настройки протокола Spanning Tree

Для проверки настройки протокола Spanning Tree используйте команду **show spanning-tree vlan**, как показано ниже.

```
Router# show spanning-tree vlan 200

VLAN200 is executing the ieee compatible Spanning Tree protocol

 Bridge Identifier has priority 32768, address 0050.3e8d.6401

 Configured hello time 2, max age 20, forward delay 15

 Current root has priority 16384, address 0060.704c.7000

 Root port is 264 (FastEthernet0/1/8), cost of root path is 38

 Topology change flag not set, detected flag not set

 Number of topology changes 0 last change occurred 01:53:48 ago

  Times:  hold 1, topology change 24, notification 2

          hello 2, max age 14, forward delay 10

 Timers: hello 0, topology change 0, notification 0

Port 264 (FastEthernet0/1/8) of VLAN200 is forwarding

  Port path cost 19, Port priority 128, Port Identifier 129.9.

  Designated root has priority 16384, address 0060.704c.7000
```

```
  Designated bridge has priority 32768, address 00e0.4fac.b000

  Designated port id is 128.2, designated path cost 19

  Timers: message age 3, forward delay 0, hold 0

  Number of transitions to forwarding state: 1

  BPDU: sent 3, received 3417


Router#
```

Настройка приоритета портов протокола Spanning Tree

Войдите в режим глобальной конфигурации и выполните следующие действия для настройки приоритета портов протокола Spanning Tree.

СВОДКА ШАГОВ

1. interface {{ethernet | fastethernet} *interface-id*

2. [no] spanning-tree port-priority *port_priority*

3. [no] spanning-tree vlan *vlan_*ID **port-**priority *port_priority*

4. end

ПОДРОБНОЕ ОПИСАНИЕ ШАГОВ

	Команда	Назначение
Шаг 1	`Router(config)# interface {{ethernet | fastethernet} interface-id`	Выбор интерфейса, который необходимо настроить.
Шаг 2	`Router(config-if)# [no] spanning-tree port-priority port_priority`	Настройка приоритета портов для интерфейса. Значение параметра port_priority можно изменять в диапазоне от 4 до 252 с шагом в 4. Для установки значений по умолчанию используйте эту команду с ключом **no**.
Шаг 3	`Router(config-if)# [no] spanning-tree vlan vlan_ID` **port**`-priority port_priority`	Настройка приоритета портов VLAN для интерфейса. Значение параметра port_priority можно изменять в диапазоне от 4 до 252 с шагом в 4. Для установки значений по умолчанию используйте эту команду с ключом **no**.

Шаг 4	`Router(config-if)# end`	Выход из режима настройки.

Проверка приоритета портов протокола Spanning Tree

Для отображения параметров протокола Spanning Tree и приоритета портов этого протокола используйте команду **show spanning-tree interface**, как показано ниже.

```
Router# show spanning-tree interface fastethernet 0/1/6



Port 264 (FastEthernet0/1/6) of VLAN200 is forwarding

  Port path cost 19, Port priority 100, Port Identifier 129.8.

  Designated root has priority 32768, address 0010.0d40.34c7

  Designated bridge has priority 32768, address 0010.0d40.34c7

  Designated port id is 128.1, designated path cost 0

  Timers: message age 2, forward delay 0, hold 0

  Number of transitions to forwarding state: 1

  BPDU: sent 0, received 13513

Router#
```

Настройка стоимости порта протокола Spanning Tree

Войдите в режим глобальной конфигурации и выполните следующие действия для настройки стоимости портов протокола Spanning Tree для интерфейса.

СВОДКА ШАГОВ

1. interface {{ethernet | fastethernet} *interface-id*
2. [no] spanning-tree cost *port_cost*
3. [no] spanning-tree vlan *vlan_ID* cost *port_cost*
4. end

ПОДРОБНОЕ ОПИСАНИЕ ШАГОВ

	Команда	Назначение
Шаг 1	`Router(config)# interface {{ethernet	fastethernet} interface-id`	Выбор интерфейса, который необходимо настроить.

Шаг 2	`Router(config-if)# [no] spanning-tree cost` *`port_cost`*	Настройка стоимости портов для интерфейса. Значение параметра port_cost можно изменять в диапазоне от 1 до 200 000 000 (от 1 до 65 535 в ПО Cisco IOS, версии 12.1(2)E и ниже). Для установки значений по умолчанию используйте эту команду с ключом **no**.
Шаг 3	`Router(config-if)# [no] spanning-tree vlan` *`vlan_ID`* `cost` *`port_cost`*	Настройка стоимости портов VLAN для интерфейса. Значение параметра port_cost можно изменять в диапазоне от 1 до 65 535. Для установки значений по умолчанию используйте эту команду с ключом **no**.
Шаг 4	`Router(config-if)# end`	Выход из режима настройки.

Расчет стоимости портов

Для расчета стоимости порта учитывается полоса пропускания порта. Существует два класса значений. Короткие (16-битные) значения описаны в спецификации IEEE 802.1D и находятся в диапазоне от 1 до 65 535. Длинные (32-битные) значения описаны в спецификации IEEE 802.1t и находятся в диапазоне от 1 до 200 000 000.

Назначение коротких значений стоимости портов

Значения стоимости портов в диапазоне от 1 до 65 535 можно назначать вручную. По умолчанию значения стоимости следующие.

Скорость порта	Значение стоимости по умолчанию
10 Мбит/с	100
100 Мбит/с	19

Назначение длинных значений стоимости портов

Значения стоимости портов в диапазоне от 1 до 200 000 000 можно назначать вручную. Рекомендуется использовать следующие значения стоимости портов.

Скорость порта	Рекомендуемое значение	Рекомендуемый диапазон
10 Мбит/с	2 000 000	От 200 000 до 20 000 000
100 Мбит/с	200 000	От 20 000 до 2 000 000

Проверка стоимости порта протокола Spanning Tree

Для проверки настройки стоимости портов протокола Spanning Tree используйте команду **show spanning-tree vlan**.

```
Router# show spanning-tree vlan 200



Port 264 (FastEthernet0/1/8) of VLAN200 is forwarding

Port path cost 17, Port priority 64, Port Identifier 129.8.

  Designated root has priority 32768, address 0010.0d40.34c7

  Designated bridge has priority 32768, address 0010.0d40.34c7

  Designated port id is 128.1, designated path cost 0

  Timers: message age 2, forward delay 0, hold 0

  Number of transitions to forwarding state: 1

  BPDU: sent 0, received 13513

Router#
```

Настройка приоритета моста сети VLAN

Для настройки приоритета моста сети VLAN для протокола Spanning Tree используйте в режиме глобальной конфигурации следующую команду.

Команда	Назначение
`Router(config)# [no] spanning-tree vlan` *`vlan_ID`* `priority` *`bridge_priority`*	Настройка приоритета моста сети VLAN. Значение параметра bridge_priority можно изменять в диапазоне от 1 до 65 535. Для установки значений по умолчанию используйте эту команду с ключом **no**.

Внимание Соблюдайте осторожность при использовании данной команды. В большинстве случаев для изменения приоритета моста рекомендуется использовать команды **spanning-tree vlan vlan_ID root primary** и **spanning-tree vlan vlan_ID root secondary**.

Проверка приоритета моста сети VLAN

Для проверки приоритета моста используйте команду **show spanning-tree vlan bridge**, как показано ниже.

```
Router# show spanning-tree vlan 200 bridge brief

                                     Hello Max Fwd

Vlan                   Bridge ID      Time  Age Delay  Protocol

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

VLAN200          33792 0050.3e8d.64c8    2   20    15  ieee

Router#
```

Настройка параметра Hello Time

Для настройки интервала параметра Hello Time (времени приветствия) протокола Spanning Tree используйте следующую команду в режиме глобальной конфигурации.

Команда	Назначение
`Router(config)# [no] spanning-tree` **`vlan`** `vlan_ID` **`hello`**`-time` *`hello_time`*	Настройка времени приветствия для сети VLAN. Значение параметра **hello_time** можно изменять в диапазоне от 1 до 10 секунд. Для установки значений по умолчанию используйте эту команду с ключом **no**.

Настройка параметра Forward-Delay Time (времени задержки пересылки) для сети VLAN

Команда	Назначение
`Router(config)# [no] spanning-tree vlan` *`vlan_ID`* `forward-time` *`forward_time`*	

Настройка параметра Maximum Aging Time (максимального времени устаревания) для сети VLAN

Для настройки интервала времени устаревания протокола Spanning Tree используйте следующую команду в режиме глобальной конфигурации.

Команда	Назначение
`Router(config)# [no] spanning-tree vlan` *`vlan_ID`* `max-age` *`max_age`*	Настройка максимального времени устаревания для сети VLAN. Значение параметра **max_age** можно изменять в диапазоне от 6 до 40 секунд. Для установки значений по умолчанию

	используйте эту команду с ключом **no**.

Настройка корневого моста

Интерфейсная плата EtherSwitch HWIC поддерживает отдельный экземпляр протокола Spanning Tree для каждой сети VLAN, настроенной на коммутаторе. Идентификатор моста, состоящий из приоритета и MAC-адреса моста, связан с каждым экземпляром. В каждой сети VLAN корневым становится мост с наименьшим идентификатором моста.

Для настройки экземпляра сети VLAN в качестве корневого моста можно изменить приоритет моста со значения по умолчанию (32768) до гораздо более низкого значения, чтобы этот мост стал корневым для указанной сети VLAN. Для изменения приоритета моста используйте команду spanning-tree vlan vlan-ID root.

Коммутатор проверяет приоритет моста текущего корневого моста для каждой сети VLAN. Приоритет моста для некоторых сетей VLAN имеет значение 8192 на тот случай, если при этом значении коммутатор станет корневым мостом для указанных сетей VLAN.

Если корневой коммутатор для указанных сетей VLAN имеет приоритет моста ниже 8192, коммутатор устанавливает приоритет моста для указанных сетей VLAN на 1 меньше наименьшего значения приоритета моста.

Например, если на всех коммутаторах в сети значение приоритета моста сети VLAN 100 составляет 32768, после ввода на коммутаторе команды «spanning-tree vlan 100 root primary» для сети VLAN 100 значение приоритета моста будет изменено на 8192, а коммутатор станет корневым мостом для сети VLAN 100.

Примечание. Корневой коммутатор для каждого экземпляра протокола Spanning Tree должен представлять собой опорный или распределительный коммутатор. Запрещается настраивать в качестве корневого коммутатора протокола Spanning Tree коммутатор доступа.

Для задания диаметра сети (т.е. максимального количества мостовых переходов между любыми двумя конечными станциями сети) уровня 2 используйте ключевое слово «diameter». При задании диаметра сети коммутатор автоматически устанавливает оптимальное время приветствия, время задержки пересылки и максимальное время устаревания для сети указанного диаметра, что в значительной степени помогает снизить время конвергенции сети. Для изменения автоматически рассчитываемого времени приветствия можно использовать ключевое слово «hello».

Примечание. После настройки коммутатора в качестве корневого моста не рекомендуется изменять время приветствия, время задержки пересылки и максимальное время устаревания вручную.

Для настройки коммутатора в качестве корневого моста используйте следующую команду в режиме глобальной конфигурации.

Команда	Назначение
`Router(config)# [no] spanning-tree vlan vlan_ID root primary [diameter hops [hello-time seconds]]`	Настройка коммутатора в качестве корневого моста. Для установки значений по умолчанию используйте эту команду с ключом **no**.

Отключение протокола Spanning Tree

Команда	Назначение
`Router(config)# no spanning-tree vlan vlan_ID`	Отключение протокола Spanning Tree для отдельных сетей VLAN.

Проверка отключения протокола Spanning Tree.

Для проверки отключения протокола Spanning Tree используйте команду **show spanning-tree vlan**, как показано ниже.

```
Router# show spanning-tree vlan 200

<output truncated>

Spanning tree instance for VLAN 200 does not exist.

Router#
```

Настройка обработки таблицы MAC-адресов

- Разрешение трафика от известных MAC-адресов
- Создание статической записи в таблице MAC-адресов
- Настройка таймера устаревания
- Проверка времени устаревания

Разрешение трафика от известных MAC-адресов

Войдите в привилегированный режим EXEC и выполните следующие действия для включения параметра безопасности MAC-адресов.

СВОДКА ШАГОВ

1. **configure terminal**
2. [no] mac-address-table secure <*mac-address*> fastethernet *interface-id* [vlan <*vlan id*>]
3. end

ПОДРОБНОЕ ОПИСАНИЕ ШАГОВ

	Команда	Назначение

Шаг 1	`Router# configure terminal`	
Шаг 2	`Router(config)# [no] mac-address-table secure <mac-address> fastethernet interface-id [vlan <vlan id>]`	Включение функции безопасного трафика для MAC-адресов порта.
Шаг 3	`Router(config)# end`	Выход из режима настройки.

Проверка параметра безопасности таблицы MAC-адресов

Для проверки настройки используйте команду **show mac-address-table secure**, как показано ниже.

```
Router# show mac-address-table secure


Secure Address Table:

Destination Address  Address Type  VLAN  Destination Port

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

0000.0002.0001          Secure        2     FastEthernet0/1/1
```

Создание статической записи в таблице MAC-адресов

Войдите в привилегированный режим EXEC и выполните следующие действия для создания статической записи в таблице MAC-адресов.

СВОДКА ШАГОВ

1. **configure terminal**
2. mac-address-table static *mac-address* fastethernet *interface-id* [vlan <*vlan id*>]
3. end

ПОДРОБНОЕ ОПИСАНИЕ ШАГОВ

	Команда	Назначение
Шаг 1	`Router# configure terminal`	
Шаг 2	`Router(config)# mac-address-table static mac-address fastethernet interface-id [vlan <vlan id>]`	Создание статической записи в таблице MAC-адресов. Если значение параметра vlan-id не

		задано, по умолчанию используется значение VLAN 1.
Шаг 3	`Router(config)# end`	Выход из режима настройки.

Проверка таблицы MAC-адресов.

Для проверки таблицы MAC-адресов используйте команду **show mac**, как показано ниже.

```
Router# show mac-address-table


Destination Address  Address Type  VLAN  Destination Port

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

00ff.ff0d.2dc0          Self         1     Vlan1

0007.ebc7.ff84          Static       1     FastEthernet0/3/5

0007.ebc8.018b          Static       1     FastEthernet0/3/6

000b.bf94.0006          Static       1     FastEthernet0/3/3

000b.bf94.0038          Static       1     FastEthernet0/3/0

000b.bf94.0039          Static       1     FastEthernet0/3/1

000b.bf94.0008          Static     314     FastEthernet0/3/2

000b.bf94.0038          Static     314     FastEthernet0/3/0

000b.bf94.0008          Static     331     FastEthernet0/3/2

000b.bf94.0038          Static     331     FastEthernet0/3/0

000b.bf94.0008          Static     348     FastEthernet0/3/2

000b.bf94.0038          Static     348     FastEthernet0/3/0
```

Настройка таймера устаревания

Для таймера устаревания можно установить значение в диапазоне от 16 до 4080 секунд с интервалом в 16 секунд.

Войдите в привилегированный режим EXEC и выполните следующие действия для настройки значения таймера устаревания.

СВОДКА ШАГОВ

1. **configure terminal**

2. mac-address-table aging-time <10-1000000>

3. end

ПОДРОБНОЕ ОПИСАНИЕ ШАГОВ

	Команда	Назначение
Шаг 1	`Router# configure terminal`	Вход в режим глобальной конфигурации.
Шаг 2	`Router(config)# mac-address-table aging-time <10-1000000>`	Настройка значения таймера устаревания MAC-адреса в секундах.
Шаг 3	`Router(config)# end`	Выход из режима настройки.

⚠

Внимание Компания Cisco не рекомендует изменять значение таймера устаревания, потому что это может привести к потере синхронизации интерфейсной платы EtherSwitch HWIC.

Проверка времени устаревания

Для проверки значения времени устаревания таблицы MAC-адресов используйте команду **show mac-address-table aging-time**, как показано ниже.

```
Router # show mac-address-table aging-time

Mac address aging time 320
```

Настройка протокола Cisco Discovery Protocol

- Включение протокола Cisco Discovery Protocol
- Включение протокола CDP на интерфейсе
- Мониторинг и поддержка протокола CDP

Включение протокола Cisco Discovery Protocol

Для включения протокола Cisco Discovery Protocol (CDP) используйте следующую команду в режиме глобальной конфигурации.

Команда	Назначение
`Router(config)# cdp run`	Глобальное включение протокола CDP.

Проверка глобальной настройки протокола CDP

Для проверки настройки протокола CDP используйте команду **show cdp**.

```
Router# show cdp


Global CDP information:

       Sending CDP packets every 120 seconds

       Sending a holdtime value of 180 seconds

       Sending CDPv2 advertisements is enabled

Router#
```

Включение протокола CDP на интерфейсе

Для включения протокола CDP на интерфейсе используйте следующую команду в режиме настройки интерфейса.

Команда	Назначение
`Router(config-if)# cdp enable`	Включение протокола CDP на интерфейсе.

В следующем примере показано включение протокола CDP на интерфейсе Fast Ethernet 0/1/1.

```
Router(config)# interface fastethernet 0/1/1

Router(config-if)# cdp enable
```

Проверка настройки интерфейса CDP

Для проверки настройки протокола CDP для интерфейса используйте команду **show cdp interface**.

```
Router# show cdp interface fastethernet 0/1/1


FastEthernet0/1/1 is up, line protocol is up

 Encapsulation ARPA

 Sending CDP packets every 120 seconds

 Holdtime is 180 seconds

Router#
```

Проверка соседей по протоколу CDP

Для проверки информации о соседних устройствах используйте команду **show cdp neighbors**.

```
Router# show cdp neighbors


Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge

                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID

tftp-switch      Fas 0/0             125       R S I     2811      Fas 0/3/6

hwic-3745-2      Fas 0/1/0           149       R S I     3745      Fas 0/1

Router#
```

Мониторинг и поддержка протокола CDP

Команда	Назначение
Router# clear cdp counters	Сброс значений всех счетчиков трафика.
`Router# clear cdp table`	Удаление таблицы данных протокола CDP о соседних устройствах.
Router# show cdp	Проверка глобальной информации, например, частоты передач и времени удержания передаваемых пакетов.
Router# show cdp entry entry_name [*protocol* | *version*]	Проверка информации об указанном соседнем устройстве. Отображаемые данные можно ограничить информацией о версии протокола.
Router# show cdp interface *interface-id*	Проверка информации об интерфейсах, на которых включен протокол CDP.
`Router# show cdp neighbors` *interface-id* [*detail*]	Проверка информации о соседних устройствах. Отображаемые данные можно ограничить информацией для соседних устройств на заданном интерфейсе либо расширить для отображения дополнительной информации.
Router# show cdp traffic	Проверка состояния счетчиков CDP, включая количество принятых и отправленных пакетов и ошибки контрольной суммы.

Настройка анализатора коммутируемых портов (SPAN)

В данном разделе приведено описание настройки сеанса SPAN на интерфейсной плате EtherSwitch HWIC.

Примечание. Интерфейсная плата EtherSwitch HWIC поддерживает не более одного сеанса SPAN.

Примечание. Поддерживается либо тип мониторинга Tx, либо типы Tx и Rx одновременно.

- Настройка источников SPAN
- Настройка узлов назначения SPAN
- Проверка сеанса SPAN
- Удаление источников или узлов назначения из сеанса SPAN

Настройка источников SPAN

Для настройки источника для сеанса SPAN используйте следующую команду в режиме глобальной конфигурации.

Команда	Назначение
Router(config)# monitor session **1** {source { interface *interface-id*} | {vlan *vlan_ID*}} [, | - | rx | tx | both]	Задание номера сеанса SPAN (номер 1), интерфейсов источника или сетей VLAN и направление передачи трафика, за которым осуществляется мониторинг.

В следующем примере показана настройка сеанса SPAN для мониторинга двунаправленного трафика от интерфейса источника Fast Ethernet 0/3/1.

```
Router(config)# monitor session 1 source interface fastethernet 0/3/1
```

Настройка узлов назначения SPAN

Для настройки узла назначения для сеанса SPAN используйте следующую команду в режиме глобальной конфигурации.

Команда	Назначение
Router(config)# monitor session **1** {destination {interface *type interface-id*} [Router#] | {vlan *vlan*_ID}}	Задание номера сеанса SPAN (номер 1), интерфейсов назначения или сетей VLAN.

Проверка сеанса SPAN

Для проверки интерфейсов источника и назначения для сеанса SPAN используйте команду **show monitor session**.

```
Router# show monitor session 1

Session 1

---------

Source Ports:

RX Only: None

TX Only: None

Both: Fa0/1/0

Source VLANs:

RX Only: None

TX Only: None

Both: None

Destination Ports: Fa0/1/1

Filter VLANs: None
```

Удаление источников или узлов назначения из сеанса SPAN

Для удаления интерфейсов источника или назначения из сеанса SPAN используйте следующую команду в режиме глобальной конфигурации.

Команда	Назначение
Router(config)# no monitor session **1**	Сброс настроек текущей конфигурации SPAN.

Настройка управления электропитанием на интерфейсе

Войдите в привилегированный режим EXEC и выполните следующие действия для управления электропитанием IP-телефонов Cisco.

СВОДКА ШАГОВ

1. **configure terminal**

2. **interface fastethernet** *interface-id*

3. power inline auto/never

ПОДРОБНОЕ ОПИСАНИЕ ШАГОВ

	Команда	Назначение
Шаг 1	Router# configure terminal	Вход в режим глобальной конфигурации.
Шаг 2	Router(config)# **interface fastethernet** *interface-id*	Выбор интерфейса Fast Ethernet, который необходимо настроить.
Шаг 3	Router(config-if)# power inline auto/never	Настройка порта, который будет использоваться для автоматического обеспечения электропитания IP-телефона Cisco. Для отключения электропитания порта от линии используйте команду **never**.

Проверка настроек управления электропитанием на интерфейсе

Для проверки настроек электропитания портов используйте команду **show power inline**, как показано ниже.

```
Router# show power inline


PowerSupply   SlotNum.   Maximum   Allocated    Status

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

INT-PS          0       120.000    101.500     PS GOOD


Interface     Config     Phone     Powered      PowerAllocated

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

Fa0/1/0         auto       Cisco     On           6.300 Watts

Fa0/1/1         auto       Cisco     On           6.300 Watts

Fa0/1/2         auto       Cisco     On           6.300 Watts

Fa0/1/3         auto       Cisco     On           6.300 Watts

Fa0/1/4         auto       Cisco     On           6.300 Watts

Fa0/1/5         auto       Cisco     On           6.300 Watts

Fa0/1/6         auto       Cisco     On           6.300 Watts

Fa0/1/7         auto       Cisco     On           6.300 Watts
```

```
Fa0/3/0         auto       Cisco     On           6.300 Watts

Fa0/3/1         auto       Cisco     On           6.300 Watts

Fa0/3/2         auto       Cisco     On           6.300 Watts

Fa0/3/3         auto       Cisco     On           6.300 Watts

Fa0/3/4         auto       Cisco     On           6.300 Watts

Fa0/3/5         auto       Cisco     On           6.300 Watts

Fa0/3/6         auto       IEEE-2    On           7.000 Watts

Fa0/3/7         auto       Cisco     On           6.300 Watts
```

Проверка других параметров электропитания с помощью интерфейса командной строки

Для проверки настроек электропитания портов используйте команду **show power inline**, как показано ниже.

```
Router# show power inline [actual | interface fastethernet interface-id | configured]
```

Настройка коммутации с мультиадресной IP-рассылкой уровня 3

В этих разделах приведено описание настройки коммутации с мультиадресной IP-рассылкой уровня 3.

- Глобальное включение маршрутизации с мультиадресной IP-рассылкой
- Включение протокола PIM на интерфейсах уровня 3
- Проверка параметров коммутации аппаратного обеспечения с мультиадресной IP-рассылкой уровня 3
- Проверка таблицы маршрутизации мультиадресной IP-рассылки

Глобальное включение маршрутизации с мультиадресной IP-рассылкой

Перед включением коммутации с мультиадресной IP-рассылкой уровня 3 на интерфейсах уровня 3 необходимо произвести глобальное включение маршрутизации с мультиадресной IP-рассылкой.

Полную информацию и описание процедур см. в следующих публикациях:

- *Руководство по настройке IP для Cisco IOS*, версия 12.2. Перейдите по следующему адресу:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/

- *Справочник по командам IP Cisco IOS, том 1 из 3: Адресация и услуги*, версия 12.2. Перейдите по следующему адресу:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipras_r/index.htm

- *Справочник по командам IP Cisco IOS, том 2 из 3: Протоколы и маршрутизация*, версия 12.2. Перейдите по следующему

адресу:

/en/US/products/sw/iosswrel/ps1835/products_command_reference_book09186a008008027c.html

• *Справочник по командам IP Cisco IOS, том 3 из 3: Мультиадресная рассылка*, версия 12.2. Перейдите по следующему адресу:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fiprmc_r/index.htm

Для глобального включения маршрутизации с мультиадресной IP-рассылкой используйте следующую команду в режиме глобальной конфигурации.

Команда	Назначение
Router(config)# **ip multicast-routing**	Глобальное включение маршрутизации с мультиадресной IP-рассылкой.

Включение мультиадресной IP-рассылки, не зависящей от протокола (PIM) на интерфейсах уровня 3

Перед включением функции коммутации с мультиадресной IP-рассылкой уровня 3 на интерфейсах необходимо включить протокол PIM на интерфейсах уровня 3.

Войдите в режим глобальной конфигурации и выполните следующие действия для включения протокола PIM на интерфейсах уровня 3.

СВОДКА ШАГОВ

1. **interface vlan** vlan-id

2. **ip pim** {**dense-mode** | **sparse-mode** | **sparse-dense-mode**}

ПОДРОБНОЕ ОПИСАНИЕ ШАГОВ

	Команда	Назначение
Шаг 1	`Router(config)# interface vlan vlan-id`	Выбор интерфейса, который необходимо настроить.
Шаг 2	`Router(config-if)# ip pim {dense-mode | sparse-mode | sparse-dense-mode}`	Включение протокола PIM на интерфейсах уровня 3.

В следующем примере показано включение протокола PIM на интерфейсе с использованием режима по умолчанию (**sparse-dense-mode**).

```
Router(config-if)# ip pim sparse-dense mode

Router(config-if)#
```

В следующем примере показан способ включения разреженного режима PIM на интерфейсе.

```
Router(config-if)# ip pim sparse-mode

Router(config-if)#
```

Проверка параметров коммутации аппаратного обеспечения с мультиадресной IP-рассылкой уровня 3

Примечание. Команда **show interface statistics** не используется для проверки пакетов, коммутируемых аппаратно. Используйте ее только для проверки пакетов, коммутируемых программным способом.

Команда **show ip pim interface count** используется для проверки включения коммутации с мультиадресной IP-рассылкой уровня 3 на интерфейсах IP PIM, а также для проверки количества пакетов, полученных и отправленных через интерфейс.

Для проверки информации о коммутации с мультиадресной IP-рассылкой уровня 3 на интерфейсе IP PIM уровня 3 используйте команду **show**.

Шаг 1 `VLAN Name Status Ports` **show ip pim interface count**

```
State:* - Fast Switched, D - Distributed Fast Switched

      H - Hardware Switching Enabled

Address          Interface            FS  Mpackets In/Out

10.0.0.1         VLAN1                *   151/0

Router#
```

Шаг 2 `----` `--------------------------------` `---------` `--------------------------------` **show ip mroute count**

```
IP Multicast Statistics

5 routes using 2728 bytes of memory

4 groups, 0.25 average sources per group

Forwarding Counts:Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second

Other counts:Total/RPF failed/Other drops(OIF-null, rate-limit etc)


Group:224.9.9.9, Source count:1, Packets forwarded: 0, Packets received: 66
```

```
 Source:10.0.0.2/32, Forwarding:0/0/0/0, Other:66/0/66

Group:224.10.10.10, Source count:0, Packets forwarded: 0, Packets received: 0

Group:224.0.1.39, Source count:0, Packets forwarded: 0, Packets received: 0

Group:224.0.1.40, Source count:0, Packets forwarded: 0, Packets received: 0

Router#
```

Примечание. Отрицательное значение счетчика означает, что список исходящих интерфейсов для соответствующей записи NULL, а поток данных еще активен.

Шаг 3 `1 default active Fa0/1/0, Fa0/1/1, Fa0/1/2/` **show ip interface vlan 1**

```
Vlan1 is up, line protocol is up

 Internet address is 10.0.0.1/24

 Broadcast address is 255.255.255.255

 Address determined by setup command

 MTU is 1500 bytes

 Helper address is not set

 Directed broadcast forwarding is disabled

 Multicast reserved groups joined: 224.0.0.1 224.0.0.2 224.0.0.22 224.0.0.13

 Outgoing access list is not set

 Inbound  access list is not set

 Proxy ARP is enabled

 Local Proxy ARP is disabled

 Security level is default

 Split horizon is enabled

 ICMP redirects are always sent

 ICMP unreachables are always sent

 ICMP mask replies are never sent

 IP fast switching is enabled
```

```
 IP fast switching on the same interface is disabled

 IP Flow switching is disabled

 IP CEF switching is enabled

 IP CEF Fast switching turbo vector

 IP multicast fast switching is enabled

 IP multicast distributed fast switching is disabled

 IP route-cache flags are Fast, CEF

 Router Discovery is disabled

 IP output packet accounting is disabled

 IP access violation accounting is disabled

 TCP/IP header compression is disabled

 RTP/IP header compression is disabled

 Policy routing is disabled

 Network address translation is disabled

 WCCP Redirect outbound is disabled

 WCCP Redirect inbound is disabled

 WCCP Redirect exclude is disabled

 BGP Policy Mapping is disabled

Router#
```

Проверка таблицы маршрутизации мультиадресной IP-рассылки

Для проверки таблицы маршрутизации мультиадресной IP-рассылки используйте команду **show ip mroute**.

```
Router# show ip mroute 224.10.103.10


IP Multicast Routing Table

Flags:D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,

      L - Local, P - Pruned, R - RP-bit set, F - Register flag,

      T - SPT-bit set, J - Join SPT, M - MSDP created entry,

      X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
```

```
      U - URD, I - Received Source Specific Host Report, Z - Multicast Tunnel,

      Y - Joined MDT-data group, y - Sending to MDT-data group

Outgoing interface flags:H - Hardware switched, A - Assert winner

Timers:Uptime/Expires

Interface state:Interface, Next-Hop or VCD, State/Mode



(*, 224.10.10.10), 00:09:21/00:02:56, RP 0.0.0.0, flags:DC

 Incoming interface:Null, RPF nbr 0.0.0.0

 Outgoing interface list:

   Vlan1, Forward/Sparse-Dense, 00:09:21/00:00:00, H



Router#
```

Примечание. Флаг RPF-MFD указывает на то, что для потока данных осуществляется только аппаратная коммутация. Флаг H указывает на то, что для потока данных осуществляется аппаратная коммутация на исходящем интерфейсе.

Настройка функции IGMP Snooping

В данном разделе приведена информация по настройке функции IGMP Snooping (отслеживания IGMP) на маршрутизаторе. Раздел содержит следующую информацию и описание следующих процедур.

- Включение и отключение функции IGMP Snooping
- Включение обработки IGMP Immediate-Leave
- Статическая настройка интерфейса для присоединения к группе
- Настройка порта мультиадресной рассылки маршрутизатора

Включение и отключение функции IGMP Snooping

По умолчанию функция IGMP Snooping на интерфейсных платах EtherSwitch HWIC глобально включена. При глобальном включении или выключении параметры изменяются на всех существующих интерфейсах сетей VLAN. По умолчанию функция IGMP Snooping включена на всех сетях VLAN, однако ее можно включать и выключать для каждой сети в отдельности.

При глобальном изменении параметров функции IGMP Snooping изменяются параметры функции IGMP Snooping, настроенные для отдельных сетей VLAN. Если глобальное отслеживание отключено, включить отслеживание для сетей VLAN невозможно. Если глобальное отслеживание включено, можно включить отслеживание для отдельных сетей VLAN.

Войдите в привилегированный режим EXEC и выполните следующие действия для глобального включения функции IGMP Snooping на интерфейсных платах EtherSwitch HWIC.

СВОДКА ШАГОВ

1. **configure terminal**
2. **ip igmp snooping**
3. **end**
4. **show ip igmp snooping**
5. **copy running-config startup-config**

ПОДРОБНОЕ ОПИСАНИЕ ШАГОВ

	Команда	Назначение
Шаг 1	`configure terminal`	Вход в режим глобальной конфигурации.
Шаг 2	`ip igmp snooping`	Глобальное включение функции IGMP Snooping на всех существующих интерфейсах сетей VLAN.
Шаг 3	`end`	Возврат к привилегированному режиму EXEC.
Шаг 4	`show ip igmp snooping`	Отображение настроек отслеживания.
Шаг 5	`copy running-config startup-config`	Сохранение настроек в загрузочной конфигурации (необязательно).

Для глобального отключения функции IGMP Snooping на всех интерфейсах VLAN используйте команду **no ip igmp snooping** в режиме глобальной конфигурации.

Войдите в привилегированный режим EXEC и выполните следующие действия для включения функции IGMP Snooping на интерфейсе сети VLAN.

СВОДКА ШАГОВ

1. **configure terminal**
2. **ip igmp snooping vlan** vlan-id
3. **end**
4. **show ip igmp snooping** [**vlan** vlan-id]
5. **copy running-config startup-config**

ПОДРОБНОЕ ОПИСАНИЕ ШАГОВ

	Команда	Назначение
Шаг 1	**configure terminal**	Вход в режим глобальной конфигурации.
Шаг 2	**ip igmp snooping vlan** vlan-id	Включение функции IGMP Snooping на интерфейсе сети VLAN.
Шаг 3	**end**	Возврат к привилегированному режиму EXEC.
Шаг 4	**show ip igmp snooping** [**vlan** vlan-id]	Отображение настроек отслеживания. *vlan-id* — номер сети VLAN (необязательно).
Шаг 5	**copy running-config startup-config**	Сохранение настроек в загрузочной конфигурации (необязательно).

Для отключения функции IGMP Snooping на интерфейсе сети VLAN используйте команду **no ip igmp snooping vlan** *vlan-id* в режиме глобальной конфигурации, указав номер сети VLAN (например, vlan1).

Включение обработки IGMP Immediate-Leave

После включения обработки IGMP Immediate-Leave интерфейсная плата EtherSwitch HWIC немедленно удаляет порт из группы мультиадресной IP-рассылки при обнаружении сообщения выхода IGMP версии 2 на этом порте. Обработка Immediate-Leave позволяет коммутатору удалять из таблицы переадресации интерфейс, с которого было отправлено сообщение о выходе, без предварительной отправки на интерфейс запросов о группе. Функцию Immediate-Leave следует использовать только в том случае, если для каждого порта сети VLAN имеется только одно принимающее устройство.

Войдите в привилегированный режим EXEC и выполните следующие действия для включения обработки IGMP Immediate-Leave.

СВОДКА ШАГОВ

1. **configure terminal**
2. **ip igmp snooping vlan** *vlan-id* **immediate-leave**
3. **end**

ПОДРОБНОЕ ОПИСАНИЕ ШАГОВ

	Команда	Назначение
Шаг 1	**configure terminal**	Вход в режим глобальной конфигурации.
	ip igmp snooping vlan *vlan-id*	

Шаг 2	**immediate-leave**	Включение обработки IGMP Immediate-Leave на интерфейсе сети VLAN.
Шаг 3	**end**	Возврат к привилегированному режиму EXEC.

Для отключения обработки Immediate-Leave выполните действия шагов 1 и 2 для входа в режим настройки интерфейса, затем используйте команду **no ip igmp snooping vlan** *vlan-id* **immediate-leave** в режиме глобальной конфигурации.

Статическая настройка интерфейса для присоединения к группе

Порты обычно добавляются в группы мультиадресной рассылки после получения отчета IGMP, однако также существует возможность выполнить статическую настройку сетевого узла на интерфейсе.

Войдите в привилегированный режим EXEC и выполните следующие действия для добавления порта в группу мультиадресной рассылки.

СВОДКА ШАГОВ

1. **configure terminal**
2. **ip igmp snooping vlan** *vlan-id* **static** mac-address **interface** interface-id
3. **end**
4. **show mac-address-table multicast** [**vlan** vlan-id] [**user** | **igmp-snooping**] [**count**]
5. **copy running-config startup-config**

ПОДРОБНОЕ ОПИСАНИЕ ШАГОВ

	Команда	Назначение
Шаг 1	**configure terminal**	Вход в режим глобальной конфигурации.
Шаг 2	**ip igmp snooping vlan** *vlan-id* **static** mac-address **interface** interface-id	Статическая настройка порта в качестве члена группы мультиадресной рассылки. • *vlan-id* — идентификатор сети VLAN группы мультиадресной рассылки. • *mac-address* — MAC-адрес группы. • *interface-id* — порт, входящий в состав группы.
Шаг 3	**end**	Возврат к привилегированному режиму EXEC.
	show mac-address-table multicast [**vlan**	

Шаг 4	vlan-id] [**user** | **igmp-snooping**] [**count**]	Вывод записей таблицы MAC-адресов для сети VLAN. • *vlan-id* — идентификатор сети VLAN группы мультиадресной рассылки. • **user** — вывод только записей мультиадресной рассылки, настроенных пользователем. • **igmp-snooping** — вывод записей, полученных в ходе отслеживания IGMP. • **count** — вывод общего количества записей по выбранным критериям, а не фактического количества записей.
Шаг 5	**copy running-config startup-config**	Сохранение настроек в загрузочной конфигурации (необязательно).

Настройка порта мультиадресной рассылки маршрутизатора

Войдите в привилегированный режим EXEC и выполните следующие действия для установки статического соединения с мультиадресным маршрутизатором.

СВОДКА ШАГОВ

1. **configure terminal**
2. **ip igmp snooping vlan** *vlan-id* **mrouter** {**interface** *interface-id* | **learn pim-dvmrp**}
3. **end**
4. **show ip igmp snooping** [**vlan** *vlan-id*]
5. **show ip igmp snooping mrouter** [**vlan** vlan-id]
6. **copy running-config startup-config**

ПОДРОБНОЕ ОПИСАНИЕ ШАГОВ

	Команда	Назначение
Шаг 1	**configure terminal**	Вход в режим глобальной конфигурации.
Шаг 2	**ip igmp snooping vlan** *vlan-id* **mrouter** {**interface** *interface-id* | **learn pim-dvmrp**}	Задание идентификатора сети VLAN мультиадресного маршрутизатора (от 1 до 1001).

		Задание интерфейса доступа к мультиадресному маршрутизатору.
Шаг 3	**end**	Возврат к привилегированному режиму EXEC.
Шаг 4	**show ip igmp snooping** [**vlan** *vlan-id*]	Проверка включения функции IGMP Snooping на интерфейсе сети VLAN.
Шаг 5	**show ip igmp snooping mrouter** [**vlan** vlan-id]	Отображение информации об интерфейсах мультиадресных маршрутизаторов, настроенных как динамически, так и вручную.
Шаг 6	**copy running-config startup-config**	Сохранение настроек в загрузочной конфигурации (необязательно).

Настройка контроля шторма по портам

Для блокировки пересылки ненужного лавинного трафика можно использовать следующие процедуры. В данном разделе приведено описание настройки контроля шторма по портам и соответствующих параметров маршрутизатора. Раздел содержит следующие процедуры настройки.

- Включение контроля шторма по портам
- Выключение контроля шторма по портам

По умолчанию подавление одноадресной, широковещательной и мультиадресной рассылок отключено.

Включение контроля шторма по портам

Войдите в привилегированный режим EXEC и выполните следующие действия для включения контроля шторма по портам.

СВОДКА ШАГОВ

1. **configure terminal**
2. **interface** *interface-id*
3. **storm-control** {**broadcast** | **multicast** | **unicast**} **level** level-high [level-low]
4. **storm-control action shutdown**
5. **end**
6. **show storm-control** [**interface**] [{**broadcast** | **multicast** | **unicast** | **history**}]

ПОДРОБНОЕ ОПИСАНИЕ ШАГОВ

	Команда	Назначение
Шаг 1	**configure terminal**	Вход в режим глобальной конфигурации.
Шаг 2	**interface** *interface-id*	Вход в режим настройки интерфейса и указание порта, который необходимо настроить.
Шаг 3	**storm-control** {**broadcast** | **multicast** | **unicast**} **level** level-high [level-low]	Настройка контроля шторма для портов при одноадресной, широковещательной и мультиадресной рассылке. Укажите верхний порог для трафика одноадресной, широковещательной и мультиадресной рассылки. Функция контроля шторма срабатывает при достижении этого уровня обработки трафика. Укажите нижний порог (необязательно). Передача будет продолжена в нормальном режиме (если задействуется функция фильтрации) после снижения объема трафика ниже этого уровня.
Шаг 4	**storm-control action shutdown**	Для отключения порта во время шторма используйте ключевое слово **shutdown**. По умолчанию включается фильтрация трафика.
Шаг 5	**end**	Возврат к привилегированному режиму EXEC.
Шаг 6	**show storm-control** [**interface**] [{**broadcast** | **multicast** | **unicast** | **history**}]	Проверка введенных пользователем данных.

Примечание. Если для какого-либо типа трафика будет превышен верхний порог, передача других видов трафика также будет остановлена.

Выключение контроля шторма по портам

Войдите в привилегированный режим EXEC и выполните следующие действия для выключения контроля шторма по портам.

СВОДКА ШАГОВ

1. **configure terminal**

2. **interface** *interface-id*

3. **no storm-control** {**broadcast** | **multicast** | **unicast**} **level**

4. **no storm-control action shutdown**

5. **end**

6. **show storm-control** {**broadcast** | **multicast** | **unicast**}

ПОДРОБНОЕ ОПИСАНИЕ ШАГОВ

	Команда	Назначение
Шаг 1	**configure terminal**	Вход в режим глобальной конфигурации.
Шаг 2	**interface** *interface-id*	Вход в режим настройки интерфейса и указание порта, который необходимо настроить.
Шаг 3	**no storm-control** {**broadcast** | **multicast** | **unicast**} **level**	Выключение контроля шторма по портам.
Шаг 4	**no storm-control action shutdown**	Выключение определенного действия функции контроля шторма.
Шаг 5	**end**	Возврат к привилегированному режиму EXEC.
Шаг 6	**show storm-control** {**broadcast** | **multicast** | **unicast**}	Проверка введенных пользователем данных.

Настройка стеков

Стек — это два модуля коммутатора, объединенные в одном шасси и выполняющие функцию одного коммутатора. Если шасси содержит два модуля коммутатора, пользователь должен настроить оба модуля для работы в стековом режиме. Это достигается посредством выбора одного порта в каждом модуле и настройки его для работы в качестве партнера в стеке. После настройки портов для работы в стеке их необходимо физически соединить посредством кабеля. Для работы в качестве партнера в стеке можно выбрать любой порт модуля коммутатора.

Войдите в привилегированный режим EXEC и выполните следующие действия для пары портов двух различных модулей коммутатора для работы в качестве партнера в стеке.

СВОДКА ШАГОВ

1. interface fastethernet *interface-id*

2. no shutdown

3. **switchport stacking-partner interface FastEthernet** *partner-interface-id*

4. exit

5. interface fastethernet partner-*interface-id*

6. no shutdown

7. end

ПОДРОБНОЕ ОПИСАНИЕ ШАГОВ

	Команда	Назначение
Шаг 1	`Router(config)#interface fastethernet` *interface-id*	Выбор интерфейса, который необходимо настроить.
Шаг 2	`Router(config-if)#no shutdown`	Активация интерфейса. Используется только в том случае, если интерфейс был отключен.
Шаг 3	`Router(config-if)#`**`switchport stacking-partner interface FastEthernet`** *partner-interface-id*	Выбор и настройка порта — партнера в стеке.
Шаг 4	`Router(config-if)#exit`	Выход из режима настройки интерфейса.
Шаг 5	`Router(config)#interface fastethernet` partner-*interface-id*	Выбор интерфейса — партнера в стеке.
Шаг 6	`Router(config-if)#no shutdown`	Активация интерфейса — партнера в стеке.
Шаг 7	`Router(config-if)#end`	Выход из режима настройки.

Примечание. На обоих портах — партнерах в стеке для параметров **speed** и **duplex** необходимо установить значение **auto**.

Внимание Если стек не используется, то интерфейсы, настроенные для работы в стеке, переходят в состояние отключения **shutdown**. Другие порты, не настроенные для работы в стеке, продолжают работать в нормальном режиме.

Настройка мостового соединения при отказе

В данном разделе приведено описание настройки мостового соединения при отказе для коммутатора. Раздел содержит следующую информацию по настройке.

- Настройки параметров мостового соединения при отказе по умолчанию
- Создание группы моста
- Предотвращение пересылки данных о станциях, полученных в динамическом режиме

- Настройка времени устаревания таблицы моста
- Фильтрация кадров посредством указанного MAC-адреса
- Настройка параметров протокола Spanning Tree
- Мониторинг и обслуживание сети

Настройки параметров мостового соединения при отказе по умолчанию

В таблице 2 показана настройка параметров мостового соединения при отказе по умолчанию.

Функция	Значение по умолчанию
Bridge groups (Группы мостов)	Не указываются и не назначаются интерфейсу. Протокол STP для моста сети VLAN не задан.
Switch forwards frames for stations that it has dynamically learned (Коммутатор пересылает кадры для станций, данные о которых получены в динамическом режиме).	Включено
Bridge table aging time for dynamic entries (Время устаревания таблицы моста для динамических записей)	300 секунд.
MAC-layer frame filtering (Фильтрация кадров уровня MAC-адресов)	Отключено.
Параметры протокола Spanning Tree. • Switch priority (Приоритет коммутатора) • Interface priority (Приоритет интерфейса) • Interface path cost (Стоимость пути к интерфейсу) • Hello BPDU interval (Интервал пакетов приветствия BPDU) • Forward-delay interval (Интервал задержки пересылки) • Maximum idle interval (Максимальный интервал простоя)	• 32768. • 128. • 10 Мбит/с: 100. 100 Мбит/с: 19. 1000 Мбит/с: 4. • 2 секунды. • 20 секунд. • 30 секунд.

Создание группы моста

Для настройки мостового соединения при отказе для интерфейсов SVI эти интерфейсы должны быть назначены группам моста. Все интерфейсы одной группы принадлежат одному домену моста. Каждый интерфейс SVI может быть назначен

только одной группе моста.

Войдите в привилегированный режим EXEC и выполните следующие действия для создания группы моста и назначения ей интерфейса.

СВОДКА ШАГОВ

1. **configure terminal**
2. **no ip routing**
3. **bridge** *bridge-group* **protocol vlan-bridge**
4. **interface** *interface-id*
5. **bridge-group** *bridge-group*
6. **end**
7. **show vlan-bridge**
8. **show running-config**
9. **copy running-config startup-config**

ПОДРОБНОЕ ОПИСАНИЕ ШАГОВ

	Команда	Назначение
Шаг 1	**configure terminal**	Вход в режим глобальной конфигурации.
Шаг 2	**no ip routing**	Отключение IP-маршрутизации.
Шаг 3	**bridge** *bridge-group* **protocol vlan-bridge**	Назначение номера группы моста и задание протокола Spanning Tree моста сети VLAN, который будет использоваться в группе моста. Ключевые слова **ibm** and **dec** не поддерживаются. Для параметра *bridge-group* укажите номер группы моста. Диапазон значений составляет от 1 до 255. Мостовая передача кадров производится только между интерфейсами одной группы.
Шаг 4	**interface** *interface-id*	Вход в режим настройки интерфейса и выбор интерфейса, которому необходимо назначить группу моста. Необходимо указать интерфейс SVI: это интерфейс сети VLAN, созданный посредством команды

		глобальной настройки **interface vlan** *vlan-id.* Для этих портов необходимо назначить IP-адреса.
Шаг 5	**bridge-group** *bridge-group*	Назначение интерфейса группе моста, созданной в шаге 2. По умолчанию интерфейс не назначается ни одной группе моста. Один интерфейс можно назначить только одной группе моста.
Шаг 6	**end**	Возврат к привилегированному режиму EXEC.
Шаг 7	**show vlan-bridge**	Проверка режима пересылки (необязательно).
Шаг 8	**show running-config**	Проверка введенных пользователем данных (необязательно).
Шаг 9	**copy running-config startup-config**	Сохранение записей в файл конфигурации (необязательно).

Для удаления группы моста используйте команду глобальной настройки **no bridge** *bridge-group* **protocol vlan-bridge**. Для удаления интерфейса из группы моста используйте команду настройки интерфейса **no bridge-group** *bridge-group.*

Предотвращение пересылки данных о станциях, полученных в динамическом режиме

По умолчанию коммутатор пересылает кадры для станций, полученные в динамическом режиме. После отключения этой функции коммутатор отправляет только кадры, адреса которых были статически настроены в кэш пересылки.

Войдите в привилегированный режим EXEC и выполните следующие действия для предотвращения пересылки данных о станциях, полученных в динамическом режиме.

СВОДКА ШАГОВ

1. **configure terminal**
2. **no bridge** *bridge-group* **acquire**
3. **end**
4. **show running-config**
5. **copy running-config startup-config**

ПОДРОБНОЕ ОПИСАНИЕ ШАГОВ

	Команда	Назначение

Шаг 1	**configure terminal**	Вход в режим глобальной конфигурации.
Шаг 2	**no bridge** *bridge-group* **acquire**	Остановка пересылки коммутатором данных о станциях, полученных в динамическом режиме посредством режима обнаружения и ограничение пересылки кадров на станции, которые были настроены статически. Коммутатор будет фильтровать все кадры за исключением тех, адреса назначения которых были статически настроены в кэш пересылки. Для настройки статического адреса используйте команду **bridge** *bridge-group* **address** *mac-address* {**forward** | **discard**} в режиме глобальной конфигурации. Для параметра *bridge-group* укажите номер группы моста. Диапазон значений составляет от 1 до 255.
Шаг 3	**end**	Возврат к привилегированному режиму EXEC.
Шаг 4	**show running-config**	Проверка введенных пользователем данных.
Шаг 5	**copy running-config startup-config**	Сохранение записей в файл конфигурации (необязательно).

Для включения отправки коммутатором пересылки кадров на станции, данные о которых были получены в динамическом режиме, используйте команду **bridge** *bridge-group* **acquire** в режиме глобальной конфигурации.

Настройка времени устаревания таблицы моста

На основании данных таблицы моста коммутатор пересылает, распространяет лавинным методом или отбрасывает пакеты. В таблице моста содержатся как статические, так и динамические записи. Статические записи вводятся пользователем. Динамические записи вводятся в ходе процесса обучения моста. По истечении определенного промежутка времени (времени устаревания) динамическая запись автоматически удаляется. Это время отсчитывается от момента создания или последнего обновления записи.

Если на коммутируемой сети существует вероятность перемещения узлов, уменьшите время устаревания, чтобы коммутатор быстрее адаптировался к измененным значениям параметров. Если узлы в коммутируемой сети отправляют пакеты не постоянно, увеличьте время устаревания для обеспечения более длительного хранения динамических записей и снижения вероятности лавинного потока при повторной отправке пакетов узлами.

Войдите в привилегированный режим EXEC и выполните следующие действия для настройки времени устаревания.

СВОДКА ШАГОВ

1. **configure terminal**
2. **bridge** *bridge-group* **aging-time** *seconds*
3. **end**

4. **show running-config**

5. **copy running-config startup-config**

ПОДРОБНОЕ ОПИСАНИЕ ШАГОВ

	Команда	Назначение
Шаг 1	**configure terminal**	Вход в режим глобальной конфигурации.
Шаг 2	**bridge** *bridge-group* **aging-time** *seconds*	Указание времени, в течение которого динамическая запись остается в таблице моста (время отсчитывается с момента создания или последнего обновления записи). • Для параметра *bridge-group* укажите номер группы моста. Диапазон значений составляет от 1 до 255. • Для параметра *seconds* введите значение от 0 до 1 000 000. Значение по умолчанию — 300 секунд.
Шаг 3	**end**	Возврат к привилегированному режиму EXEC.
Шаг 4	**show running-config**	Проверка введенных пользователем данных.
Шаг 5	**copy running-config startup-config**	Сохранение записей в файл конфигурации (необязательно).

Для возврата к значению времени устаревания по умолчанию используйте команду **no bridge** *bridge-group* **aging-time** в режиме глобальной конфигурации.

Фильтрация кадров посредством указанного MAC-адреса

Коммутатор анализирует кадры и отправляет их через объединенную сеть на адрес назначения. На исходный сегмент сети кадр не пересылается. Для настройки конкретных административных фильтров кадров по другим критериям (помимо путей к адресу назначения) можно использовать программное обеспечение.

Кадры можно фильтровать по MAC-адресу назначения станции. В системе, в которой не настроены потери по производительности, можно настроить любое количество адресов.

Войдите в привилегированный режим EXEC и выполните следующие действия для включения фильтрации по MAC-адресам.

СВОДКА ШАГОВ

1. **configure terminal**

2. **bridge** *bridge-group* **address** *mac-address* {**forward** | **discard**} [*interface-id*]

3. **end**

4. **show running-config**

5. **copy running-config startup-config**

ПОДРОБНОЕ ОПИСАНИЕ ШАГОВ

	Команда	Назначение
Шаг 1	**configure terminal**	Вход в режим глобальной конфигурации.
Шаг 2	**bridge** *bridge-group* **address** *mac-address* {**forward** | **discard**} [*interface-id*]	Задание MAC-адреса для игнорирования или пересылки. • Для параметра *bridge-group* укажите номер группы моста. Диапазон значений составляет от 1 до 255. • Для параметра **address** *mac-address* укажите MAC-адрес назначения для фильтрации. • Для пересылки кадра, отправляемого на определенный интерфейс, укажите ключевое слово **forward**. Если кадр необходимо проигнорировать, укажите ключевое слово **discard**. • Для параметра *interface-id* укажите интерфейс, на котором можно достичь этого адреса (необязательно).
Шаг 3	**end**	Возврат к привилегированному режиму EXEC.
Шаг 4	**show running-config**	Проверка введенных пользователем данных.
Шаг 5	**copy running-config startup-config**	Сохранение записей в файл конфигурации (необязательно).

Для отключения функции пересылки кадров используйте команду **no bridge** *bridge-group* **address** *mac-address* в режиме глобальной конфигурации.

Настройка параметров протокола Spanning Tree

Если некоторые значения параметров протокола Spanning Tree по умолчанию не отвечают требованиям настроек коммутатора, возможно, их потребуется изменить. Для изменения параметров, влияющих на работу протокола Spanning Tree в глобальном масштабе, используется команда **bridge** в режиме глобальной конфигурации в различных вариациях. Для изменения параметров, относящихся к интерфейсу, используется команда **bridge-group** в режиме глобальной конфигурации в различных вариациях.

Для настройки параметров протокола Spanning Tree можно выполнить любую задачу из следующих разделов.

- Изменение приоритета коммутатора
- Изменение приоритета интерфейса
- Назначение стоимости пути
- Настройка интервалов BPDU
- Отключение протокола Spanning Tree на интерфейсе

Примечание. Настройка параметров протокола Spanning Tree должна осуществляться только администраторами сети, хорошо разбирающимися в работе коммутаторов и параметрах протокола STP. Настройка параметров без предварительного планирования может привести к снижению производительности. Компетентным источником по коммутации является спецификация IEEE 802.1d; дополнительную информацию см. в приложении «Ссылки и рекомендованная литература» документа *Основы конфигурации Cisco IOS. Справочник по командам*, версия 12.2.

Изменение приоритета коммутатора

Можно глобально изменить приоритет отдельного коммутатора, если два коммутатора могут быть назначены в качестве корневого коммутатора, а также изменить вероятность выбора коммутатора в качестве корневого. Приоритет является настройкой по умолчанию, однако пользователь имеет возможность изменить его.

Войдите в привилегированный режим EXEC и выполните следующие действия для изменения приоритета коммутатора.

СВОДКА ШАГОВ

1. **configure terminal**
2. **bridge** *bridge-group* **priority** *number*
3. **end**
4. **show running-config**
5. **copy running-config startup-config**

ПОДРОБНОЕ ОПИСАНИЕ ШАГОВ

	Команда	Назначение
Шаг 1	**configure terminal**	Вход в режим глобальной конфигурации.
Шаг 2	**bridge** *bridge-group* **priority** *number*	Изменение приоритета коммутатора. • Для параметра *bridge-group* укажите номер группы моста. Диапазон значений составляет от 1 до 255.

		• Для параметра *number* введите значение от 0 до 65535. Значение по умолчанию — 32768. Чем меньше число, тем выше вероятность того, что коммутатор будет выбран в качестве корневого.
Шаг 3	**end**	Возврат к привилегированному режиму EXEC.
Шаг 4	**show running-config**	Проверка введенных пользователем данных.
Шаг 5	**copy running-config startup-config**	Сохранение записей в файл конфигурации (необязательно).

С ключом **no** эта команда не используется. Для возврата к значению по умолчанию используйте команду **bridge** *bridge-group* **priority** *number* в режиме глобальной конфигурации. Для изменения приоритета на интерфейсе используйте команду **bridge-group priority** в режиме настройки интерфейса (описание см. в следующем разделе).

Изменение приоритета интерфейса

Приоритет интерфейса можно изменять. Если два коммутатора имеют равные возможности для назначения в качестве корневого коммутатора, посредством изменения приоритета можно выбрать один из них. В качестве корневого будет назначен коммутатор с меньшим значением приоритета интерфейса.

Войдите в привилегированный режим EXEC и выполните следующие действия для изменения приоритета интерфейса.

СВОДКА ШАГОВ

1. **configure terminal**
2. **interface** *interface-id*
3. **bridge-group** *bridge-group* **priority** *number*
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

ПОДРОБНОЕ ОПИСАНИЕ ШАГОВ

	Команда	Назначение
Шаг 1	**configure terminal**	Вход в режим глобальной конфигурации.
Шаг 2	**interface** *interface-id*	Вход в режим настройки интерфейса и указание интерфейса, приоритет которого необходимо изменить.

Шаг 3	**bridge-group** *bridge-group* **priority** *number*	Изменение приоритета интерфейса. • Для параметра *bridge-group* укажите номер группы моста. Диапазон значений составляет от 1 до 255. • Для параметра *number* введите значение от 0 до 255. Чем меньше число, тем выше вероятность того, что интерфейс на коммутаторе будет выбран в качестве корневого. Значение по умолчанию — 128.
Шаг 4	**end**	Возврат к привилегированному режиму EXEC.
Шаг 5	**show running-config**	Проверка введенных пользователем данных.
Шаг 6	**copy running-config startup-config**	Сохранение записей в файл конфигурации (необязательно).

Для возврата к значению по умолчанию используйте команду **bridge-group** *bridge-group* **priority** *number* в режиме настройки интерфейса.

Назначение стоимости пути

С каждым интерфейсом связано значение стоимости пути. Условлено, что стоимость пути рассчитывается по формуле «1000/скорость передачи данных локальной сети» (Мбит/с).

Войдите в привилегированный режим EXEC и выполните следующие действия для назначения стоимости пути.

СВОДКА ШАГОВ

1. **configure terminal**
2. **interface** *interface-id*
3. **bridge-group** *bridge-group* **path-cost** *cost*
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

ПОДРОБНОЕ ОПИСАНИЕ ШАГОВ

	Команда	Назначение
Шаг 1	**configure terminal**	Вход в режим глобальной конфигурации.

Шаг 2	**interface** *interface-id*	Вход в режим настройки интерфейса и указание интерфейса, для которого необходимо задать стоимость пути.
Шаг 3	**bridge-group** *bridge-group* **path-cost** *cost*	Назначение стоимости пути для интерфейса. • Для параметра *bridge-group* укажите номер группы моста. Диапазон значений составляет от 1 до 255. • Для параметра *cost* введите значение от 1 до 65536. Чем больше значение, тем выше стоимость. – Для сети со скоростью передачи данных 10 Мбит/с значение стоимости пути по умолчанию — 100. – Для сети со скоростью передачи данных 100 Мбит/с значение стоимости пути по умолчанию — 19. – Для сети со скоростью передачи данных 1000 Мбит/с значение стоимости пути по умолчанию — 4.
Шаг 4	**end**	Возврат к привилегированному режиму EXEC.
Шаг 5	**show running-config**	Проверка введенных пользователем данных.
Шаг 6	**copy running-config startup-config**	Сохранение записей в файл конфигурации (необязательно).

Для возврата к значению стоимости пути по умолчанию используйте команду **no bridge-group** *bridge-group* **path-cost** *cost* в режиме настройки интерфейса.

Настройка интервалов BPDU

Интервалы BPDU можно изменять, как описано в следующих разделах.

- Изменение интервала между пакетами Hello BPDU
- Изменение интервала задержки пересылки
- Изменение максимального интервала простоя

Примечание. Каждый коммутатор протокола Spanning Tree имеет интервал между BPDU приветствия, интервал задержки пересылки и максимальный интервал простоя корневого коммутатора независимо от настройки собственных параметров.

Изменение интервала между пакетами Hello BPDU

Войдите в привилегированный режим EXEC и выполните следующие действия для изменения BPDU приветствия.

СВОДКА ШАГОВ

1. **configure terminal**
2. **bridge** *bridge-group* **hello-time** *seconds*
3. **end**
4. **show running-config**
5. **copy running-config startup-config**

ПОДРОБНОЕ ОПИСАНИЕ ШАГОВ

	Команда	Назначение
Шаг 1	**configure terminal**	Вход в режим глобальной конфигурации.
Шаг 2	**bridge** *bridge-group* **hello-time** *seconds*	Задание интервала между BPDU приветствия. • Для параметра *bridge-group* укажите номер группы моста. Диапазон значений составляет от 1 до 255. • Для параметра *seconds* введите значение от 1 до 10. Значение по умолчанию — 2 секунд.
Шаг 3	**end**	Возврат к привилегированному режиму EXEC.
Шаг 4	**show running-config**	Проверка введенных пользователем данных.
Шаг 5	**copy running-config startup-config**	Сохранение записей в файл конфигурации (необязательно).

Для возврата к значению по умолчанию используйте команду **no bridge** *bridge-group* **hello-time** в режиме глобальной конфигурации.

Изменение интервала задержки пересылки

Интервал задержки пересылки — это время, затрачиваемое на прослушивание информации об изменении топологии после активации интерфейса для коммутации и перед началом фактической пересылки.

Войдите в привилегированный режим EXEC и выполните следующие действия для изменения интервала задержки пересылки.

СВОДКА ШАГОВ

1. **configure terminal**
2. **bridge** *bridge-group* **forward-time** *seconds*
3. **end**
4. **show running-config**
5. **copy running-config startup-config**

ПОДРОБНОЕ ОПИСАНИЕ ШАГОВ

	Команда	Назначение
Шаг 1	**configure terminal**	Вход в режим глобальной конфигурации.
Шаг 2	**bridge** *bridge-group* **forward-time** *seconds*	Задание интервала задержки пересылки. • Для параметра *bridge-group* укажите номер группы моста. Диапазон значений составляет от 1 до 255. • Для параметра *seconds* введите значение от 10 до 200. Значение по умолчанию — 20 секунд.
Шаг 3	**end**	Возврат к привилегированному режиму EXEC.
Шаг 4	**show running-config**	Проверка введенных пользователем данных.
Шаг 5	**copy running-config startup-config**	Сохранение записей в файл конфигурации (необязательно).

Для возврата к значению по умолчанию используйте команду **no bridge** *bridge-group* **forward-time** *seconds* в режиме глобальной конфигурации.

Изменение максимального интервала простоя

Если коммутатор не получает BPDU от корневого коммутатора в течение заданного временного интервала, он рассчитывает топологию Spanning Tree повторно.

Войдите в привилегированный режим EXEC и выполните следующие действия для изменения максимального интервала простоя (максимального времени устаревания).

СВОДКА ШАГОВ

1. **configure terminal**

2. **bridge** *bridge-group* **max-age** *seconds*

3. **end**

4. **show running-config**

5. **copy running-config startup-config**

ПОДРОБНОЕ ОПИСАНИЕ ШАГОВ

	Команда	Назначение
Шаг 1	**configure terminal**	Вход в режим глобальной конфигурации.
Шаг 2	**bridge** *bridge-group* **max-age** *seconds*	Задание интервала ожидания коммутатором BPDU от корневого коммутатора. • Для параметра *bridge-group* укажите номер группы моста. Диапазон значений составляет от 1 до 255. • Для параметра *seconds* введите значение от 10 до 200. Значение по умолчанию — 30 секунд.
Шаг 3	**end**	Возврат к привилегированному режиму EXEC.
Шаг 4	**show running-config**	Проверка введенных пользователем данных.
Шаг 5	**copy running-config startup-config**	Сохранение записей в файл конфигурации (необязательно).

Для возврата к значению по умолчанию используйте команду **no bridge** *bridge-group* **max-age** в режиме глобальной конфигурации.

Отключение протокола Spanning Tree на интерфейсе

Если между двумя коммутируемыми подсетями существует путь без зацикливания, можно предотвратить воздействие BPDU, созданных в одной из коммутируемых подсетей, на устройства в другой коммутируемой подсети, поддерживая одновременно с этим коммутацию во всей сети целиком. Если, например, коммутируемые подсети локальной сети разделены посредством сети WAN, можно запретить прохождение BPDU по каналу сети WAN.

Войдите в привилегированный режим EXEC и выполните следующие действия для отключения протокола Spanning Tree на интерфейсе.

СВОДКА ШАГОВ

1. **configure terminal**

2. **interface** *interface-id*

3. **bridge-group** *bridge-group* **spanning-disabled**

4. **end**

5. **show running-config**

6. **copy running-config startup-config**

ПОДРОБНОЕ ОПИСАНИЕ ШАГОВ

	Команда	Назначение
Шаг 1	**configure terminal**	Вход в режим глобальной конфигурации.
Шаг 2	**interface** *interface-id*	Вход в режим настройки интерфейса и задание идентификатора интерфейса.
Шаг 3	**bridge-group** *bridge-group* **spanning-disabled**	Отключение протокола Spanning Tree на интерфейсе. Для параметра *bridge-group* укажите номер группы моста. Диапазон значений составляет от 1 до 255.
Шаг 4	**end**	Возврат к привилегированному режиму EXEC.
Шаг 5	**show running-config**	Проверка введенных пользователем данных.
Шаг 6	**copy running-config startup-config**	Сохранение записей в файл конфигурации (необязательно).

Для повторного включения протокола Spanning Tree на интерфейсе используйте команду **no bridge-group** *bridge-group* **spanning-disabled** в режиме настройки интерфейса.

Мониторинг и обслуживание сети

Для выполнения мониторинга и обслуживания сети войдите в привилегированный режим EXEC и используйте следующие команды.

Команда	Назначение
clear bridge *bridge-group*	Удаление всех полученных в ходе обучения записей из базы данных пересылки и сброс счетчиков приема и отправки для всех статически

	настроенных записей.
show bridge [*bridge-group*]	Отображение подробной информации о группе моста.
show bridge [*bridge-group*] [*interface-id*] [*address*] [**group**] [**verbose**]	Отображение классов записей в базе данных пересылки моста.

Настройка отдельных подсетей для голоса и данных

Для упрощения администрирования сети и повышенной масштабируемости администраторы сети могут настраивать интерфейсные платы EtherSwitch HWIC для поддержки IP-телефонов Cisco таким образом, чтобы голос и данные хранились в разных подсетях. При наличии возможности сегментации существующего пространства IP-адресов филиала предприятия следует всегда использовать отдельные сети VLAN.

Для реализации приоритета в коммутаторах Ethernet используются биты приоритета части 802.1p заголовка стандарта 802.1Q. Это важнейший компонент при создании сетей Cisco AVVID.

Интерфейсная плата EtherSwitch HWIC используется для реализации производительности и интеллектуальных служб Cisco IOS для приложений филиала предприятия. Интерфейсная плата EtherSwitch HWIC может определять задействованные пользователем приложения, например использование голосовых служб или мультиадресной передачи видео, и соответствующим образом классифицировать трафик с надлежащим уровнем приоритета.

Примечание. Дополнительную информацию по использованию службы QoS для связи конечных точек при развертывании решений Cisco AVVID см. в документе *Руководство по проектированию Cisco AVVID с использованием QoS*.

Войдите в режим глобальной конфигурации и выполните следующие действия для автоматической настройки IP-телефонов Cisco на отправку голосового трафика по идентификатору сети VLAN (VVID) на каждом порте (см. раздел «Голосовой трафик и VVID»).

СВОДКА ШАГОВ

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **switchport mode trunk**
5. **switchport voice vlan** vlan-id

ПОДРОБНОЕ ОПИСАНИЕ ШАГОВ

	Команда	Назначение
Шаг 1	Router(config)# **enable**	Вход в привилегированный режим EXEC. Для входа в этот режим

		может потребоваться ввести заранее установленный пароль.
Шаг 2	Router(config)# **configure terminal**	Вход в режим глобальной конфигурации.
Шаг 3	`300 VLAN0300 active` **interface** *interface-id*	Вход в режим настройки интерфейса и выбор порта, который необходимо настроить (например, interface fa0/3/1).
Шаг 4	Router(config-if)# **switchport mode trunk**	Включение магистрального режима для порта.
Шаг 5	Router(config-if)# **switchport voice vlan** vlan-id	Настройка голосового порта с идентификатором VVID, который будет использоваться только для голосового трафика.

Голосовой трафик и VVID

Интерфейсная плата EtherSwitch HWIC может настраивать голосовую сеть VLAN в автоматическом режиме. Эта функция позволяет устранить трудоемкую процедуру наложения голосовой топологии на сеть передачи данных с сохранением качества голосового трафика. Функция автоматической настройки голосовой сети VLAN дает возможность администраторам сети сегментировать телефоны в отдельные логические сети, используя единую физическую инфраструктуру для передачи данных и голоса. Функция голосовой сети VLAN размещает телефоны в собственных сетях VLAN, устраняя необходимость вмешательства со стороны конечного пользователя. Пользователь может подключить телефон к коммутатору, после чего коммутатор передает на телефон всю необходимую информацию о сети VLAN.

Настройка одной подсети для голоса и данных

В сетях, топология которых предусматривает постепенное развитие IP-телефонии, сетевые администраторы могут настроить интерфейсную плату EtherSwitch HWIC таким образом, что трафик голоса и данных будет проходить через одну подсеть. Это необходимо в тех случаях, когда выделение дополнительной IP-подсети для IP-телефонов или разделение существующего пространства IP-адресов для образования дополнительной подсети в удаленном филиале является неудобным способом, поскольку для всех филиалов необходимо использовать единое пространство IP-адресов. Описанный путь является более простым способом развертывания IP-телефонии.

Данный способ настройки должен отвечать двум основным требованиям.

- Сетевые администраторы должны обеспечить достаточное количество уникальных IP-адресов для новых IP-телефонов Cisco в уже существующих подсетях.

- Администрирование сети, в одной подсети которой используются как IP-телефоны, так и рабочие станции, может стать достаточно трудной задачей.

Войдите в привилегированный режим EXEC и выполните следующие действия для автоматической настройки IP-телефонов Cisco на отправку голосового трафика и данных через одну сеть VLAN.

СВОДКА ШАГОВ

1. **configure terminal**

2. **interface** *interface-id*

3. **switchport access vlan** vlan-id

4. end

ПОДРОБНОЕ ОПИСАНИЕ ШАГОВ

	Команда	Назначение
Шаг 1	Router# **configure terminal**	Вход в режим глобальной конфигурации.
Шаг 2	`1002 fddi-default active` **interface** *interface-id*	Вход в режим настройки интерфейса и выбор порта, который необходимо настроить (например, interface fa0/1/1).
Шаг 3	`1003 token-ring-default active` **switchport access vlan** vlan-id	Использование исходной сети VLAN для непомеченного трафика. Значение параметра *vlan-id* — это идентификатор сети VLAN, которая используется для приема и отправки непомеченного трафика на данном порте. Диапазон действительных идентификаторов составляет от 1 до 1001. Использование начальных нулей недопустимо.
Шаг 4	Router# **end**	Возврат к привилегированному режиму EXEC.

Проверка настроек коммутируемого порта

Для проверки настроек коммутируемого порта используйте команду **show run interface**.

```
Router# show run interface interface-id
```

Для сохранения текущих настроек во флэш-памяти используйте команду **write memory**.

```
Router# write memory
```

Управление интерфейсными платами EtherSwitch HWIC

В данном разделе приведена информация по выполнению основных задач управления интерфейсными платами EtherSwitch HWIC посредством интерфейса командной строки Cisco IOS. Данная информация может быть полезной при настройке коммутатора с использованием сценариев, описанных ранее.

В разделе описываются следующие темы.

- Добавление диспетчеров асинхронных прерываний
- Настройка информации IP-адресации
- Включение анализатора коммутируемых портов

- Управление таблицей ARP
- Управление таблицами MAC-адресов
- Удаление динамических адресов
- Добавление безопасных адресов
- Настройка статических адресов
- Очистка всех таблиц MAC-адресов

Добавление диспетчеров асинхронных прерываний

Диспетчер асинхронных прерываний — это станция управления, которая получает и обрабатывает асинхронные прерывания. При настройке диспетчера асинхронных прерываний строки сообществ для каждого рядового коммутатора должны быть уникальными. Если рядовому коммутатору назначен IP-адрес, станция управления получает доступ к коммутатору посредством использования этого адреса.

По умолчанию диспетчер асинхронных прерываний не назначен, а асинхронные прерывания не отправляются.

Войдите в привилегированный режим EXEC и выполните следующие действия для добавления диспетчера асинхронных прерываний и строки сообщества.

СВОДКА ШАГОВ

1. **configure terminal**
2. **snmp-server host 172.2.128.263** *traps1* **snmp vlan-membership**
3. **end**

ПОДРОБНОЕ ОПИСАНИЕ ШАГОВ

	Команда	Назначение
Шаг 1	Router# **configure terminal**	Вход в режим глобальной конфигурации.
Шаг 2	Router(config)# **snmp-server host 172.2.128.263** *traps1* **snmp vlan-membership**	Ввод IP-адреса, строки сообщества и асинхронных прерываний для диспетчера асинхронных прерываний.
Шаг 3	Router(config)# **end**	Возврат к привилегированному режиму EXEC.

Проверка диспетчеров асинхронных прерываний

Для отображения текущих настроек с целью проверки корректности введенных данных используйте команду **show running-**

config.

Router# **show running-config**

Настройка информации IP-адресации

В данном разделе приведено описание назначения информации IP-адресации на интерфейсной плате EtherSwitch HWIC. В разделе описываются следующие темы.

- Назначение информации IP-адресации коммутатору
- Задание имени домена и настройка DNS

Назначение информации IP-адресации коммутатору

Для автоматического назначения информации IP-адресации коммутатору можно использовать сервер BOOTP; однако сервер BOOTP должен быть развернут заранее и иметь базу данных физических MAC-адресов и соответствующих IP-адресов, масок подсетей и адресов шлюзов по умолчанию. Кроме того, коммутатор должен иметь возможность доступа к серверу BOOTP через один из собственных портов. При запуске коммутатор без назначенного IP-адреса запрашивает нужную информацию у сервера BOOTP; запрашиваемая информация сохраняется в файле конфигурации коммутатора. Для гарантированного сохранения информации об IP-адресации после перезапуска коммутатора необходимо сохранить настройки с использованием команды **write memory** в привилегированном режиме EXEC.

Можно изменять содержимое следующих полей. Маска определяет биты, которые указывают на номер сети в IP-адресе. При использовании маски для выделения подсети маска называется «маской подсети». Широковещательный адрес резервируется для отправки сообщений всем узлам сети. ЦП отправляет трафик на незнакомый IP-адрес через шлюз по умолчанию.

Войдите в привилегированный режим EXEC и выполните следующие действия для ввода информации IP-адресации.

СВОДКА ШАГОВ

1. **configure terminal**
2. **interface vlan 1**
3. **ip address** ip-address subnet-mask
4. **exit**
5. **ip default-gateway** ip-address
6. **end**

ПОДРОБНОЕ ОПИСАНИЕ ШАГОВ

	Команда	Назначение
Шаг 1	Router# **configure terminal**	Вход в режим глобальной конфигурации.
Шаг 2	Router(config)# **interface vlan**	Вход в режим настройки интерфейса и указание сети VLAN,

	1	которой назначается информация IP-адресации. Сеть VLAN 1 является административной сетью VLAN, однако можно указать идентификатор в диапазоне от 1 до 1001.
Шаг 3	Router(config)# **ip address** ip-address subnet-mask	Ввод IP-адреса и маски подсети.
Шаг 4	Router(config)# **exit**	Возврат в режим глобальной конфигурации.
Шаг 5	Router# **ip default-gateway** ip-address	Ввод IP-адреса маршрутизатора по умолчанию.
Шаг 6	Router# **end**	Возврат к привилегированному режиму EXEC.

Для удаления из настроек коммутатора информации об IP-адресации используйте следующую процедуру.

Примечание. После использования команды **no ip address** в режиме настройки стек протокола IP отключается, а информация об IP-адресации удаляется. Членам кластера без IP-адресов необходимо, чтобы стек протокола IP был включен.

Войдите в режим глобальной конфигурации и выполните следующие действия для удаления IP-адреса.

СВОДКА ШАГОВ

1. **interface vlan 1**
2. **no ip address**
3. **end**

ПОДРОБНОЕ ОПИСАНИЕ ШАГОВ

	Команда	Назначение
Шаг 1	Router(config)# **interface vlan 1**	Вход в режим настройки интерфейса и указание сети VLAN, которой назначается информация IP-адресации. Сеть VLAN 1 является административной сетью VLAN, однако можно указать идентификатор в диапазоне от 1 до 1001.
Шаг 2	Router(config-subif)# **no ip address**	Удаление IP-адреса и маски подсети.
Шаг 3	Router(config-subif)# **end**	Возврат к привилегированному режиму EXEC.

⚠

Внимание При удалении IP-адреса посредством сеанса Telnet соединение с коммутатором будет потеряно.

Задание имени домена и настройка DNS

С каждым уникальным IP-адресом связано имя узла сети. Программное обеспечение Cisco IOS поддерживает режим EC и соответствующие операции для сеансов Telnet. Наличие этого кэша ускоряет процесс преобразования имен в адреса.

IP-адрес определяет иерархическую схему именования, которая позволяет идентифицировать устройство по его расположению или домену. Имена доменов составляются с использованием символа «точка» (.) и символов-разделителей. Например, Cisco Systems — это коммерческая организация, IP-адрес которой определяется именем домена *com*, поэтому имя домена компании — *cisco.com*. Конкретное устройство в домене, например, FTP-сервер, может быть идентифицировано как *ftp.cisco.com*.

Для отслеживания имен доменов протоколом IP используется служба DNS, в задачи которой входит хранение кэша (базы данных) имен, связанных с IP-адресами. Для связи имен домена с IP-адресами сначала необходимо определить имена узлов сети, затем указать DNS-сервер и включить службу DNS — глобальную систему наименования узлов в Интернете, позволяющую присваивать сетевым устройствам уникальные идентификаторы.

Задание имени домена

Можно задать имя домена по умолчанию, которое будет использоваться программным обеспечением для выполнения запросов имени домена. Можно задать одно имя домена или список имен. При задании имени домена перед добавлением в таблицу сетевых узлов это имя добавляется ко всем именам IP-узлов, не имеющих имени домена.

Задание DNS-сервера

Выполнять функцию DNS-сервера могут до шести узлов, которые будут предоставлять информацию об именах службе DNS.

Включение службы DNS

Если устройствам в вашей сети необходимо устанавливать соединения с устройствами в сетях, в которых управление назначением имен для вас невозможно, можно назначить для устройств собственной сети уникальные имена, которые будут использоваться для идентификации устройств во всей сети Интернет. Эта функция выполняется службой DNS — глобальной системой наименования узлов в Интернете. Эта служба включена по умолчанию.

Включение анализатора коммутируемых портов

Можно отслеживать трафик на определенном порте посредством пересылки входящего и исходящего трафика на другой порт в этой же сети VLAN. Порт анализатора коммутируемых портов (SPAN) не может использоваться для мониторинга портов из другой сети VLAN, и должен быть назначен как порт статического доступа. В качестве портов SPAN можно назначить любое количество портов, при этом возможно проводить мониторинг любого сочетания портов. Функция SPAN поддерживается максимум для 2 сеансов.

Войдите в привилегированный режим EXEC и выполните следующие действия для включения функции SPAN.

СВОДКА ШАГОВ

1. **configure terminal**

2. **monitor session** session-id {**destination** | **source**} {**interface** | **vlan** interface-id | vlan-id}} [**,** | **-** | **both** | **tx** | **rx**]

3. **end**

ПОДРОБНОЕ ОПИСАНИЕ ШАГОВ

	Команда	Назначение
Шаг 1	Router# **configure terminal**	Вход в режим глобальной конфигурации.
Шаг 2	`1004 fddinet-default active` **monitor session** session-id {**destination** | **source**} {**interface** | **vlan** interface-id | vlan-id}} **[,** | **-** | both | tx | rx]	Включение мониторинга портов для заданного сеанса («*number*»). Дополнительно можно также указать интерфейса назначения SPAN *destination* и интерфейс источника *source*.
Шаг 3	Router(config)# **end**	Возврат к привилегированному режиму EXEC.

Войдите в привилегированный режим EXEC и выполните следующие действия для отключения функции SPAN.

СВОДКА ШАГОВ

1. **configure terminal**
2. **no monitor session** session-id
3. **end**

ПОДРОБНОЕ ОПИСАНИЕ ШАГОВ

	Команда	Назначение
Шаг 1	Router# **configure terminal**	Вход в режим глобальной конфигурации.
Шаг 2	Router(config)# **no monitor session** session-id	Отключение мониторинга портов для заданного сеанса.
Шаг 3	Router(config)# **end**	Возврат к привилегированному режиму EXEC.

Управление таблицей ARP

Для установки связи с устройством (например, через интерфейс Ethernet) программное обеспечение сначала определяет 48-битный MAC-адрес или адрес локального канала передачи данных этого устройства. Процесс определения адреса локального канала передачи данных через IP-адрес называется *разрешением адресов*.

Протокол разрешения адресов (Address Resolution Protocol, ARP) используется для связи IP-адреса узла сети с соответствующей средой или MAC-адресом и идентификатором сети VLAN. Используя в качестве входных данных IP-

адрес, протокол ARP определяет связанный с ним MAC-адрес. После определения MAC-адреса соответствие «IP-адрес — MAC-адрес» сохраняется в кэше протокола ARP для быстрого извлечения в дальнейшем. Затем IP-датаграмма инкапсулируется в кадр канального уровня и передается по сети. Инкапсуляция IP-датаграмм, запросов ARP и ответов на запросы в сетях IEEE 802 (помимо Ethernet) определяются протоколом доступа к подсетям (Subnetwork Access Protocol, SNAP). По умолчанию стандартная инкапсуляция ARP для Ethernet (обозначается ключевым словом **arpa**) включена на IP-интерфейсе.

При добавлении в таблицу ARP записей вручную посредством интерфейса командной строки необходимо помнить, что эти записи не устаревают, и их необходимо удалять вручную.

Управление таблицами MAC-адресов

В данном разделе приведено описание управления таблицами MAC-адресов на интерфейсной плате EtherSwitch HWIC. В разделе описываются следующие темы.

- Понятие MAC-адресов и сетей VLAN
- Изменение времени устаревания адреса
- Настройка времени устаревания
- Проверка настройки времени устаревания

Для пересылки трафика между портами коммутатор использует таблицы MAC-адресов. Каждый MAC-адрес в таблице адресов связан с одним или несколькими портами. Таблицы MAC-адресов содержат адреса следующих типов:

- динамический адрес — исходный MAC-адрес, получаемый коммутатором и отбрасываемый на то время, когда адрес не используется;
- безопасный адрес — вводимый вручную индивидуальный адрес, связанный с безопасным портом. Безопасные адреса не устаревают.
- статический адрес — вводимый вручную индивидуальный или групповой адрес, который не устаревает и остается действительным даже при перезагрузке коммутатора.

В таблице адресов указывается MAC-адрес назначения, а также идентификатор сети VLAN, модуль и номер порта, связанный с адресом. Ниже приведен пример списка адресов, выводимого в таблице динамических, безопасных или статических адресов.

```
Router# show mac-address-table



Destination Address  Address Type  VLAN  Destination Port

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

000a.000b.000c          Secure      1      FastEthernet0/1/8

000d.e105.cc70          Self        1      Vlan1

00aa.00bb.00cc          Static      1      FastEthernet0/1/0
```

Понятие MAC-адресов и сетей VLAN

Все адреса связаны с определенной сетью VLAN. Адрес может существовать в нескольких сетях VLAN и обозначать различные узлы в каждой из них. Групповые адреса, к примеру, могут пересылаться на порт 1 в сети VLAN 1 и на порты 9, 10 и 11 в сети VLAN 5.

В каждой сети VLAN создается собственная таблица логических адресов. Известный в одной сети VLAN адрес является неизвестным в другой сети до тех пор, пока информация о нем не будет получена или он не будет статическим связанным с портом во второй сети VLAN. Адрес может использоваться как безопасный в одной сети VLAN и как динамический в другой. Адреса, вводимые в одной сети VLAN как статические, должны быть статическими во всех других сетях VLAN.

Изменение времени устаревания адреса

Динамические адреса — это исходные MAC-адреса, получаемые коммутатором и отбрасываемые на то время, когда они не используется. Для задания временного интервала, в течение которого коммутатор сохраняет в таблице невидимые адреса, используйте поле Aging Time (Время устаревания). Этот параметр применяется ко всем сетям VLAN.

Настройка времени устаревания

В случае задания слишком короткого интервала времени устаревания адреса могут быть преждевременно удалены из таблицы. Если впоследствии коммутатор получит пакет с неизвестным конечным адресом, он будет лавинно передавать его на все порты сети VLAN, которой принадлежит порт-получатель. Этот ненужный лавинный трафик может снизить быстродействие сети. В случае задания слишком длинного интервала времени устаревания таблица адресов может переполниться неиспользуемыми адресами. Это может вызывать задержки при установке соединения в случае переключения рабочей станции на другой порт.

Войдите в режим глобальной конфигурации и выполните следующие действия для настройки времени устаревания таблицы динамических адресов.

СВОДКА ШАГОВ

1. **configure terminal**
2. **mac-address-table aging-time** seconds
3. **end**

ПОДРОБНОЕ ОПИСАНИЕ ШАГОВ

	Команда	Назначение
Шаг 1	Router(config)# **configure terminal**	Вход в режим глобальной конфигурации.
Шаг 2	Router(config)# **mac-address-table aging-time** seconds	Ввод времени в секундах, в течение которого динамические адреса будут храниться в таблице адресов. Допускаются значения от 10 до 1 000 000.
Шаг 3	Router(config)# **end**	Возврат к привилегированному режиму EXEC.

Проверка настройки времени устаревания

Для проверки настройки используйте команду **show mac-address-table aging-time**.

Router# **show mac-address-table aging-time**

Удаление динамических адресов

Войдите в привилегированный режим EXEC и выполните следующие действия для удаления записи из таблицы динамических адресов.

СВОДКА ШАГОВ

1. **configure terminal**
2. **no mac-address-table dynamic** hw-addr
3. **end**

ПОДРОБНОЕ ОПИСАНИЕ ШАГОВ

	Команда	Назначение
Шаг 1	Router# **configure terminal**	Вход в режим глобальной конфигурации.
Шаг 2	Router(config)# **no mac-address-table dynamic** hw-addr	Ввод MAC-адреса, который необходимо удалить из таблицы динамических MAC-адресов.
Шаг 3	Router(config)# **end**	Возврат к привилегированному режиму EXEC.

Можно удалить все записи динамических адресов посредством команды **clear mac-address-table dynamic** в привилегированном режиме EXEC.

Проверка динамических адресов

Для проверки настройки используйте команду **show mac-address-table dynamic**.

```
Router# show mac-address-table dynamic
```

Добавление безопасных адресов

В таблице безопасных адресов хранятся безопасные MAC-адреса, связанные с ними номера портов и идентификаторы сетей VLAN. Безопасный адрес — это вводимый вручную индивидуальный адрес, пересылаемый только на один порт в сети VLAN. При вводе адреса, уже назначенного другому порту, коммутатор переназначает безопасный адрес новому порту.

Порту можно назначать безопасный адрес даже в том случае, когда порт еще не принадлежит сети VLAN. Если впоследствии порт будет назначен какой-либо сети VLAN, пакеты, направленные на этот адрес, будут пересылаться на этот порт.

Войдите в привилегированный режим EXEC и выполните следующие действия для добавления безопасного адреса.

СВОДКА ШАГОВ

1. **configure terminal**
2. **mac-address-table secure address** hw-addr **interface** interface-id **vlan** vlan-id
3. **end**

ПОДРОБНОЕ ОПИСАНИЕ ШАГОВ

	Команда	Назначение
Шаг 1	Router# **configure terminal**	Вход в режим глобальной конфигурации.
Шаг 2	`1005 trnet-default active` **mac-address-table secure address** hw-addr **interface** interface-id **vlan** vlan-id	Ввод MAC-адреса, связанного с ним номера порта и идентификатора сети VLAN.
Шаг 3	Router(config)# **end**	Возврат к привилегированному режиму EXEC.

Войдите в привилегированный режим EXEC и выполните следующие действия для удаления безопасного адреса.

СВОДКА ШАГОВ

1. **configure terminal**
2. **no mac-address-table secure** hw-addr **vlan** vlan-id
3. **end**

ПОДРОБНОЕ ОПИСАНИЕ ШАГОВ

	Команда	Назначение
Шаг 1	Router# **configure terminal**	Вход в режим глобальной конфигурации.
Шаг 2	`Router#` **no mac-address-table secure** hw-addr **vlan** vlan-id	Ввод MAC-адреса, связанного с ним номера порта и идентификатора сети VLAN, которые необходимо удалить.
Шаг 3	Router(config)# **end**	Возврат к привилегированному режиму EXEC.

Можно удалить все записи безопасных адресов посредством команды **clear mac-address-table secure** в привилегированном режиме EXEC.

Проверка безопасных адресов

Для проверки настройки используйте команду **show mac-address-table secure**.

```
Router# show mac-address-table secure
```

Настройка статических адресов

Статический адрес характеризуется следующими свойствами.

- Его необходимо вручную добавлять и удалять из таблицы адресов.
- Статический адрес может быть как индивидуальным, так и групповым.
- Он не имеет времени устаревания и сохраняется после перезагрузки коммутатора.

Поскольку все порты связаны, по меньшей мере, с одной сетью VLAN, коммутатор получает идентификатор сети VLAN для адреса из портов, выбираемых пользователем в карте пересылки. Если адрес является статическим в одной сети VLAN, он должен быть статическим во всех других сетях VLAN. Пакет со статическим адресом, получаемый сетью VLAN, в которой адрес не указан как статический, лавинно передается на все порты и не запоминается.

Войдите в привилегированный режим EXEC и выполните следующие действия для добавления статического адреса.

СВОДКА ШАГОВ

1. **configure terminal**
2. **mac-address-table static** hw-addr [**interface**] interface-id [**vlan**] vlan-id
3. **end**

ПОДРОБНОЕ ОПИСАНИЕ ШАГОВ

	Команда	Назначение
Шаг 1	`Router#`**configure terminal**	Вход в режим глобальной конфигурации.
Шаг 2	`Router(config)#`**mac-address-table static** hw-addr [**interface**] interface-id [**vlan**] vlan-id	Ввод статического MAC-адреса, интерфейса и идентификатора сети VLAN для указанных портов.
Шаг 3	Router(config)# **end**	Возврат к привилегированному режиму EXEC.

Войдите в привилегированный режим EXEC и выполните следующие действия для удаления статического адреса.

СВОДКА ШАГОВ

1. **configure terminal**

2. **no mac-address-table static** hw-addr [**interface**] interface-id [**vlan**] vlan-id

3. **end**

ПОДРОБНОЕ ОПИСАНИЕ ШАГОВ

:

	Команда	Назначение
Шаг 1	Router# **configure terminal**	Вход в режим глобальной конфигурации.
Шаг 2	`FastEthernet0/1/0 is up, line protocol is up` **no mac-address-table static** hw-addr [**interface**] interface-id [**vlan**] vlan-id	Ввод статического MAC-адреса, интерфейса и идентификатора сети VLAN для портов, которые необходимо удалить.
Шаг 3	Router(config)# **end**	Возврат к привилегированному режиму EXEC.

Можно удалить все записи статических адресов посредством команды **clear mac-address-table static** в привилегированном режиме EXEC.

Проверка статических адресов

Для проверки настройки используйте команду **show mac-address-table static**.

```
Router # show mac-address-table static

Static Address Table

Destination Address  Address Type  VLAN  Destination Port

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

000a.000b.000c          Static        1     FastEthernet0/1/0
```

Очистка всех таблиц MAC-адресов

Для удаления всех адресов используйте команду **clear mac-address** в привилегированном режиме EXEC.

Команда	Назначение
Router# **clear mac-address-table**	Удаление всех данных из таблиц MAC-адресов.

Примеры конфигурации для интерфейсных плат EtherSwitch HWIC

В этом разделе приведены следующие примеры конфигурации.

- Диапазон интерфейса: примеры
- Дополнительные характеристики интерфейса: примеры
- Стеки: примеры
- Настройка сети VLAN: пример
- Транкинг сети VLAN с использованием протокола VTP: пример
- Протокол Spanning Tree: примеры
- Обработка таблицы MAC-адресов: пример
- Источник анализатора коммутируемых портов (SPAN): примеры
- Функция IGMP Snooping: пример
- Контроль шторма: пример
- Коммутация Ethernet: примеры

Диапазон интерфейса: примеры

- Пример настройки одиночного диапазона
- Пример задания макроса диапазона

Пример настройки одиночного диапазона

В следующем примере показано включение всех интерфейсов Fast Ethernet интерфейсной платы HWIC-4ESW, установленной в слот 2.

```
Router(config)#int range fastEthernet 0/3/0 - 8

Router(config-if-range)#no shut

Router(config-if-range)#

*Mar  21 14:01:21.474: %LINK-3-UPDOWN: Interface FastEthernet0/3/0, changed state to up

*Mar  21 14:01:21.490: %LINK-3-UPDOWN: Interface FastEthernet0/3/1, changed state to up

*Mar  21 14:01:21.502: %LINK-3-UPDOWN: Interface FastEthernet0/3/2, changed state to up
```

```
*Mar  21 14:01:21.518: %LINK-3-UPDOWN: Interface FastEthernet0/3/3, changed state to up

*Mar  21 14:01:21.534: %LINK-3-UPDOWN: Interface FastEthernet0/3/4, changed state to up

*Mar  21 14:01:21.546: %LINK-3-UPDOWN: Interface FastEthernet0/3/5, changed state to up

*Mar  21 14:01:21.562: %LINK-3-UPDOWN: Interface FastEthernet0/3/6, changed state to up

*Mar  21 14:01:21.574: %LINK-3-UPDOWN: Interface FastEthernet0/3/7, changed state to up

*Mar  21 14:01:21.590: %LINK-3-UPDOWN: Interface FastEthernet0/3/8, changed state to up

Router(config-if-range)#
```

Пример задания макроса диапазона

В следующем примере показано создание макроса для указания диапазона интерфейсов под именем «enet_list» для выбора интерфейсов Fast Ethernet с 0/1/0 по 0/1/3.

```
Router(config)#define interface-range enet_list fastethernet 0/1/0 - 0/1/3



Router(config)#
```

В следующем примере показан способ изменения режима настройки диапазона интерфейсов с использованием макроса «enet_list».

```
Router(config)#interface range macro enet_list
```

Дополнительные характеристики интерфейса: примеры

- Пример настройки скорости интерфейса
- Пример настройки дуплексного режима интерфейса
- Пример добавления описания к интерфейсу

Пример настройки скорости интерфейса

В следующем примере показано изменение скорости интерфейса Fast Ethernet 0/3/7 на 100 Мбит/с.

```
Router(config)#interface fastethernet 0/3/7



Router(config-if)# speed 100
```

Пример настройки дуплексного режима интерфейса

В следующем примере показана установка для интерфейса Fast Ethernet 0/3/7 дуплексного режима.

```
Router(config)#interface fastethernet 0/3/7
```

```
Router(config-if)#duplex full
```

Пример добавления описания к интерфейсу

В следующем примере показано добавление к интерфейсу Fast Ethernet 0/3/7 описания.

```
Router(config)#interface fastethernet 0/3/7
```

```
Router(config-if)#description Link to root switch
```

Стеки: примеры

В следующем примере показана установка в стек двух интерфейсных плат.

```
Router(config)#interface FastEthernet 0/1/8
```

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

```
Router(config-if)#switchport stacking-partner interface FastEthernet 0/3/8
```

```
Router(config-if)#interface FastEthernet 0/3/8
```

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

Примечание. На практике команду **switchport stacking-partner interface FastEthernet** *0/partner-slot/partner-port* необходимо вводить только для одного из портов, используемых для работы в стеке. Второй порт будет автоматически настроен программным обеспечением Cisco IOS для работы в стеке. Команду **no shutdown**, с другой стороны, необходимо вводить для обоих портов, использующихся для работы в стеке.

Настройка сети VLAN: пример

В следующем примере показана настройка маршрутизации между сетями VLAN.

```
Router#vlan database
```

```
Router(vlan)#vlan 1
```

```
Router(vlan)#vlan 2
```

```
Router(vlan)#exit
```

```
Router#configure terminal
```

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

```
Router(config-if)#ip address 1.1.1.1 255.255.255.0
```

```
Router(config-if)#no shut

Router(config-if)#interface vlan 2

Roouter(config-if)#ip address 2.2.2.2 255.255.255.0

Router(config-if)#no shut

Router(config-if)#interface FastEthernet 0/1/0

Router(config-if)#switchport access vlan 1

Router(config-if)#interface Fast Ethernet 0/1/1

Router(config-if)#switchport access vlan 2

Router(config-if)#exit
```

Транкинг сети VLAN с использованием протокола VTP: пример

В следующем примере показана настройка коммутатора в качестве VTP-сервера.

```
Router# vlan database

Router(vlan)# vtp server

Setting device to VTP SERVER mode.

Router(vlan)# vtp domain Lab_Network

Setting VTP domain name to Lab_Network

Router(vlan)# vtp password WATER

Setting device VLAN database password to WATER.

Router(vlan)# exit

APPLY completed.

Exiting....

Router#
```

В следующем примере показана настройка коммутатора в качестве VTP-клиента.

```
Router# vlan database

Router(vlan)# vtp client

Setting device to VTP CLIENT mode.

Router(vlan)# exit
```

```
In CLIENT state, no apply attempted.

Exiting....

Router#
```

В следующем примере показана настройка коммутатора с прозрачным режимом VTP.

```
Router# vlan database

Router(vlan)# vtp transparent

Setting device to VTP TRANSPARENT mode.

Router(vlan)# exit

APPLY completed.

Exiting....

Router#
```

Протокол Spanning Tree: примеры

- Пример интерфейса протокола Spanning Tree и настройки приоритета портов протокола Spanning Tree
- Пример настройки стоимости порта протокола Spanning Tree
- Приоритет моста сети VLAN
- Пример настройки времени приветствия
- Пример настройки времени задержки пересылки для сети VLAN
- Пример настройки максимального времени устаревания для сети VLAN
- Протокол Spanning Tree: примеры
- Пример корневого моста для протокола Spanning Tree

Пример интерфейса протокола Spanning Tree и настройки приоритета портов протокола Spanning Tree

В следующем примере показана настройка приоритета порта сети VLAN для интерфейса.

```
Router# configure terminal

Router(config)# interface fastethernet 0/3/2

Router(config-if)# spanning-tree vlan 20 port-priority 64
```

```
Router(config-if)# end

Router#
```

В следующем примере показана проверка настройки сети VLAN 200 на интерфейсе в качестве порта магистрального канала.

```
Router# show spanning-tree vlan 20


VLAN20 is executing the ieee compatible Spanning Tree protocol
 Bridge Identifier has priority 32768, address 00ff.ff90.3f54
 Configured hello time 2, max age 20, forward delay 15
 Current root has priority 32768, address 00ff.ff10.37b7
 Root port is 33 (FastEthernet0/3/2), cost of root path is 19
 Topology change flag not set, detected flag not set
 Number of topology flags 0 last change occurred 00:05:50 ago
 Times: hold 1, topology change 35, notification 2
    hello 2, max age 20, forward delay 15
 Timers: hello 0, topology change 0, notification 0, aging 0


Port 33 (FastEthernet0/3/2) of VLAN20 is forwarding
 Port path cost 18, Port priority 64, Port Identifier 64.33
 Designated root has priority 32768, address 00ff.ff10.37b7
 Designated bridge has priority 32768, address 00ff.ff10.37b7
 Designated port id is 128.13, designated path cost 0
 Timers: message age 2, forward delay 0, hold 0
 Number of transitions to forwarding state: 1
 BPDU: sent 1, received 175

Router#
```

Пример настройки стоимости порта протокола Spanning Tree

В следующем примере показан способ изменения стоимости порта протокола Spanning Tree интерфейса Fast Ethernet.

```
Router# configure terminal

Router(config)# interface fastethernet 0/3/2

Router(config-if)# spanning-tree cost 18

Router(config-if)# end

Router#


Router#show run interface fastethernet0/3/2

Building configuration...


Current configuration: 140 bytes

!

interface FastEthernet0/3/2

switchport access vlan 20

 no ip address

 spanning-tree vlan 20 port-priorityy 64

 spanning-tree cost 18

end
```

В следующем примере показана проверка настройки интерфейса в качестве порта доступа.

```
Router# show spanning-tree interface fastethernet 0/3/2

Port 33 (FastEthernet0/3/2) of VLAN20 is forwarding

 Port path cost 18, Port priority 64, Port Identifier 64.33

 Designated root has priority 32768, address 00ff.ff10.37b7

 Designated bridge has priority 32768, address 00ff.ff10.37b7

 Designated port id is 128.13, designated path cost 0

 Timers: message age 2, forward delay 0, hold 0

 Number of transitions to forwarding state: 1

 BPDU: sent 1, received 175

Router#
```

Приоритет моста сети VLAN

В следующем примере показана настройка приоритета моста сети VLAN 20 со значением 33792.

```
Router# configure terminal

Router(config)# spanning-tree vlan 20 priority 33792

Router(config)# end

Router#
```

Пример настройки времени приветствия

В следующем примере показана настройка времени приветствия для сети VLAN 20 со значением 7 секунд.

```
Router# configure terminal

Router(config)# spanning-tree vlan 20 hello-time 7

Router(config)# end

Router#
```

Пример настройки времени задержки пересылки для сети VLAN

```
Router# configure terminal

Router(config)# spanning-tree vlan 20 forward-time 21

Router(config)# end

Router#
```

Пример настройки максимального времени устаревания для сети VLAN

```
Router# configure terminal

Router(config)# spanning-tree vlan 20 max-age 36

Router(config)# end

Router#
```

Протокол Spanning Tree: примеры

```
Router# configure terminal

Router(config)# spanning-tree vlan 20

Router(config)# end
```

```
Router#
```

Примечание. Протокол Spanning Tree включен по умолчанию, поэтом при вводе команды «show running» для просмотра настройки команда, использованная для включения протокола Spanning Tree, в выходных данных отображаться не будет.

```
Router# configure terminal

Router(config)# no spanning-tree vlan 20

Router(config)# end

Router#
```

Пример корневого моста для протокола Spanning Tree

В следующем примере показана настройка коммутатора в качестве корневого моста для сети VLAN 10 в сети с диаметром 4.

```
Router# configure terminal

Router(config)# spanning-tree vlan 10 root primary diameter 4

Router(config)# exit

Router#
```

Обработка таблицы MAC-адресов: пример

```
Router(config)# mac-address-table static beef.beef.beef int fa0/1/5

Router(config)# end
```

В следующем примере показана настройка безопасности порта в таблице MAC-адресов.

```
Router(config)# mac-address-table secure 0000.1111.2222 fa0/1/2 vlan 3

Router(config)# end
```

Источник анализатора коммутируемых портов (SPAN): примеры

- Пример настройки источника SPAN
- Пример настройки узла назначения SPAN
- Пример удаления источников или узлов назначения из сеанса SPAN

Пример настройки источника SPAN

В следующем примере показана настройка сеанса 1 SPAN для мониторинга двунаправленного трафика от интерфейса источника Fast Ethernet 0/1/1.

```
Router(config)# monitor session 1 source interface fastethernet 0/1/1
```

Пример настройки узла назначения SPAN

В следующем примере показана настройка интерфейса Fast Ethernet 0/3/7 в качестве узла назначения для сеанса 1 SPAN.

```
Router(config)# monitor session 1 destination interface fastethernet 0/3/7
```

Пример удаления источников или узлов назначения из сеанса SPAN

В следующем примере показано удаление интерфейса Fast Ethernet 0/3/2, использовавшегося в качестве источника для сеанса 1 SPAN.

```
Router(config)# no monitor session 1 source interface fastethernet 0/3/2
```

Функция IGMP Snooping: пример

В следующем примере показаны выходные данные команд настройки функции IGMP Snooping.

```
Router# show mac-address-table multicast igmp-snooping



HWIC Slot: 1

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

   MACADDR     VLANID     INTERFACES



0100.5e05.0505    1        Fa0/1/1

0100.5e06.0606    2



HWIC Slot: 3

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

   MACADDR     VLANID     INTERFACES



0100.5e05.0505    1        Fa0/3/4

0100.5e06.0606    2        Fa0/3/0



Router#
```

В следующем примере показаны выходные данные команды **sh run int**, введенной в привилегированном режиме EXEC для сети VLAN 1.

```
Router#sh run int vlan 1


Building configuration...


Current configuration :82 bytes

!

interface Vlan1

ip address 192.168.4.90 255.255.255.0

ip pim sparse-mode

end


Router#sh run int vlan 2


Building configuration...


Current configuration :82 bytes

!

interface Vlan2

ip address 192.168.5.90 255.255.255.0

ip pim sparse-mode

end


Router#

Router# sh ip igmp group


IGMP Connected Group Membership

Group Address    Interface                Uptime    Expires   Last Reporter

239.255.255.255  Vlan1                    01:06:40  00:02:20  192.168.41.101

224.0.1.40       Vlan2                    01:07:50  00:02:17  192.168.5.90
```

```
224.5.5.5        Vlan1                    01:06:37  00:02:25  192.168.41.100

224.5.5.5        Vlan2                    01:07:40  00:02:21  192.168.31.100

224.6.6.6        Vlan1                    01:06:36  00:02:22  192.168.41.101

224.6.6.6        Vlan2                    01:06:39  00:02:20  192.168.31.101

Router#
```

```
Router# show ip mroute
```

```
IP Multicast Routing Table

Flags:D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C -

Connected,

      L - Local, P - Pruned, R - RP-bit set, F - Register flag,

      T - SPT-bit set, J - Join SPT, M - MSDP created entry,

      X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,

      U - URD, I - Received Source Specific Host Report

Outgoing interface flags:H - Hardware switched

Timers:Uptime/Expires

Interface state:Interface, Next-Hop or VCD, State/Mode


(*, 239.255.255.255), 01:06:43/00:02:17, RP 0.0.0.0, flags:DC

 Incoming interface:Null, RPF nbr 0.0.0.0

 Outgoing interface list:

   Vlan1, Forward/Sparse, 01:06:43/00:02:17


(*, 224.0.1.40), 01:12:42/00:00:00, RP 0.0.0.0, flags:DCL

 Incoming interface:Null, RPF nbr 0.0.0.0

 Outgoing interface list:

   Vlan2, Forward/Sparse, 01:07:53/00:02:14


(*, 224.5.5.5), 01:07:43/00:02:22, RP 0.0.0.0, flags:DC
```

```
 Incoming interface:Null, RPF nbr 0.0.0.0

 Outgoing interface list:

   Vlan1, Forward/Sparse, 01:06:40/00:02:22

   Vlan2, Forward/Sparse, 01:07:44/00:02:17


(*, 224.6.6.6), 01:06:43/00:02:18, RP 0.0.0.0, flags:DC

 Incoming interface:Null, RPF nbr 0.0.0.0

 Outgoing interface list:

   Vlan1, Forward/Sparse, 01:06:40/00:02:18

   Vlan2, Forward/Sparse, 01:06:43/00:02:16


Router#
```

Контроль шторма: пример

В следующем примере показано включение подавления мультиадресной рассылки на интерфейсе Fast Ethernet interface 2 со значением 70 процентов.

```
Router# configure terminal

Router(config)# interface FastEthernet0/3/3

Router(config-if)# storm-control multicast threshold 70.0 30.0

Router(config-if)# end


Router#show storm-control multicast

Interface  Filter State  Upper    Lower    Current

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

Fa0/1/0    inactive      100.00%  100.00%  N/A

Fa0/1/1    inactive      100.00%  100.00%  N/A

Fa0/1/2    inactive      100.00%  100.00%  N/A

Fa0/1/3    inactive      100.00%  100.00%  N/A

Fa0/3/0    inactive      100.00%  100.00%  N/A

Fa0/3/1    inactive      100.00%  100.00%  N/A
```

```
Fa0/3/2    inactive      100.00%  100.00%  N/A

Fa0/3/3    Forwarding     70.00%   30.00%  0.00%

Fa0/3/4    inactive      100.00%  100.00%  N/A

Fa0/3/5    inactive      100.00%  100.00%  N/A

Fa0/3/6    inactive      100.00%  100.00%  N/A

Fa0/3/7    inactive      100.00%  100.00%  N/A

Fa0/3/8    inactive      100.00%  100.00%  N/A
```

Коммутация Ethernet: примеры

- Пример подсетей для голоса и данных
- Пример маршрутизации между сетями VLAN
- Пример настройки одиночной сети
- Пример использования портов Ethernet на IP-телефонах с несколькими портами

Пример подсетей для голоса и данных

В следующем примере показана настройка отдельных сетей для голоса и данных на интерфейсной плате EtherSwitch HWIC.

```
interface FastEthernet0/1/1

    description DOT1Q port to IP Phone

    switchport native vlan 50

    switchport mode trunk

    switchport voice vlan 150


interface Vlan 150

description voice vlan

ip address 10.150.1.1 255.255.255.0

ip helper-address 172.20.73.14 (See Note below)


interface Vlan 50
```

```
description data vlan

ip address 10.50.1.1 255.255.255.0
```

При этой настройке IP-телефон получает инструкцию на отправку пакета со значением идентификатора 802.1Q VLAN ID, равным 150, и значением 802.1p, равным 5 (значением для голосового трафика по умолчанию).

Примечание. В централизованной модели развертывания CallManager DHCP-сервер может быть подключен по каналу WAN. В этом случае на голосовом интерфейсе VLAN для IP-телефона необходимо использовать команду **ip helper-address**, указывающую на DHCP-сервер. Это необходимо для получения его IP-адреса, а также адреса TFTP-сервера, необходимого для настройки.
Помните, что IOS поддерживает функцию DHCP-сервера. При использовании этой функции интерфейсная плата EtherSwitch HWIC выступает в качестве локального DHCP-сервера, а вспомогательный адрес не требуется.

Пример маршрутизации между сетями VLAN

Настройка маршрутизации между сетями VLAN идентична настройке интерфейсной платы EtherSwitch HWIC с MSFC. Настройка интерфейса для маршрутизации WAN одинакова на других платформах IOS.

В следующем примере показан образец настройки.

```
interface Vlan 160

    description voice vlan

    ip address 10.6.1.1 255.255.255.0



interface Vlan 60

description data vlan

ip address 10.60.1.1 255.255.255.0



interface Serial0/3/0

ip address 160.3.1.2 255.255.255.0
```

Примечание. Интерфейсная плата EtherSwitch HWIC поддерживает стандартные протоколы маршрутизации IGP, например RIP, IGRP, EIGRP и OSPF. Мультиадресная маршрутизация также поддерживается для разреженного режима PIM, уплотненного режима PIM и режима разрежения-уплотнения.

Пример настройки одиночной подсети

Интерфейсная плата EtherSwitch HWIC поддерживает использование параметра 802.1p при настройке голосовой сети VLAN. Использование этого параметра позволяет IP-телефону помечать пакеты VoIP атрибутом CoS со значением 5 в

собственной сети VLAN, в то время как остальной трафик от компьютера будет отправляться непомеченным.

В следующем примере показана настройка одной подсети для интерфейсной платы EtherSwitch HWIC.

```
Router# FastEthernet 0/1/2

description Port to IP Phone in single subnet

    switchport access vlan 40
```

Интерфейсная плата EtherSwitch HWIC дает IP-телефону инструкцию на отправку кадра 802.1Q с нулевым значением идентификатора VLAN ID и со значением 802.1p (атрибут COS со значением 5 для трафика канала). В данном примере для голоса и данных используется сеть VLAN 40.

Пример использования портов Ethernet на IP-телефонах с несколькими портами

В следующем примере показана настройка IP-телефона.

```
interface FastEthernet0/x/x

    switchport voice vlan x

    switchport mode trunk
```

В следующем примере показана настройка компьютера.

```
interface FastEthernet0/x/y

    switchport mode access

    switchport access vlan y
```

Примечание. Метод с использованием отдельной подсети и отдельного адресного IP-пространства может быть невозможным для некоторых малых офисов вследствие особых настроек IP-маршрутизации. Если IP-маршрутизация предусматривает выделение дополнительной подсети в удаленном офисе, можно использовать Cisco Network Registrar и вторичную адресацию.

Дополнительные ссылки

В следующих разделах приведены дополнительные ссылки, относящиеся к интерфейсным платам EtherSwitch HWIC.

Дополнительная документация

Смежные темы	Название документа
Установка интерфейсных плат	Руководство по установке интерфейсных плат Cisco

Информация о настройке функций Voice over IP	Руководство по настройке обмена голосовыми, видео- и факсимильными данными для Cisco IOS
Команды Voice over IP	Справочник по командам настройки обмена голосовыми, видео- и факсимильными данными Cisco IOS, версия 12.3 T

Стандарты

Стандарты	Название
Эта функциональная возможность не поддерживает новые или измененные стандарты и не изменила поддержки существующих стандартов.	—

Базы данных MIB

Базы данных MIB	Ссылка на базы данных MIB
Эта функциональная возможность не поддерживает новые или измененные базы данных MIB и не изменила поддержки существующих баз данных MIB.	Для поиска и загрузки баз данных управляющей информации (Management Information Base, MIB) для выбранных платформ, версий Cisco IOS и наборов характеристик воспользуйтесь страницей поиска баз данных Cisco MIB Locator по следующему адресу: http://www.cisco.com/go/mibs

Документы RFC

Документы RFC	Название
Эта функциональная возможность не поддерживает новые или измененные документы RFC и не изменила поддержки существующих документов RFC.	—

Техническая поддержка

Описание	Ссылка
Главная страница центра технической поддержки (Technical Assistance Center, TAC), содержащая 30 000 страниц технической информации с возможностью поиска, включая ссылки на продукты, технологии, решения, технические	http://www.cisco.com/cisco/web/support/index.html

советы и инструментальные средства. Зарегистрированные пользователи веб-сайта cisco.com могут войти в систему со следующей страницы и получить еще более обширную информацию.	

Дата генерации PDF файла: Jan 05, 2010

http://www.cisco.com/support/RU/customer/content/9/97378/prod_sw_iosswrel_ps5207_prod_feature_guide09186a00802c6bb6.shtml