Меньшуткин А В

Справочник по настройке сетевого оборудования Cisco

Александр Меньшуткин

Справочник по настройке сетевого оборудования Cisco

«ЛитРес: Самиздат»

2020

Меньшуткин А. В.

Справочник по настройке сетевого оборудования Cisco /
А. В. Меньшуткин — «ЛитРес: Самиздат», 2020

Данная книга является справочником по конфигурации и траблшутингу сетевых устройств компании Cisco, в ней приведены описания и примеры настроек сетевых протоколов, к примеру, таких, как STP, EIGRP, OSPF, BGP, MPLS.

Содержание

Введение

Об этой книги

В процессе подготовки к получению сертификатов нарабатывался материал, файлы с командами и выводами show и debug которые приходилось систематизировать и объединять в один большой файл для удобства поиска, изучения и хранения. Результатом это работы и стала эта книга и она является справочным материалом для настройки сетевого оборудования компании Cisco. К сожаленью должен предупредить, что возможно не корректное отображение команд show и debug, а также возможны опечатки и ошибки, но я буду продолжать дополнять и редактировать это произведение по этому не судите строго, всё отраженные в данной книге команды были отработаны лично мною. Также стоит заметить, что некоторые команды на новом оборудование могут иметь другой синтаксис.

С обозначением, всё достаточно просто, адреса на оборудование совпадают с номером устройства, к примеру 10.0.21.1 принадлежит маршрутизатору r1, по третьему октету видно что он соединен с маршрутизатором r2, другой пример адрес 10.0.214.1 общий для маршрутизаторов r1, r2, r4. Сеть 10.0.12.0 также находится между ними где маршрутизатору r1 принадлежит адрес 10.0.12.1, а r2 10.0.12.2. Также в некоторых примерах есть Frame-relay не обращайте внимание, просто на нем было на тот момент проще сделать, хотя я лично не встречал данного типа сетей.

Первоначальная настройка коммутаторов и маршрутизаторов

Оборудование Cisco имеет два основных режима работы: пользовательский (user mode) и привилегированный (privileged mode). Пользовательский режим использует приглашение

Router>

В данном режиме имеется множественные ограничения, просмотреть, что доступно из данного режима можно вводом знака вопроса ?, который также является подсказкой. Для того чтобы изменить конфигурацию устройства необходимо войти в привилегированный режим, для этого вводиться команда enable

Router>enable

И переходим в привилегированный режим:

Router#

Для того чтобы приступить к настройке устройства, необходимо перейти в режим настройки командой configure terminal

Router#configure terminal

Переходим в режим глобального конфигурирования:

Router(config)#

Для выхода из этого режима можно воспользоваться командой exit, end или Ctrl+Z, команда exit переводит на шаг назад, а две других сразу в привилегированный режим

Для сохранения изменений в устройстве необходимо в привилегированном режиме ввести команду

Router#copy running-config startup-config

или

Router#write

Либо это можно сделать в любом другом режиме, используя команду do:

Router(config)#do copy running-config startup-config

Просмотреть сделанные изменения или конфигурацию, можно путем команды show. К примеру, для просмотра конфигурации достаточно набрать

Router#show running-config

Для просмотра из режима настройки

Router(config)#do show running-config

При этом не надо набирать команду целиком, достаточно набрать sh run, если для устройства команда будет не понятна, оно обозначит не понятный символ символов каретки (^).

Для полного удаления конфигураций, Вам нужно использовать старый маршрутизатор или коммутатор на новом месте, воспользуйтесь командой:

Router#erase startup-config

После этого перегрузите его командой:

Router#reload

Также можно перегрузить устройство в определенное время, Вы хотите это сделать в 20:00 сегодня:

Switch# reload at 20:00

И в определенный день:

Switch# reload at 20:00 jun 10

Также надо помнить, что коммутатор содержит таблицы виртуальных локальных сетей (vlan) в отдельном файле и для их удаления Вам необходимо удалить этот файл или удалить виртуальные локальные сети вручную.

Удаление всех виртуальных локальных сетей:

sw2#delete flash:vlan.dat

Удаление виртуальной локальной сети (vlan) под номером 234:

sw2(config)#no vlan 234

Так же считаю очень полезным знание клавиш редактирования в командной строке, ниже приведена таблица:

Клавиша	Описание
Ctrl+A	Возвращает курсор к началу текущей строки
Ctrl+B	Перемещает курсор на один символ назад
Ctrl+D	Удаляет символ слева от курсора
Ctrl+E	Перемещает курсор в конец строки
Ctrl+F	Перемещает курсор вперед на один символ
Ctrl+K	Удаляет все символы от текущего положения курсора до конца строки
Ctrl+N	Переход на следующую в предыстории сеанса команду
Ctrl+P	Переход на предыдущую в предыстории сеанса команду
Ctrl+T	Меняет местами текущий символ и символ слева от курсора
Ctrl+R	Перерисовывает или вводит заново текущую строку
Ctrl+U	Очищает строку
Ctrl+W	Удаляет слово слева от курсора
Ctrl+X	Удаляет все символы от текущего положения курсора и до начала строки
Ctrl+Y	Вставляет символы, удаленные последними, на место соответствующие текущему положению курсора
Ctrl+Z	Выход из текущего режима конфигурирования и возврат в предыдущий режим
Табуляция	Попытка завершить текущую команду
↑	Переход назад в предыстории команд
↓	Переход вперед в предыстории команд
←	Перевод курсора влево
→	Перевод курсора вправо
Ctrl+^, затем X	Прерывание выполнения любой команды
Пробел	Позволяет пролистывать блоками.

Следует знать команды оптимизации запросов, пример:

Switch#show running-config

При вводе Вам будет показана вся конфигурация, но Вы можете оптимизировать запрос, используя команды begin, include, exclude и применяемую только для маршрутизаторов команду section. Как это выглядит на практике:

Switch#show running-config | begin interface

При выводе Вам будет представлена информация с того момента где в строке есть слово interface, соответственно если вы примените include, то получите только те строки, где присутствует интересующая Вас команда:

Switch# show interface | include protocol

Vlan 1 is up, line protocol is up

FastEthernet0/0 is up, line protocol is up

Ваше сетевое оборудование, для удобства, должно иметь имена, задается это командой:

Router(config)#hostname r1

После ввода команды видно как мы назвали маршрутизатор:

r1(config)#

В начале настройки устройства, для удобства работы на нем следует ввести несколько команд, которые я привожу ниже.

Для отключения разрешения символьных имен:

r1(config)#no ip domain-lookup

r1(config)#line console 0

Вводим бесконечное значение тайм-аута, не будет отключаться сессия:

r1(config-line)#exec-timeout 0 0

Делаем синхронизацию вывода не запрошенных сообщений:

r1(config-line)#logging synchronous

r1(config-line)#exit

Для удаленного управления оборудование мы должны ввести следующие команды:

Заводим пользователя и пароль для него и выставляем самый высокий уровень привилегий:

r1(config)#username admin privilege 15 password cisco

Но лучше сделать это вот так:

Заменяем слово password на secret, и Ваш пароль будет защищён.

r1(config)#username admin privilege 15 secret cisco

Настраиваем доступ по SSH, для этого вводим следующие команды:

Нужно указать Ваш домен, имя маршрутизатору мы уже выбрали:

r1(config)#ip domain-name cisco.net

r1(config)#crypto key generate rsa

Далее появиться запрос на размер ключа, ставим 2048, так как желательно самое большое значение, если данное значение ввести не удается ставим максимально возможное.

Вводим нужную версию:

r1(config)#ip ssh version 2

Ниже задаем, сколько подключений возможно, в примере ниже мы установили пять, с 0 по 4, но можем установить и больше:

r1(config)#line vty 0 4

Позволяем вход для локально заданных пользователей:

r1(config-line)#login local

Разрешаем два типа подключений:

r1(config-line)#transport input telnet ssh

Выходим и сохраняемся:

r1(config-line)#end

r1#write

Проверить мы можем командой show running-config, а также show ip ssh.

Посмотреть информацию об открытых сессиях можно командой show sessions, а через show users информацию об активных линиях.

Не забывайте сохраняться после внесения изменений:

r1# copy running-config startup-config

Также для удобства важно подписывать интерфейсы, как показано ниже:

r1(config)#interface f0/0

r1(config-if)#description *** Connects to router r2 ***

И задаём адрес на интерфейсе:

r1(config-if)#ip address 10.1.1.1 255.255.255.0

На этом примере показано изменение скорость и дуплекс на интерфейсе:

sw1#configure terminal

sw1(config)#interface f0/0

sw1(config-if)#speed ?

10 Force 10 Mbps operation

100 Force 100 Mbps operation

auto Enable AUTO speed configuration

sw1(config-if)#duplex ?

auto Enable AUTO duplex configuration
full Force full duplex operation
half Force half-duplex operation

Проверив командой show, мы видим, что по умолчанию на данном интерфейсе установлено авто скорость и дуплекс:

sw1(config-if)#do sh int f0/0 | inc Auto
Auto-duplex, Auto-speed

При попытке задать адрес на интерфейсе коммутатора, мы получим следующие сообщение:

sw1(config-if)#ip address 10.1.1.1 255.255.255.0
% IP addresses may not be configured on L2 links.

И если нам нужно задать на этом порту IP адрес нам надо сделать данный интерфейс интерфейсом третьего уровня, мы должны сделать следующие:

sw1(config-if)#no switchport

И после этого вводим адрес и проверяем интерфейс:

sw1(config-if)#ip address 10.1.1.1 255.255.255.0
sw1(config-if)#do show run interface f0/0
Building configuration…
Current configuration : 83 bytes
!
interface FastEthernet0/0
no switchport
ip address 10.1.1.1 255.255.255.0
end

Мы установили нужный адрес.

Если мы хотим отменить данную команду и сделать данный интерфейс интерфейсом второго уровня, вводим:

sw1(config-if)#switchport

Команда shutdown отключает интерфейс, команда no shutdown включает его, на маршрутизаторах интерфейсы по умолчанию выключены.

Мы можем при необходимости изменять MTU на нашем устройстве:

По умолчанию оно 1500, для интерфейсов от 10 до 100 Mb/s область от 1500 до 1998 byte.

sw1(config)#system mtu <указываем значение>

По умолчанию оно 1500,для интерфейсов 1000 Mb/s область от 1500 до 9000 byte.

sw1(config)#system mtu jumbo <указываем значение>

По умолчанию оно 1500 и может быть любым, но не факт, что будет принято.

r1(config)#system mtu routing <указываем значение>

Для того чтобы новое MTU вступило в силу требуется сохранить конфигурацию и перегрузить устройство.

Иногда требуется восстановить настройки интерфейса по умолчанию, это делается командой приведенной ниже:

sw1(config)#default interface f0/0
Building configuration…
Interface FastEthernet0/0 set to default configuration
sw1(config)#

Так же на любом интерфейсе можно создать под интерфейсы, делается это так:

r1(config)#interface s0/0/0

Удалили адрес на интерфейсе:

r1(config-if)#no ip address

Включили интерфейс, как я писал ранее, он по умолчанию отключен:

r1(config-if)#no shutdown

Задаем пару под интерфейсов:

r1(config-if)#interface s0/0/0.1 point-to-point

r1(config-if)#ip address 10.1.1.1 255.255.255.0

r1(config-if)#interface s0/0/0.2 point-to-point

r1(config-if)#ip address 10.1.2.1 255.255.255.0

На одном интерфейсе можно задать несколько адресов:

r1(config)#interface s0/0/0

r1(config-if)#ip address 10.1.1.1 255.255.255.0

Просто добавляем в конце команду secondary:

r1(config-if)#ip address 10.1.2.1 255.255.255.0 secondary

Также на оборудование используется петлевой интерфейс, данный интерфейс удобен для тестирования оборудования, создается он командой:

r1(config)# interface loopback 0

r1(config-if)# ip address 1.1.1.1 255.255.255.255

Мы можем настраивать сразу насколько интерфейсов, это удобно при настройке портов доступа на коммутаторе.

Команда range позволяет это сделать:

sw1(config)#interface range f0/1 – 24

Для обнаружения соседних устройств, в оборудование Cisco используется частный протокол CDP – Cisco Discovery Protocol, протокол может быть включен как глобально на устройстве, так и только на определенном интерфейсе:

Глобальное включение, выключение:

r1(config)#(no) cdp run

r1(config)#interface s0/0/0

Пример включения, выключение на интерфейсе:

r1(config-if)#(no) cdp enable

Просмотр соседних устройств, при добавлении слова detail будет предоставлена более детальная информация о соседних устройствах:

r1#show cdp neighbors (detail)

Следует также помнить об открытом протоколе LLDP – Link Layer Discovery Protocol который также помогает собрать информацию о соседях, он включается командой показанной ниже и проверяется похожими с cdp командами:

r1(config)#run lldp

r1# show lldp ?

Данная ниже команда отобразит информацию о программном обеспечении, самом устройстве и его аппаратной части:

r1#show version

Cisco IOS Software, C2900 Software (C2900-UNIVERSALK9-M), Version 15.1(4)M1, RELEASE SOFTWARE (fc1)

Technical Support: http://www.cisco.com/techsupport

Copyright (c) 1986-2011 by Cisco Systems, Inc.

Compiled Tue 14-Jun-11 19:25 by prod_rel_team

ROM: System Bootstrap, Version 15.0(1r)M12, RELEASE SOFTWARE (fc1)

r1 uptime is 13 hours, 43 minutes

System returned to ROM by reload at 18:25:57 MSK Tue May 28 2013

System restarted at 18:27:34 MSK Tue May 28 2013
System image file is "flash0:c2900-universalk9-mz.SPA.151-4.M1.bin"
Last reload type: Normal Reload
Last reload reason: Reload Command
— часть информации удалена –
Cisco CISCO2901/K9 (revision 1.0) with 487424K/36864K bytes of memory.
Processor board ID FCZ1540C5LU
2 Gigabit Ethernet interfaces
1 terminal line
DRAM configuration is 64 bits wide with parity enabled.
255K bytes of non-volatile configuration memory.
255744K bytes of ATA System CompactFlash 0 (Read/Write)
License Info:
License UDI:
—
Device# PID SN
—
*0 CISCO2901/K9 FCZXXXXXXX

Technology Package License Information for Module:'c2900'
—
Technology Technology-package Technology-package
Current Type Next reboot
—
ipbase ipbasek9 Permanent ipbasek9
security None None None
uc None None None
data None None None
Configuration register is 0x2102

Для установки времени используем следующие команды:

Устанавливаем время:

r1#clock set 08:00:00 Jan 2011

Часовой пояс:

r1(config)#clock timezone MSK+4

Задаем для маршрутизатора сервер времени:

r1(config)#ntp server 10.1.1.2

Данной командой маршрутизатор назначается сервером времени:

r2(config)#ntp master

Данная команда показывает время на нашем устройстве:

r1#show clock

Заставляет маршрутизатор обновлять часы по времени NTP-сервера:

r1(config)#clock update-calendar

Заставляет маршрутизатор задействовать внутренний календарь для получения эталонного времени:

r1(config)#clock calendar-valid

Подводим итог:

Для первоначальной настройки маршрутизатора или коммутатора мы должны ввести следующие команды и обязательно на подключенном к нашей сети интерфейсе указать адрес:

Router>enable

```
Router#conf t
Router(config)#hostname r1
r1(config)#interface F0/0
r1(config-if)#no shutdown
r1(config-if)#ip add 10.0.12.1 255.255.255.0
r1(config)#ip route 0.0.0.0 0.0.0.0 10.0.12.2
r1(config)#no ip domain-lookup
r1(config)#line console 0
r1(config-line)#exec-timeout 0 0
r1(config-line)#logging synchronous
r1(config-line)#exit
r1(config)#username admin privilege 15 secret cisco
r1(config)#ip domain-name cisco.net
r1(config)#crypto key generate rsa 2048
r1(config)#ip ssh version 2
r1(config)#line vty 0 4
r1(config-line)#login local
r1(config-line)#transport input telnet ssh
r1(config-line)#exit
r1(config)#exit
r1#clock set 08:00:00 Jan 2020
r1#write
```

Теперь мы можем подключиться к данному устройству по протоколам telnet и ssh с соседнего устройства, к примеру тут на него указан маршрут по умолчанию.

Коммутация

Виртуальная локальная сеть

Virtual
Local
Area
Network
(
Vlan
)

Для виртуально локальной сети (vlan) могут быть назначены номера от 1 до 1005, в прозрачном варианте (transparent) от 1 до 4094. Для Vlan можно назначить любое имя, но предпочтительнее называть их по их функциям, к примеру, admin ту, в которой работают администраторы и так далее:

Создаем виртуальную локальную сеть (vlan):

sw1(config)#vlan 234

Следующей командой задаем имя для данной виртуальной локальной сети:

sw1(config-vlan)#name VLAN234
sw1(config-vlan)#end
sw1#wr

Удалить виртуальную локальную сеть (vlan) можно простои командой no, пример приведён ниже:

sw1(config)#no vlan 234

Порт, предназначенный для одной виртуальной локальной сети, называется – портом доступа (access port). Порт настраивается следующими командами:

sw1(config)#interface f0/2

Назначаем порт портом доступа:

sw1(config-if)# switchport mode access

Задаем ему виртуальную локальную сеть (vlan):

sw1(config-if)# switchport access vlan 234

Проверить порт можно командой, показанной ниже:

sw1#show interface f0/2 switchport
Name: Fa0/2
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 234 (Support)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none

Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none

Пример создание двух виртуальных локальных сетей (vlan) и назначения им интерфейсов:

sw1(config)#vlan 5
sw1(config-vlan)#name vlan5
sw1(config-vlan)#vlan 43
sw1(config-vlan)#name vlan43
sw1(config-vlan)#exit
sw1(config)#interface FastEthernet0/5
sw1(config-if)#switchport access vlan 5
sw1(config-if)#interface FastEthernet0/24
sw1(config-if)#switchport access vlan 43
sw1(config-if)#end
sw1#wr

Посмотреть мы можем, командой:

sw1#show interface status
Port Name Status Vlan Duplex Speed Type
Fa0/1 notconnect 1 auto auto 10/100BaseTX
Fa0/2 notconnect 1 auto auto 10/100BaseTX
Fa0/3 connected 1 a-half a-10 10/100BaseTX
Fa0/4 notconnect 1 auto auto 10/100BaseTX
Fa0/5 vlan5 connected 5 a-half a-10 10/100BaseTX
Fa0/24 vlan43 connected 43 a-half a-10 10/100BaseTX
— часть информации удалена –

Если мы хотим поменять одну виртуальную локальную сеть (vlan) на другую, делается это просто:

Для начала данная виртуальная локальная сеть (vlan) должна присутствовать на коммутаторе. Проверить виртуальную локальную сеть можно командой show vlan brief.

Ниже приведен пример команды:

sw1#show vlan brief
VLAN Name Status Ports
— – – –
1 default active Fa0/6,Fa0/7,Fa0/8, Fa0/9
Fa0/11,Fa0/12,Fa0/13,Fa0/14
Fa0/15,Fa0/16,Fa0/17,Fa0/18
Gi0/1, Gi0/2

30 VLAN30 active
33 VLAN33 active
42 VLAN42 active
51 VLAN51 active Fa0/5
54 VALN54 active Fa0/4
234 VLAN234 active Fa0/2
243 VLAN243 active
300 VALN300 active Fa0/3
1002 fddi-default act/unsup
1003 trcrf-default act/unsup

Допустим, мы хотим установить, на интерфейс Fa0/3 vlan 30 для этого вводим следующие команды

sw1(config)#interface f0/3
sw1(config)#switchport access vlan 30
sw1(config)#exit
sw1#show vlan brief | i 30
30 VLAN30 active Fa0/3

После проверки мы видим, что на третьем интерфейсе вместо 300 находиться 30 виртуальная локальная сеть (vlan), ну соответственно мы должны обязательно сохранить наши изменения командой wr.

Магистральный протокол виртуальной локальной сети (VTP) Vlan Trunking Protocol

Протокол VTP используется для создания и управления виртуальными локальными сетями. Для настройки VTP перейдем в режиме конфигурирования и введем vtp

После ввода знака вопроса, мы видим, что мы можем настроить

sw1(config)#vtp ?

domain Set the name of the VTP administrative domain.

file Configure IFS file system file where VTP configuration is stored.

interface Configure interface as the preferred source for the VTP IP updater address.

mode Configure VTP device mode

password Set the password for the VTP administrative domain

pruning Set the administrative domain to permit pruning

version Set the administrative domain to VTP version

Добавив команду режим (mode) мы видим, что существует три модели настройки VTP:

sw2(config)#vtp mode ?

client Set the device to client mode.

server Set the device to server mode.

transparent Set the device to transparent mode

Режим прозрачный (transparent) поддерживает расширенные виртуальные локальные сети (vlans) от 1 до 4094. Он более удобен в использовании, так как в прозрачном режиме коммутатор только передает информацию и не применяет её к своей конфигурации.

Режим клиент (client)применяет к себе все настройки сделанные на сервере.

Режим сервер (server) предназначен для ввода и удаления новых виртуальных локальных сетей, на коммутаторах он установлен по умолчанию.

Показанный ниже утилита используется, только в режиме сервера (server) позволяет сократить трафик в сети. Но при этом очень сильно загружает коммутатор, который, является сервером:

sw1(config)#vtp pruning

Мы настраиваем свои коммутаторы так:

sw1(config)#vtp domain CISCO

sw1(config)#vtp mode transparent

sw1(config)#vtp password cisco

Не обязательно для VTP задавать домен и паспорт, но очень важно указать модель использования коммутатора, по умолчанию коммутатор находиться в режиме сервера (server).

Для проверки вводим команду, показанную ниже, и получаем:

sw1#show vtp status

VTP Version : running VTP2

Configuration Revision : 0

Maximum VLANs supported locally : 1005

Number of existing VLANs : 16

VTP Operating Mode : Transparent

VTP Domain Name : CISCO

VTP Pruning Mode : Disabled

VTP V2 Mode : Enabled

VTP Traps Generation : Disabled

MD5 digest : 0x07 0x4A 0x67 0xF3 0xA0 0x0E 0x9B 0xAD

Configuration last modified by 150.2.20.1 at 3-1-93 01:18:04

Данная ниже команда показывает заданный нами паспорт:

```
sw1#show vtp password
```

Конечно, настроить VTP область можно и так:

```
sw1(config)#vtp domain CISCO
sw1(config)#vtp mode server
sw1(config)#vtp password cisco
```

А на все другие коммутаторы сделать клиентами:

```
sw2(config)#vtp domain CISCO
sw2(config)#vtp mode client
sw2(config)#vtp password cisco
```

При данной модели, как уже было, написано все изменения можно будет вносить на сервере, и они будут применяться ко всем коммутаторам сети. Но данный вариант настройки имеет один недостаток, если в систему будет, поставлен коммутатор с более высоким номером Configuration Revision он, перестроит всю систему. Что приведет к выводу сети из строя.

Протокол VTP для маршрутизаторов, при наличии в нем модуля коммутатора, настраивается другим способом, пример приводиться ниже:

```
sw1#vlan database
sw1(vlan)#vtp transparent
sw1(vlan)#vtp domain cisco.com
sw1(vlan)#vtp password cisco
```

Также мы можем добавить нужные нам функции pruning и т.д.

```
sw1(vlan)#exit
sw1#wr
```

Подводим итог:

```
sw1#conf t
sw1(config)#vtp mode transparent
sw1(config)#exit
sw1#wr
```

Для нормальной работы коммутатора достаточно одной этой команды, все изменения по vlan мы будем вносить в наши коммутаторы сами.

Коммутируемый виртуальный интерфейс Switched Virtual Interface (SVI)

Пример настройки приведен ниже.

```
sw1(config)#interface vlan 234
sw1(config-if)#ip address 10.10.234.1 255.255.255.0
sw1(config-if)#exit
```

Виртуальная локальная сеть (Vlan) на маршрутизаторах

На старых маршрутизаторах виртуальная локальная сеть задается другим способом, пример приведен ниже:

```
sw1#vlan database
sw1(vlan)#vlan 234 name ADMIN
sw1(vlan)#exit
```

Подводим итог:

```
sw1#conf t
sw1(config)#vlan 10
sw1(config-vlan)#name user_vlan
sw1(config)#vlan 11
sw1(config-vlan)#name management_vlan
sw1(config-vlan)#exit
sw1(config)#interface range f0/1 – 24
sw1(config-if)# description *** Access Interface ***
sw1(config-if)#switchport mode access
sw1(config-if)#switchport access vlan 10
sw1(config-if)#exit
sw1(config)#interface vlan 11
sw1(config-if)# description *** Management Interface ***
sw1(config-if)#ip address 10.0.11.2 255.255.255.0
sw1(config-if)#exit
sw1(config)#exit
sw1#wr
```

Мы создали две виртуальные локальные сети (vlans) для пользователей под номером 10 с портами от 1 до 24 и 11 для управления данным коммутатором, которой присвоили адрес 10.0.11.2. Обязательно в конце сохраняемся.

Магистральный порт (Trunk port)

Порт, предназначенный для множества VLAN, называется – Trunk port, магистральным портом. Протоколы магистральных портов ISL, 802.1q. Можно ещё вспомнить DTP (Dynamic Trunking Protocol), но он встречается редко в основном на очень старых коммутаторах.

ISL (Inter-Switch Link) частный протокол компании Cisco, может использоваться только на коммутаторах Cisco. Сразу стоит отметить, что на новых коммутаторах данный протокол уже не используется.

Мы задаем его сразу для двух портов, и для этого используем команду range, этой командой мы можем задать и большую область портов.

sw1(config)# interface range GigabitEthernet0/1 – 2
sw1(config-if)#switchport trunk encapsulation isl
sw1(config-if)#switchport mode trunk
Проверка осуществляется командой:
sw1#show interface trunk

802.1q открытый стандарт поддерживается всеми производителями, его мы и будем использовать, настраивается:

sw1(config)# interface range GigabitEthernet0/1 – 2
sw1(config-if)#switchport trunk encapsulation dot1q
sw1(config-if)#switchport mode trunk
На многих новых коммутаторах, достаточно ввести команду:
sw1(config)# interface range GigabitEthernet0/1 – 2
sw1(config-if)#switchport mode trunk
Так как протокол 802.1q используется по умолчанию.
Проверка осуществляется командой:
sw1#show interfaces trunk
Port Mode Encapsulation Status Native vlan
Gi0/1 on 802.1q trunking 1
Gi0/2 on 802.1q trunking 1
Port Vlans allowed on trunk
Gi0/1 1-1005
Gi0/2 1-1005
Port Vlans allowed and active in management domain
Gi0/1 1,30,33,42,51,54,234,243,300
GI0/2 1,30,33,42,51,54,234,243,300
Port Vlans in spanning tree forwarding state and not pruned
Gi0/1 1,30,33,42,51,54,234,243,300
Gi0/2 none

Также мы можем сменить native VLAN, она же не тегируемая виртуальная локальная сеть, по умолчанию она 1, но командой показанной ниже мы можем её поменять, к примеру, на 11:

sw1(config)# interface range GigabitEthernet0/1 – 2
sw1(config-if)#switchport trunk native vlan 11
Посмотреть изменения мы можем командой, показанной ниже:
sw1#show interfaces trunk
Port Mode Encapsulation Status Native vlan
Gi0/1 on 802.1q trunking 11
Gi0/2 on 802.1q trunking 11

Если нужно гарантировано отключить DTP (Dynamic Trunking Protocol) на магистральных портах, данный тип поддерживается старым оборудованием, делаем это так:

```
sw1(config)# interface range GigabitEthernet0/1 – 2
sw1(config-if)#switchport trunk encapsulation dot1q
sw1(config-if)#switchport mode trunk
sw1(config-if)#switchport nonegotiate
```

Последняя строка отключает DTP.

На магистральных портах, мы можем сделать ограничение по виртуальным локальным сетям (vlans), как это сделать показано ниже:

```
sw1(config)# interface range GigabitEthernet0/1 – 2
sw1(config-if)#switchport trunk allowed vlan 1-10
```

Существуют, также возможность удалит, добавить или исключить виртуальную локальную сеть (vlan) на магистральные порты или порт:

```
sw1(config)# interface range GigabitEthernet0/1 – 2
```

Удалили vlan 2:

```
sw1(config-if)#switchport trunk allowed vlan remove 2
```

Добавили vlan 2:

```
sw1(config-if)#switchport trunk allowed vlan add 2
```

Исключить 10 виртуальную локальную сеть:

```
sw1(config-if)#switchport trunk allowed vlan except 10
```

Подводим итог:

Для коммутатора 3560, который находиться в ядре или на уровне распределения, это выглядит так:

```
sw1#conf t
sw1(config)# interface range GigabitEthernet0/1
sw1(config-if)#switchport trunk encapsulation dot1q
sw1(config-if)#switchport mode trunk
sw1(config-if)#switchport trunk allowed vlan 1-10
sw1(config-if)#exit
sw1(config)#exit
sw1#wr
```

Для коммутатора 2960, который у нас является коммутатором уровня доступа:

```
sw2#conf t
sw2(config)# interface range GigabitEthernet0/1
sw2(config-if)#switchport mode trunk
sw2(config-if)#exit
sw2(config)#exit
sw2#wr
```

Сразу стоит отметить, что настройки на магистральных портах могут отличаться, от того, что приведено в данном примере. Мы ограничиваем доступ по виртуальным локальным сетям (vlans) на коммутаторе уровня ядра или распределения соответственно sw2 будут доступны только vlans с 1 по 10. При этом данные виртуальные сети должны быть созданы на обоих коммутаторах.

Проверка осуществляется командой:

```
sw1#show interface trunk
Port Mode Encapsulation Status Native vlan
Gi0/1 on 802.1q trunking 1
Port Vlans allowed on trunk
Gi0/1 1-4094
```

Port Vlans allowed and active in management domain
Gi0/1 1-10
Port Vlans in spanning tree forwarding state and not pruned
Gi0/1 1-10

Агрегация каналов EtherCannel 2 уровня

Позволяет объединять до 8 физических интерфейсов в один логический, создается на магистральных портах. Применяется для создания избыточности, следует отметить, что первые два варианта уже не используются и Cisco рекомендует использовать протокол LACP. Пример настройки приведен ниже:

```
sw1(config)# interface range fa0/19 – 20
sw1(config-if)# channel-group 12 mode on
sw2(config)# interface range fa0/19 – 20
sw2(config-if)# channel-group 12 mode on
```

EtherCannel 2 уровня Port Aggregation Protocol (PAgP) личный протокол Cisco, возможные применения Auto/Desirable-Desirable, настраивается так:

```
sw1(config)# interface range fa0/19 – 20
sw1(config-if)# channel-group 12 mode desirable
sw2(config)# interface range fa0/19 – 20
sw2(config-if)# channel-group 21 mode auto
```

EtherCannel 2 уровня Link Aggregation Control Protocol (LACP) открытый стандарт определенный правилом IEEE 802.3ad, возможные применения Active/Passive-Active, настраивается так:

```
sw1(config)# interface range fa0/19 – 20
sw1(config-if)# channel-group 12 mode active
sw2(config)# interface range fa0/19 – 20
sw2(config-if)# channel-group 21 mode passive
```

Подводим итог:

```
sw1#conf t
sw1(config)# interface range fa0/19 – 20
sw1(config-if)#shutdown
sw1(config-if)#switchport trunk encapsulation dot1q
sw1(config-if)#switchport mode trunk
sw1(config-if)#channel-group 12 mode active
sw1(config-if)#no shutdown
sw1(config-if)#exit
sw1(config)#exit
sw1#wr
sw2#conf t
sw2(config)# interface range fa0/19 – 20
sw2(config-if)#shutdown
sw2(config-if)#switchport trunk encapsulation dot1q
sw2(config-if)#switchport mode trunk
sw2(config-if)#channel-group 21 mode active
sw2(config-if)#no shutdown
sw2(config-if)#exit
sw2(config)#exit
sw2#wr
```

Мы подняли EtherCannel между двумя коммутаторами на портах 19 и 20. Стоит отметить команды shutdown и no shutdown при создании EtherCannel, они нужны для того, чтобы канал корректно поднялся.

Также стоит отметить, что после того как вы подняли Port-channel все изменения, к примеру добавление vlan, надо производить на интерфейсе Port-channel:

```
sw1#show run interface po12
Building configuration…
Current configuration : 127 bytes
!
interface Port-channel12
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1-10
switchport mode trunk
end
```

Проверка осуществляется командой:

```
sw1# show etherchannel summary
Flags: D – down P – in port-channel
I – stand-alone s – suspended
H – Hot-standby (LACP only)
R – Layer3 S – Layer2
U – in use f – failed to allocate aggregator
u – unsuitable for bundling
w – waiting to be aggregated
d – default port

Number of channel-groups in use: 3
Number of aggregators: 3

Group Port-channel Protocol Ports
——+——+——+——
1 Po12(SU) LACP Gi0/19(P) Gi0/20(P)
```

Агрегация каналов EtherCannel 3 уровня

Третий уровень обычно используется между уровнями ядра и распределения:

```
sw1#conf t
sw1(config)# ip routing
sw1(config)# interface port-channel 12
sw1(config-if)# no switchport
sw1(config-if)# ip address 10.1.1.1 255.255.255.0
sw1(config)# interface range fa0/19 – 20
sw1(config-if)# shutdown
sw1(config-if)# no switchport
sw1(config-if)# channel-group 12 mode on
sw1(config-if)# interface range fa0/19 – 20
sw1(config-if)#no shutdown
sw1(config-if)# end
sw1#wr
sw2#conf t
sw2(config)# ip routing
sw2(config)# interface port-channel 21
sw2(config-if)# no switchport
sw2(config-if)# ip address 10.1.1.2 255.255.255.0
sw2(config)# interface range fa0/19 – 20
sw2(config-if)# shutdown
sw2(config-if)# no switchport
sw2(config-if)# channel-group 21 mode on
sw2(config-if)#no shutdown
sw2(config-if)# interface range fa0/19 – 20
sw2(config-if)#no shutdown
sw2(config-if)# end
sw2#wr
```

Также важно помнить, что на коммутаторе должен быть включен 3 уровень, по умолчанию он может быть выключен, чтобы включить его надо ввести команду, показанную ниже, коммутаторами 3 уровня являются коммутаторы от 3500 серии и выше.

```
sw1(config)#ip routing
```

Проверка осуществляется командой:

```
sw1# show etherchannel summary
```

Агрегация

каналов
балансировка
нагрузки
(EtherChannel Load Balancing)
Ниже приведен пример настройки для простой сети.
sw1#conf t
sw1(config)#port-channel load-balance dst-ip
sw1(config)#end
sw1#wr
Возможна балансировка по разным значениям, ниже приведены возможные варианты:
dst-ip Dst IP Addr
dst-mac Dst Mac Addr
src-dst-ip Src XOR Dst IP Addr
src-dst-mac Src XOR Dst Mac Addr
src-ip Src IP Addr
src-mac Src Mac Addr
Проверка осуществляется командой:
sw1# show etherchannel load-balance
EtherChannel Load-Balancing Configuration:
dst-ip
EtherChannel Load-Balancing Addresses Used Per-Protocol:
Non-IP: Destination MAC address
IPv4: Destination IP address
IPv6: Destination IP address

Протокол

связующего
дерева
Spanning-Tree Protocol (STP)

Протокол связующего дерева, предназначен для предотвращения петель. Коммутаторы обмениваются BPDU (Bridge Protocol Data Unit) пакетами и на основании обмена данными пакетами выстраивают топологию, обмен пакетами продолжается и после того как была выстроена топология. Также происходит выборы корневого моста (bridge root), корневого порта (root port) и назначенного порта (designated port).Следует отметить, что по умолчанию на коммутаторах Cisco включен режим PVST+ (802.1d). В STP порты могут находиться в следующих состояниях:

Отключен (Disabled)
Слушает (Listening)
Изучает (Learning)
Передает (Forwarding)
Заблокирован (Blocking)

Модель STP выбирается при помощи команды указанной ниже:

```
sw1(config)#spanning-tree mode ?
mst Multiple spanning tree mode
pvst Per-Vlan spanning tree mode
rapid-pvst Per-Vlan rapid spanning tree mode
```

PVST+ (802.1d)

Протокол связующего дерева, включен по умолчанию, но он является не лучшим выбором, так как сходиться за очень большой промежуток времени, порядка 50 секунд. Существуют методы ускорения сходимости данного протокола.

Ниже показаны таймеры PVST+ и как их можно, изменить:

sw1(config)# spanning-tree vlan 1-4094 hello-time <1-10>

Hello timer 2 сек по умолчанию.

sw1(config)# spanning-tree vlan 1-4094 forward-time <4-30>

Forward Delay 15 сек по умолчанию.

sw1(config)# spanning-tree vlan 1-4094 max-age <6-40>

Max Age 20 сек по умолчанию.

Также существуют данные ниже команды, которые ускоряют PVST+, первая, ускоряет время изменения корневого порта,3-5 секунд, используется только на коммутаторах доступа. Вторая уменьшает сходимость max-age таймера, используется на всех коммутаторах.

sw1(config)#spanning-tree uplinkfast

sw1(config)#spanning-tree backbonefast

Проверка осуществляется командой:

sw1#show spanning-tree summary

Switch is in pvst mode

— часть информации удалена –

Rapid-PVST (802.1w)

Более быстрый протокол связующего дерева, для его работы надо настроить команду portfast на всех портах доступа, то есть мы указываем команду switchport mode access на простых портах и добавляем команду portfast и коммутатор не проверяет эти порты во время работы протокола STP. Данная модель более предпочтительна.

Поэтому мы задаем следующую команду на нашем коммутаторе:

sw1(config)#spanning-tree mode rapid-pvst

Проверка осуществляется командой:

sw1#show spanning-tree summary

Switch is in rapid-pvst mode

— часть информации удалена –

Протокол связующего дерева (STP) выбор корневого коммутатора

По умолчанию для 802.1d и 802.1w, корневой коммутатор будет выбран автоматический, но он может не совпасть с нашим корневым коммутатором или в результате добавления нового коммутатора в сеть, изменить всю топологию сети, поэтому настоятельно рекомендуется задать его самим. Ниже приведены два варианта команд:

```
sw1(config)# spanning-tree vlan 1-4094 priority 0
sw2(config)# spanning-tree vlan 1-4094 priority 4096
sw1(config)# spanning-tree vlan 1-4094 root primary
sw2(config)# spanning-tree vlan 1-4094 root secondary
```

В данном примере sw1 является первым корневым для всех виртуальных локальных сетей (vlans), а sw2 вторым корневым для всех виртуальных локальных сетей нашей сети.

Данная команда показывает, что данный коммутатор является корневым для vlan 9

```
sw1#show spanning-tree vlan 9
VLAN0009
Spanning tree enabled protocol rstp
Root ID Priority 9
Address 001b.544e.3280
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Bridge ID Priority 9 (priority 0 sys-id-ext 9)
Address 001b.544e.3280
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300
Interface Role Sts Cost Prio.Nbr Type
— – – – – –
Gi1/0/6 Desg FWD 4 128.6 P2p
Gi1/0/7 Desg FWD 4 128.7 P2p
Gi1/0/8 Desg FWD 4 128.8 P2p
Gi1/0/9 Desg FWD 4 128.9 P2p
Gi1/0/10 Desg FWD 4 128.10 P2p
```

Протокол

связующего
дерева
балансировка
нагрузки
со
стоимостью
порта
(STP Load balancing with Port Cost)

Мы можем также управлять балансировкой при помощи изменения стоимости портов, по умолчанию стоимость гигабитного порта 4, с помощь команды показанной ниже можно изменить её как в большую, так и в меньшую сторону:

sw1(config)#interface Gi0/1
sw1(config-if)#spanning-tree cost <1-65535>

При назначении стоимости равной 1 данный порт будет корневым для коммутатора доступа:

Проверка осуществляется командой:

Show spanning-tree vlan <vlan number>

Протокол связующего дерева балансировка нагрузки с

приоритетом порта (STP Load balancing with Port Priority)
Также возможно изменение роли порта при помощи изменения приоритета:
sw1(config)#interface Gi0/1
sw1(config-if)#spanning-tree port-priority <0-255>
Проверка осуществляется командой:
sw1#Show spanning-tree vlan <vlan number>

Множественный протокол связующего дерева MST (802.1s)

Данный протокол также как и 802.1w достаточно быстрый и используется при очень большом количестве vlan. Настраивается:

```
sw1(config)#spanning-tree mode mst
sw1(config)#spanning-tree mst configuration
sw1(config-mst)#name MYVLAN
sw1(config-mst)# revision 1
sw1(config-mst)#instance 1 vlan 10, 11, 12, 13, 14, 15
sw1(config-mst)#instance 2 vlan 16, 17, 18, 19, 20, 21
sw2(config)#spanning-tree mode mst
sw2(config)# spanning-tree mst configuration
sw2(config-mst)#name MYVLAN
sw2(config-mst)#revision 1
sw2(config-mst)#instance 1 vlan 10, 11, 12, 13, 14, 15
sw2(config-mst)#instance 2 vlan 16, 17, 18, 19, 20, 21
sw2(config)#spanning-tree mst 2 root primary
```

Последней строкой задано, что второй коммутатор является корневым для 2 инстанции:

```
sw3(config)#spanning-tree mode mst
sw3(config)#spanning-tree mst configuration
sw3(config-mst)#name MYVLAN
sw3(config-mst)#revision 1
sw3(config-mst)#instance 1 vlan 10, 11, 12, 13, 14, 15
sw3(config-mst)#instance 2 vlan 16, 17, 18, 19, 20, 21
sw3(config)#spanning-tree mst 1 root primary
```

Последней строкой задано, что третий является корневым для первой инстанции:

```
sw4(config)#spanning-tree mode mst
sw4(config)#spanning-tree mst configuration
sw4(config-mst)#name MYVLAN
sw4(config-mst)#revision 1
sw4(config-mst)#instance 1 vlan 10, 11, 12, 13, 14, 15
sw4(config-mst)#instance 2 vlan 16, 17, 18, 19, 20, 21
```

Проверка осуществляется командой:

```
show spanning-tree mst configuration
show spanning-tree mst 1
```

Множественный протокол связующего дерева балансировка нагрузки со стоимостью порта (MST Load balancing with Port Cost)

sw1(config)#interface Gi0/1
sw1(config-if)#spanning-tree mst 1 cost <1-65535>
Проверка осуществляется командой:
sw1#show spanning-tree mst 1

Множественный протокол связующего дерева балансировка нагрузки с приоритетом порта (MST Load balancing with Port Priority)

sw1(config)#interface Gi0/1
sw1(config-if)#spanning-tree mst 1 port-priority <0-255>
Проверка осуществляется командой:
sw1#show spanning-tree mst 1
Подводим итог:
sw1#conf t
sw1(config)#spanning-tree mode rapid-pvst
sw1(config)# spanning-tree vlan 1-4094 root primary
sw1(config)#end
sw1#wr
sw2#conf t
sw2(config)# spanning-tree mode rapid-pvst
sw2(config)# spanning-tree vlan 1-4094 root secondary
sw2(config)#end
sw2#wr

Мы сделали первый коммутатор корневым для всех виртуальных сетей, а второй коммутатор, вторым корневым.

Проверка осуществляется командой:
sw1#show spanning-tree vlan «номер vlan»

Утилиты Протокола связующего дерева STP
Быстрый порт (Portfast)

Данная утилита STP позволяет порту пропустить состояния listening и learning и сразу перейти в состояние forwarding. Она используется только на портах доступа. При её включении поступает предупреждение, что к данному порту нельзя подключать коммутаторы, а только хосты.

Настраивается двумя способами:

В первом варианте вводиться одной строкой и применяется ко всем портам доступа, показано ниже:

sw1(config)#spanning-tree portfast default

Проверка осуществляется командой:

sw1#show spanning-tree summary

Switch is in rapid-pvst mode

Root bridge for: none

Extended system ID is enabled

Portfast Default is enabled

PortFast BPDU Guard Default is enabled

Portfast BPDU Filter Default is disabled

Loopguard Default is disabled

EtherChannel misconfig guard is enabled

UplinkFast is disabled

BackboneFast is disabled

Configured Pathcost method used is short

Во втором варианте и этот вариант более рекомендуем, настраивается на каждом интерфейсе, показано ниже:

sw1(config)#interface FastEthernet0/1

sw1(config-if)#switchport access vlan 9

sw1(config-if)#switchport mode access

sw1(config-if)#spanning-tree portfast

Отключается на интерфейсе командой:

sw1(config-if)#spanning-tree portfast disable

Проверка осуществляется командой:

sw1#show spanning-tree interface FastEthernet 0/1 portfast

VLAN0009 enabled

Или в развернутом варианте:

sw1#show spanning-tree interface FastEthernet 0/1 detail

Port 3 (FastEthernet0/1) of VLAN0016 is designated forwarding

Port path cost 19, Port priority 128, Port Identifier 128.3.

Designated root has priority 16, address 001b.544e.3280

Designated bridge has priority 32784, address 001b.2b24.2f00

Designated port id is 128.3, designated path cost 4

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

Number of transitions to forwarding state: 1

The port is in the portfast mode

Link type is point-to-point by default

Bpdu guard is enabled

Loop guard is enabled by default on the port

BPDU: sent 33130, received 0

Защита

от
BPDU
пакетов
(Bpduguard)

Данная утилита используется на уровне доступа, она отключает интерфейс, переходит в состояние err-disable, при приходе на него BPDU пакета, используется вместе с portfast, чтобы после её срабатывания включить интерфейс, надо дать на заблокированном интерфейсе команду shutdown после этого набрать no shutdown.

В первом варианте вводиться одной строкой и применяется ко всем портам доступа, показано ниже:

sw1(config)#spanning-tree portfast default
sw1(config)#spanning-tree portfast bpduguard default
Проверка осуществляется командой:
sw1#show spanning-tree summary
Switch is in rapid-pvst mode
Root bridge for: VLAN0001, VLAN0116, VLAN0120
Extended system ID is enabled
Portfast Default is enabled
PortFast BPDU Guard Default is enabled
Portfast BPDU Filter Default is disabled
Loopguard Default is enabled
EtherChannel misconfig guard is enabled
UplinkFast is disabled
BackboneFast is disabled
Configured Pathcost method used is short
— часть информации удалена –

Во втором варианте, настраивается на каждом интерфейсе, и мы используем этот вариант, применение показано ниже:

sw1(config)#interface FastEthernet0/1
sw1(config-if)#spanning-tree bpduguard enable
Отключаем командой показанной ниже.
sw1(config-if)#spanning-tree bpduguard disable
Проверка осуществляется командой:
sw1#show spanning-tree interface FastEthernet 0/1 detail
Port 1 (FastEthernet0/1) of VLAN0009 is designated forwarding
Port path cost 19, Port priority 128, Port Identifier 128.1.
Designated root has priority 9, address 001b.544e.3280
Designated bridge has priority 32777, address 001b.54cb.e580
Designated port id is 128.1, designated path cost 4
Timers: message age 0, forward delay 0, hold 0
Number of transitions to forwarding state: 1
The port is in the portfast mode
Link type is point-to-point by default
Bpdu guard is enabled
Loop guard is enabled by default on the port
BPDU: sent 167665, received 0

Фильтр

BPDU
пакетов
(Bpdufilter)

Данная утилита предназначена, для фильтрации BPDU пакетов, она не пропускает чужой и не отправляет свой BPDU пакет и при этом не отключает интерфейс, к примеру, наш коммутатор стоит против коммутатора нашего провайдера, чтобы не пропускать его BPDU пакеты мы должны установить данную утилиту на интерфейс, обращенный к провайдеру.

Мы можем указать данную команду одной строкой для всех портов portfast:

sw1(config)#spanning-tree portfast default
sw1(config)#spanning-tree portfast bpdufilter default

Проверка осуществляется командой:

sw1#show spanning-tree summary
Switch is in rapid-pvst mode
Root bridge for: VLAN0001, VLAN0116, VLAN0120
Extended system ID is enabled
Portfast Default is enabled
PortFast BPDU Guard Default is disabled
Portfast BPDU Filter Default is enabled
Loopguard Default is enabled
EtherChannel misconfig guard is enabled
UplinkFast is disabled
BackboneFast is disabled
Configured Pathcost method used is short
— часть информации удалена –

Настраивается на определенном интерфейсе, применение показано ниже:

sw1(config)#interface FastEthernet0/1
sw1(config-if)#spanning-tree bpdufilter enable

Следует заметить, что не стоит использовать данную утилиту вместе с утилитой bpduguard.

Защита коневого коммутатора (Guard root)

Данная утилита позволяет гарантировать не избрание корневым определенного коммутатора, но для её использования обязательно требуется, чтобы до её включения мы избрали коммутатор, который будет у нас корневым и только после этого мы прописываем на интерфейсах в сторону не корневого коммутатора данную команду:

sw1(config)#interface FastEthernet0/24

sw1(config-if)#spanning-tree guard root

Проверка осуществляется командой:

sw1#show spanning-tree inconsistentports

Защита

от
петель
(Guard loop)

Данная утилита обеспечивает дополнительную защиту против образования петель, для предотвращения STP петель за счет однонаправленной связи.

Работает подобно UDLD, но вместо этого использует BDPU keepalive для определения однонаправленного движения. Заблокированные порты будут переведены в состояние LOOP_INCONSISTANT_STATE, чтобы избежать петель.

Глобально задается командой показанной ниже:

```
sw1(config)#spanning-tree loopguard default
```

Проверка осуществляется командой:

```
sw1#show spanning-tree summary
Switch is in pvst mode
Root bridge for: none
EtherChannel misconfig guard is enabled
Extended system ID is disabled
Portfast Default is disabled
PortFast BPDU Guard Default is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default is enabled
UplinkFast is disabled
BackboneFast is disabled
Pathcost method used is short
— часть информации удалена –
```

На отдельном интерфейсе задается командой, показанной ниже:

```
sw1(config)#interface FastEthernet0/24
sw1(config-if)#spanning-tree guard loop
```

Протокол обнаружения однонаправленной связи UniDirectional Link Detection (UDLD)

Протокол обнаружения однонаправленной связи (UDLD), является протоколом 2 уровня, отслеживает физическую конфигурацию кабелей и обнаруживает однонаправленные соединения и отключает порт. Данные соединения могут быть причиной петель в коммутации, образовывать черные дыры и недетерминированных перенаправлении. Чтобы включить интерфейс, после его отключения, необходимо на интерфейсе выполнить команду shutdown, а потом no shutdown.

Настраивается на интерфейсе:

```
sw1#conf t
sw1(config)# interface range fa0/19 – 20
```

Для медной пары:

```
sw1(config-if)#udld aggressive
```

Для оптического кабеля:

```
sw1(config-if)#udld
sw1(config-if)#end
sw1#wr
```

Проверка осуществляется командой:

```
sw1# show udld
```

Туннель через коммутаторы (802.1q Tunneling)

Туннель через коммутаторы 802.1q Tunneling, имеем 2 маршрутизатора их надо соединить туннелем через коммутаторы, следует отметить, что между коммутаторами есть магистральное соединение и на них прописаны vlan, настройка приводиться ниже:

```
r1(config)#interface f0/0
r1(config-if)#no shutdown
r1(config-if)#interface f0/0.10
r1(config-if)#encapsulation dot1Q 10
r1(config-if)#ip address 10.0.0.1 255.255.255.0
r1(config-if)#interface f0/0.20
r1(config-if)#encapsulation dot1Q 20
r1(config-if)#ip address 20.0.0.1 255.255.255.0
r2(config)#interface f0/0
r2(config-if)#no shutdown
r2(config-if)#interface f0/0.10
r2(config-if)#encapsulation dot1Q 10
r2(config-if)#ip address 10.0.0.2 255.255.255.0
r2(config-if)#interface f0/0.20
r2(config-if)#encapsulation dot1Q 20
r2(config-if)#ip address 20.0.0.2 255.255.255.0
sw1(config)#system mtu 1504
```

Данный интерфейс смотрит на маршрутизатор r1

```
sw1(config)#interface f0/1
sw1(config-if)#switchport access vlan 200
sw1(config-if)#switchport mode dot1q-tunnel
sw1(config-if)#l2protocol-tunnel cdp
sw1(config-if)#no cdp enable
sw1(config-if)#interface f0/19
sw1(config-if)#switchport trunk encapsulation dot1q
sw1(config-if)#switchport mode trunk
sw2(config)#system mtu 1504
```

Данный интерфейс смотрит на маршрутизатор r2

```
sw2(config)#interface f0/2
sw2(config-if)#switchport access vlan 200
sw2(config-if)#switchport mode dot1q-tunnel
sw2(config-if)#l2protocol-tunnel cdp
sw2(config-if)#no cdp enable
sw2(config-if)#interface f0/19
sw2(config-if)#switchport trunk encapsulation dot1q
sw2(config-if)#switchport mode trunk
```

Проверяем командой show cdp neighbor и ping на первом и втором маршрутизаторе.

Частные виртуальные локальные сети (Private VLANs)

Частные виртуальные локальные сети используются, когда нужно, чтобы один хост или несколько хостов не имели доступа к общей сети. Соответственно существуют три типа таких портов изолированные (isolated),сообщество (community) и прослушивающий (promiscuous), прослушивающий (promiscuous) порт может общаться со всеми видами портов в пределах частной виртуальной локальной сети. Также через него частные порты могут обмениваться между собой информацией. Варианты настройки приведены ниже:

Настройка изолированной виртуальной локальной сети (isolated vlan)

Обязательно переводим коммутатор в прозрачный режим (transparent) и после этого создаем изолированию виртуальную локальную сеть и первую виртуальную локальную сеть, только одна изолированная сеть может быть привязана к первой сети, к которой она будет привязана:

```
sw2(config)#vtp transparent
sw2(config-vlan)#vlan 201
sw2(config-vlan)#private-vlan isolated
sw2(config-vlan)#vlan 100
sw2(config-vlan)#private-vlan primary
sw2(config-vlan)#private-vlan association 201
sw2(config-vlan)#end
sw2#wr
```

Настраиваем порт, к которому будет подключен изолированный хост:

```
sw2(config)#interface f0/1
sw2(config-if)#switchport mode private-vlan host
sw2(config-if)#switchport private-vlan host-association 100 201
```

Проверка осуществляется командой:

```
sw2#show vlan private-vlan
Primary Secondary Type Ports
— – – –
100 201 isolated Fa0/1
```

Также посмотреть результат можно и этой командой

```
sw2#show interface f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: private-vlan host
Operational Mode: private-vlan host
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: 100 (VLAN00100) 201 (VLAN00201)
```

Конец ознакомительного фрагмента.