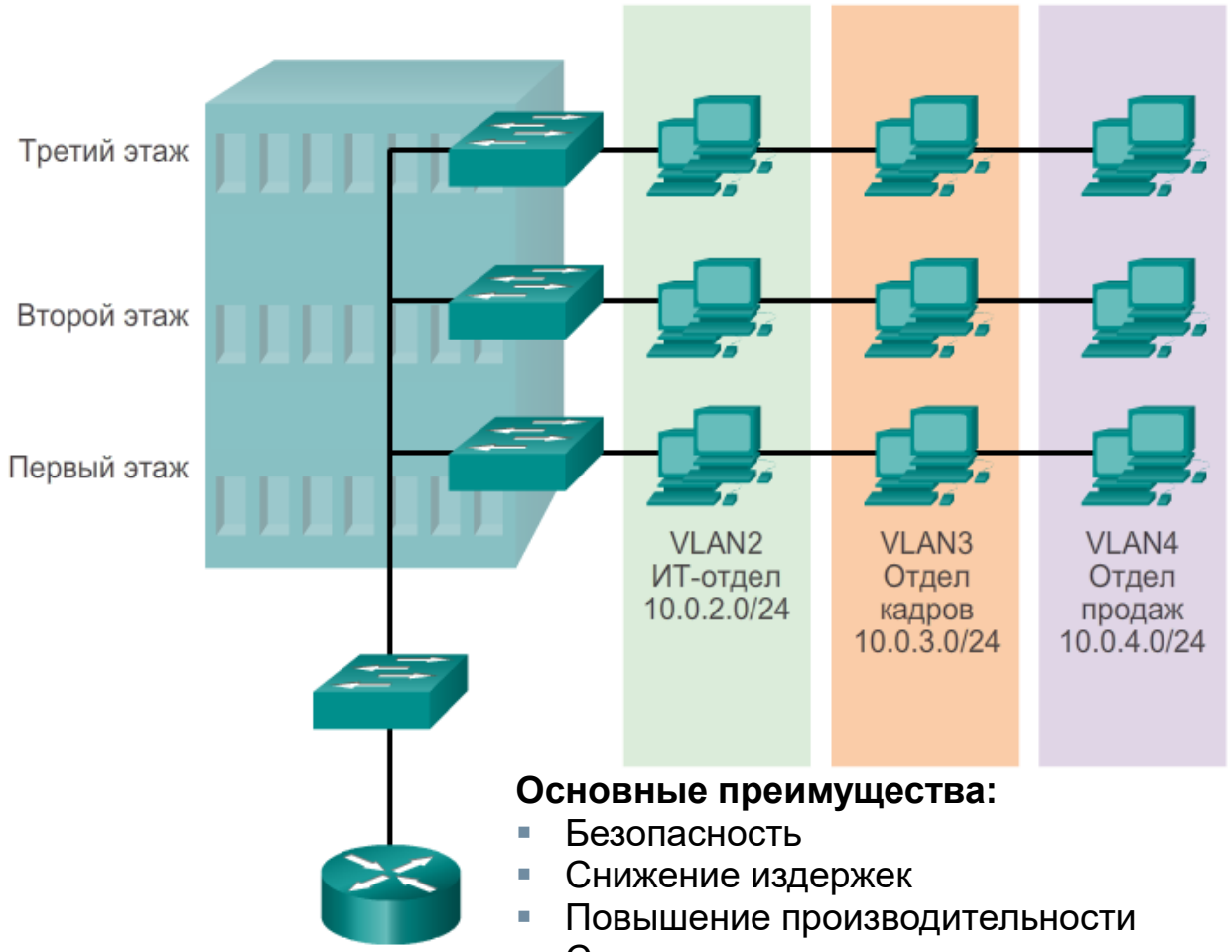
МОСКОВСКИЙ АВИАЦИОННЫЙ ИНСТИТУТ | НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

Виртуальные локальные сети VLAN

Коммутация, маршрутизация и беспроводная связь

Определение VLAN



Основные преимущества:

- Безопасность
- Снижение издержек
- Повышение производительности
- Сокращение количества доменов широковещательной рассылки
- Упрощенная форма управления проектами и приложениями

Основные понятия:

- VLAN (виртуальная LAN) — это результат логического разделения сети уровня 2.
- Можно создать несколько разделов, позволяющих сосуществовать нескольким VLAN.
- Каждая VLAN является широковещательным доменом и в большинстве случаев имеет собственную IP-сеть.
- Сети VLAN взаимно изолированы, и пакеты между ними могут передаваться только через маршрутизатор.
- Группы узлов внутри VLAN не знают о существовании VLAN.
- Процедура разделения сети уровня 2 также задействует устройство уровня 2, чаще всего коммутатор.

Краткий обзор сетей VLAN

Типы сетей VLAN

- VLAN передачи данных настроена специально для передачи трафика, генерируемого пользователем.
- VLAN по умолчанию. Все порты коммутатора становятся частью VLAN по умолчанию после первоначальной загрузки коммутатора. Порты коммутатора, находящиеся в сети VLAN по умолчанию, являются частью одного широковещательного домена. Сетью VLAN по умолчанию для коммутаторов Cisco установлена VLAN 1.
- Native VLAN назначена транковому порту 802.1Q. Транковые порты — это каналы между коммутаторами, которые поддерживают передачу трафика, связанного с более чем одной сетью VLAN. Рекомендуется настроить native VLAN как неиспользуемую VLAN, отличающуюся от сети VLAN 1 и других VLAN.
- VLAN управления настроена для доступа к функциям управления коммутатора. Сеть VLAN 1 по умолчанию является управляющей VLAN. Для создания управляющей VLAN интерфейсу SVI коммутатора данной VLAN назначаются IP-адрес и маска подсети.

Краткий обзор сетей VLAN

Типы сетей VLAN

VLAN 1

```
Switch# show vlan brief

VLAN Name                Status    Ports
---- ------------------- --------- -----------------------
1    default             active    Fa0/1,  Fa0/2,  Fa0/3,  Fa0/4
                                   Fa0/5,  Fa0/6,  Fa0/7,  Fa0/8
                                   Fa0/9,  Fa0/10, Fa0/11, Fa0/12
                                   Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                   Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                   Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                   Gi0/1,  Gi0/2
1002 fddi-default        act/unsup
1003 token-ring-default  act/unsup
1004 fddinet-default     act/unsup
1005 trnet-default       act/unsup
```

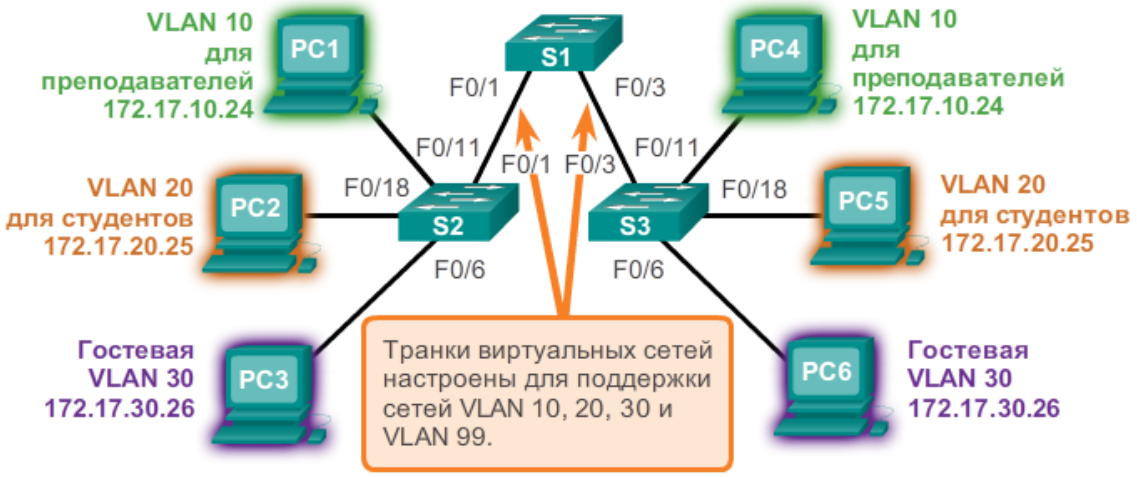
- Все порты назначены сети VLAN 1 для пересылки данных по умолчанию.
- Сетью native VLAN по умолчанию является сеть VLAN 1.
- Сетью управления VLAN по умолчанию является сеть VLAN 1.
- VLAN 1 нельзя переименовывать или удалять.

VLAN в среде со множеством коммутаторов

Транковые каналы VLAN

VLAN 10 для преподавателей и сотрудников — 172.17.10.0/24
VLAN 20 для учащихся — 172.17.20.0/24
Гостевая VLAN 30 — 172.17.30.0/24
VLAN 99 сеть native и управляющая сеть— 172.17.99.0/24.

Порты F0/1-5 — это транковые интерфейсы 802.1Q, настроенные с сетью native VLAN 99.
Порты F0/11-17 принадлежат сети VLAN 10.
Порты F0/18-24 принадлежат сети VLAN 20.
Порты F0/6-10 принадлежат сети VLAN 30.

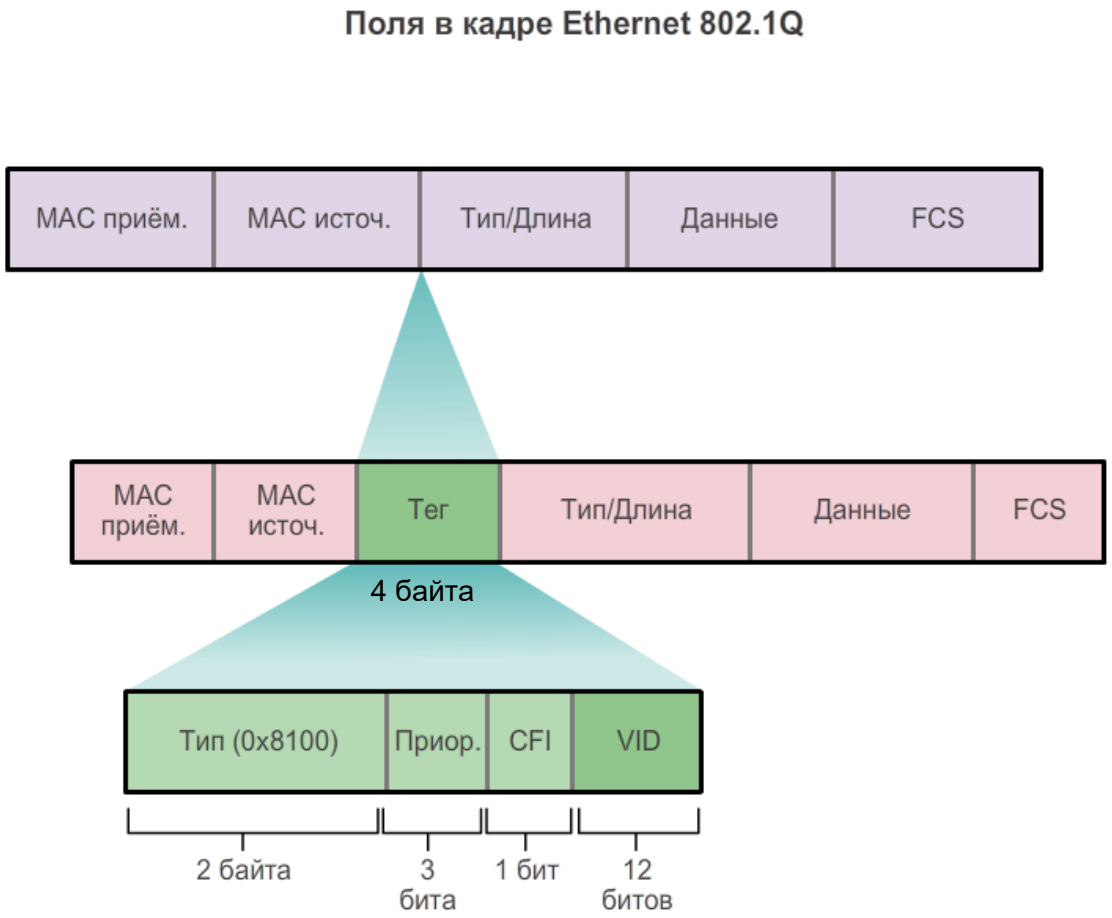


- Транковый канал VLAN поддерживает работу более одной VLAN.
- Обычно транковый канал устанавливается **между коммутаторами** для возможности связи между устройствами одной VLAN, даже если физически они подключены к разным коммутаторам.
- Транковый канал VLAN не принадлежит ни одной VLAN.
- ОС Cisco IOS поддерживает известный транковый протокол VLAN — стандарт IEEE802.1q.

Присвоение меток кадрам Ethernet для идентификации VLAN

- Присвоение **меток кадрам** используется в целях правильной **передачи множества кадров VLAN через транковый канал**.
- Метки присваиваются кадрам **коммутаторами** для определения той VLAN, которой эти кадры принадлежат. Существуют различные протоколы распределения меток (или тегирования), среди которых одним из наиболее распространённых протоколов является стандарт IEEE 802.1q.
- Метка VLAN **присваивается** кадру коммутатором **до перемещения кадра по транковому каналу** и **удаляется до пересылки кадра через нетранковый порт**.
- Кадры с соответствующей меткой могут пересекать **любое количество коммутаторов через транковый канал**, и всё равно будут направлены в правильную VLAN назначения.
- Кадру, принадлежащему **native VLAN**, не присваивается метка. Если нет связанных с native VLAN портов и никаких других транковых каналов, не отмеченный меткой кадр отбрасывается.

Присвоение меток кадрам Ethernet для идентификации VLAN



Тип — это 2-байтовое значение, которое называется значением идентификатора протокола тегирования (TPID). Значение для Ethernet имеет вид шестнадцатеричного числа ***0x8100***.

Приоритет пользователя — это 3-битовое значение, которое поддерживает реализацию уровня или сервиса.

Идентификатор канонического формата (CFI) — это 1-битовый идентификатор, который обеспечивает передачу кадров Token Ring по каналам Ethernet.

VLAN-идентификатор (VID) — это 12-битный идентификационный **номер VLAN**, который поддерживает до ***4096*** идентификаторов VLAN.

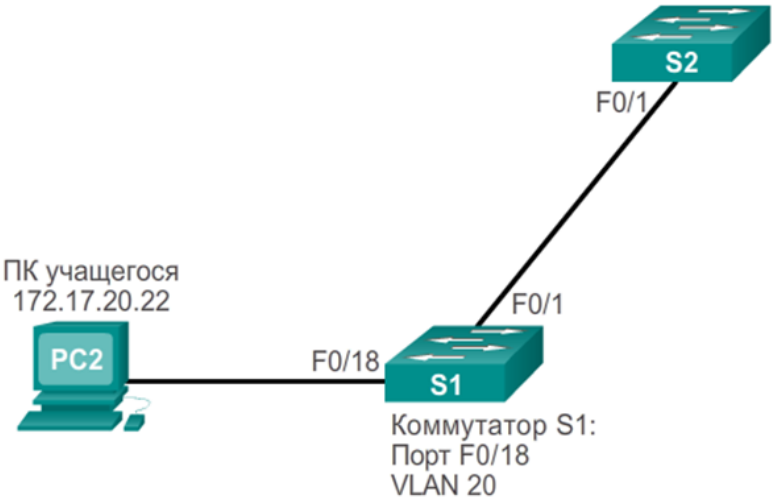
Диапазоны VLAN на коммутаторах Catalyst

- Коммутаторы Catalyst серий 2960 и 3560 способны поддерживать более 4 000 сетей VLAN.
- Данные сети VLAN можно разделить на две категории.
- К первой категории относятся сети VLAN стандартного диапазона.
  - Сюда относятся сети VLAN с номерами от 1 до 1 005.
  - Конфигурации хранятся в файле флеш-памяти vlan.dat.
  - Протокол VTP, служащий для обмена информацией о VLAN, имеющихся на выбранном транковом порту, может узнавать и хранить только сети VLAN стандартного диапазона.
- Вторая категория — это сети VLAN расширенного диапазона.
  - К данным сетям VLAN относятся сети с номерами от 1 006 до 4 096.
  - Конфигурации хранятся в энергонезависимом ОЗУ (NVRAM) в файле текущей конфигурации.
  - Протокол VTP не распознаёт сети VLAN расширенного диапазона.

Создание VLAN

Команды коммутатора Cisco под управлением ОС IOS	
Войдите в режим глобальной конфигурации.	`S1# configure terminal`
Создайте сеть VLAN с допустимым номером идентификатора.	`S1(config)# vlan vlan-id`
Укажите уникальное имя для идентификации сети VLAN.	`S1(config-vlan)# name vlan-name`
Вернитесь в привилегированный режим.	`S1(config-vlan)# end`

```
S1# configure terminal
S1(config)# vlan 20
S1(config-vlan)# name student
S1(config-vlan)# end
```



Назначение VLAN

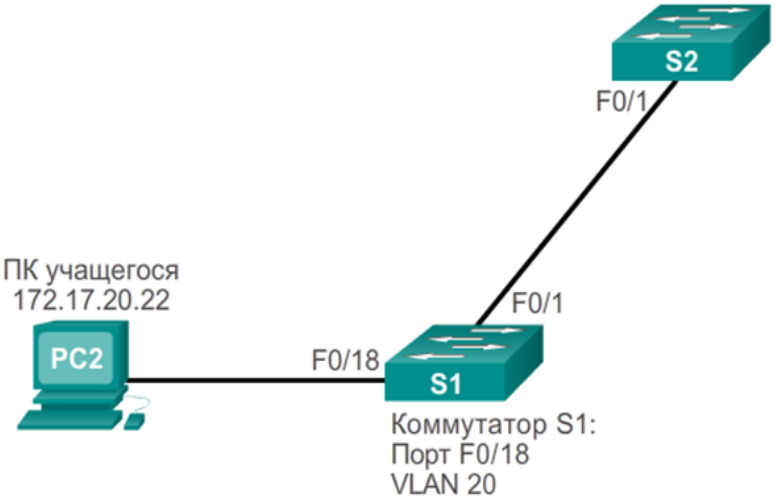
Назначение портов сетям VLAN

Команды коммутатора Cisco под управлением ОС IOS	
Войдите в режим глобальной конфигурации.	`S1# configure terminal`
Войдите в режим конфигурации интерфейса для SVI.	`S1(config)# interface` *interface_id*
Переведите порт в режим доступа.	`S1(config-if)# switchport mode access`
Назначьте порт сети VLAN.	`S1(config-if)# switchport access vlan` *vlan_id*
Вернитесь в привилегированный режим.	`S1(config-if)# end`

```
s1# configure terminal
s1(config)# interface F0/18
s1(config-if)# switchport mode access
s1(config-if)# switchport access vlan 20
s1(config-if)# end
```

```
S1# show vlan brief

VLAN Name                Status    Ports
---- ----------------- ------- -------------------------------
1    default             active  Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                 Fa0/17, Fa0/19, Fa0/20, Fa0/21
                                 Fa0/22, Fa0/23, Fa0/24
                                 Gi0/1, Gi0/2
20   student             active    Fa0/18
1002 fddi-default        act/unsup
1003 token-ring-default  act/unsup
1004 fddinet-default     act/unsup
1005 trnet-default       act/unsup
S1#
```



Назначение VLAN

Изменение принадлежности портов VLAN

```
S1(config)# int fa0/18
S1(config-if)# no switchport access vlan
S1(config-if)# end
S1# show vlan brief

VLAN Name                Status    Ports
---- ----------------- ------- -------------------------------
1    default             active  Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                 Gi0/1, Gi0/2
20   student             active
1002 fddi-default        act/unsup
1003 token-ring-default  act/unsup
1004 fddinet-default     act/unsup
1005 trnet-default       act/unsup
S1#
```

```
S1# conf t
S1(config)# no vlan 20
S1(config)# end
S1#
S1# sh vlan brief

VLAN Name                 Status    Ports
---- ----------------     --------- -------------------------------
1    default              active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                    Fa0/9, Fa0/10, Fa0/12, Fa0/13
                                    Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                    Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                    Fa0/22, Fa0/23, Fa0/24, Gi0/1
                                    Gi0/2
1002 fddi-default         act/unsup
1003 token-ring-default   act/unsup
```

```
S1# config t
S1(config)# int fa0/11
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 20
S1(config-if)# end
S1#
S1# show vlan brief

VLAN Name                 Status     Ports
---- -------------------- ---------- -------------------------------
1    default              active     Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                     Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                     Fa0/9, Fa0/10, Fa0/12, Fa0/1
                                     Fa0/14, Fa0/15, Fa0/16, Fa0/
                                     Fa0/18, Fa0/19, Fa0/20, Fa0/
                                     Fa0/22, Fa0/23, Fa0/24, Gi0/
                                     Gi0/2
20   student              active     Fa0/11
1002 fddi-default         act/unsup
1003 token-ring-default   act/unsup
1004 fddinet-default      act/unsup
1005 trnet-default        act/unsup
S1#
```

Назначение VLAN

Проверка информации о VLAN

```
S1# show vlan name student

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------
20   student                           active    Fa0/11, Fa0/18

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
20   enet  100020     1500  -      -      -        -    -        0      0

Remote SPAN VLAN
----------------
Disabled

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------

S1# show vlan summary
Number of existing VLANs              : 7
Number of existing VTP VLANs          : 7
Number of existing extended VLANS     : 0

S1#
```

```
S1#show interfaces vlan 20
Vlan20 is up, line protocol is down
  Hardware is EtherSVI, address is 001c.57ec.0641 (bia
001c.57ec.0641)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output
drops: 0
  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
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicast)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

Настройка транковых каналов по стандарту IEEE 802.1q

Команды коммутатора Cisco под управлением ОС IOS	
Войдите в режим глобальной конфигурации.	`S1# configure terminal`
Войдите в режим конфигурации интерфейса для SVI.	`S1(config)# interface` *interface_id*
Настройте канал в качестве транкового.	`S1(config-if)# switchport mode trunk`
Укажите сеть native VLAN для транков 802.1Q без меток.	`S1(config-if)# switchport trunk native vlan` *vlan_id*
Укажите список сетей VLAN, которым разрешён доступ в транковый канал.	`S1(config-if)# switchport trunk allowed vlan` *vlan-list*
Вернитесь в привилегированный режим.	`S1(config-if)# end`

```
S1(config)# interface FastEthernet0/1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# switchport trunk allowed vlan 10,20,30
S1(config-if)# end
```

Сброс настроек транкового канала до состояния по умолчанию

```
S1(config)# interface f0/1
S1(config-if)# no switchport trunk allowed vlan
S1(config-if)# no switchport trunk native vlan
S1(config-if)# end
S1# show interfaces f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
<выходные данные опущены>
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
<выходные данные опущены>
```

Возвращение порта в режим доступа

```
S1(config)# interface f0/1
S1(config-if)# switchport mode access
S1(config-if)# end
S1# show interfaces f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
<выходные данные опущены>
```

Проверка конфигурации транкового канала

Проверка конфигурации транкового канала

```
S1(config)# interface f0/1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# end
S1# show interfaces f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (VLAN0099)
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
<выходные данные опущены>
```

Динамический протокол транковых каналов

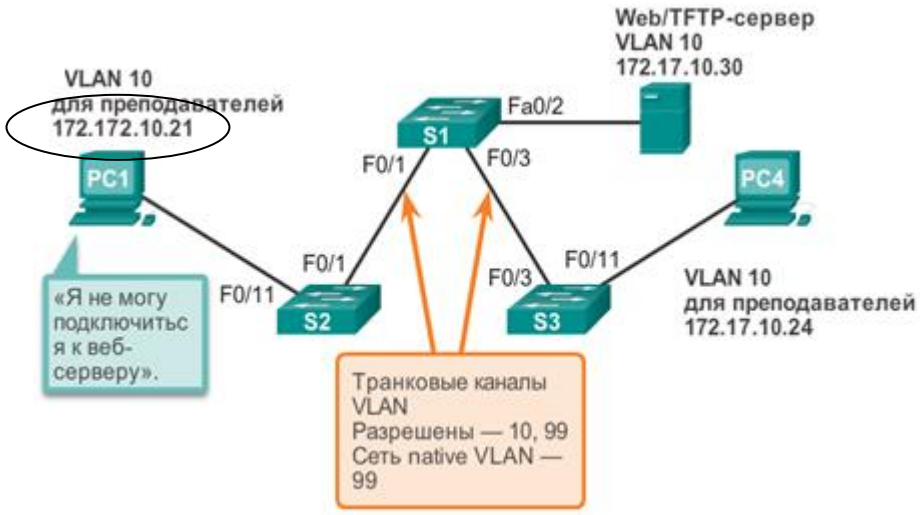
Режимы интерфейса для согласования

- Порты коммутатора можно настроить вручную для создания транковых каналов.
- Порты коммутатора также можно настроить для согласования и установления транкового канала с подключённым узлом.
- **Динамический протокол транковых каналов** (DTP) — это протокол **для управления согласованием транковых каналов**.
- DTP является собственным протоколом Cisco. Он по умолчанию доступен на коммутаторах Cisco Catalyst серии 2960 и серии 3560.
- Если порт на соседнем коммутаторе настроен в транковом режиме, поддерживающем протокол DTP, то согласованием управляет этот порт.
- По умолчанию протокол DTP на коммутаторах Cisco Catalyst 2960 и 3560 настроен с конфигурацией **dynamic auto**.
- На коммутаторах Cisco Catalyst 2960 и 3560 поддерживаются следующие транковые режимы:
  - dynamic auto (динамический автоматический)
  - dynamic desirable (динамический рекомендуемый)
  - Trunk (транк)
  - Nonegotiate (доступ)

	Динамический автоматический	Динамический рекомендуемый	Транк	Доступ
Динамический автоматический	Доступ	Транк	Транк	Доступ
Динамический рекомендуемый	Транк	Транк	Транк	Доступ
Транк	Транк	Транк	Транк	Ограниченные возможности подключения
Доступ	Доступ	Доступ	Ограниченные возможности подключения	Доступ

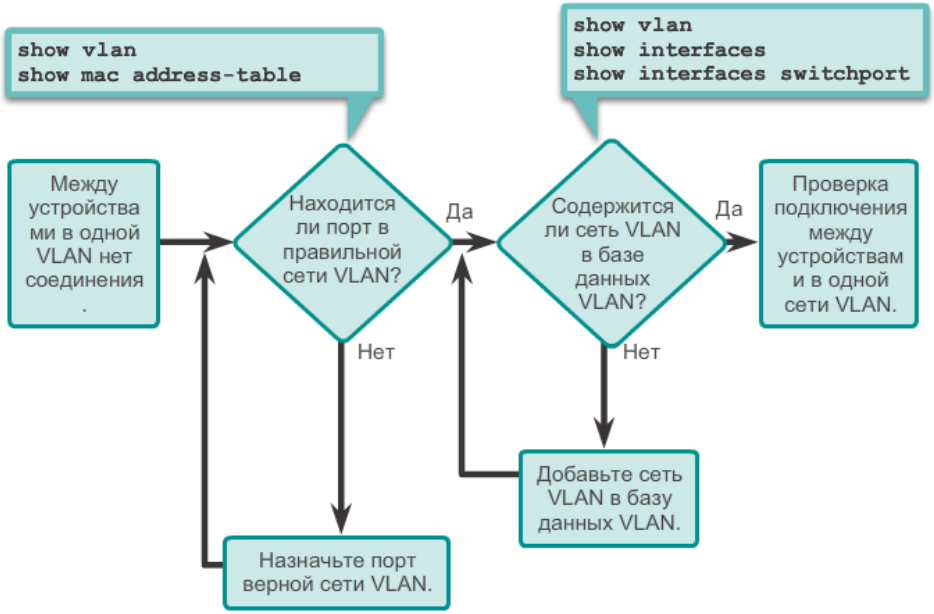
Проблемы адресации VLAN

- Настоятельно рекомендуется связывать VLAN с IP-сетью.
- Поскольку разные IP-сети поддерживают связь только через маршрутизатор, **все устройства внутри VLAN должны быть частью такой же IP-сети**, чтобы иметь возможность обмениваться информацией.
- На рисунке *PC1* не может связаться с сервером, поскольку у него *неверно настроен IP-адрес*.



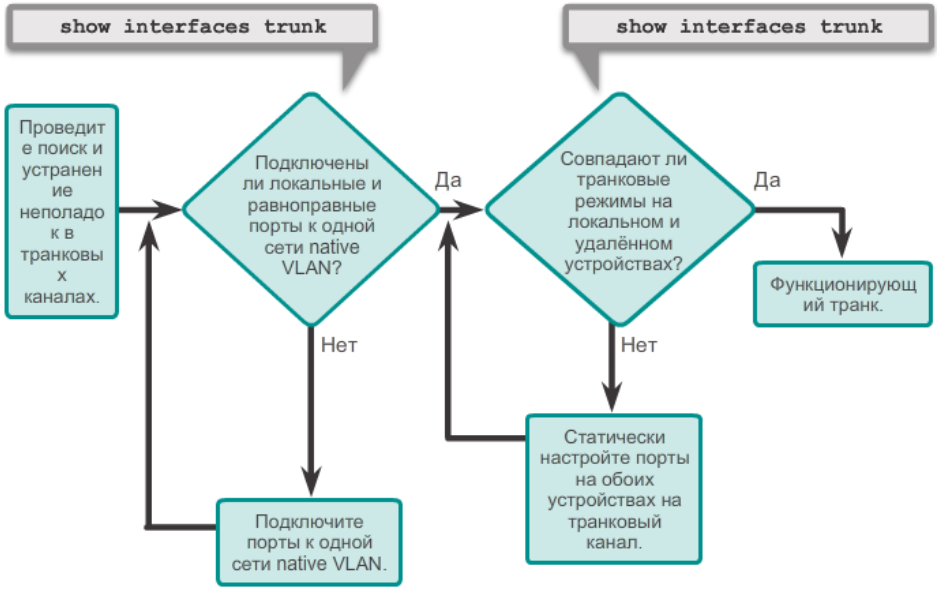
Поиск и устранение неполадок VLAN и транковых каналов

Отсутствующие VLAN



- **Наиболее распространённые ошибки конфигурации транковых каналов**:
  1. Несовпадение native VLAN;
  2. Несовпадение транковых режимов;
  3. Разрешённые VLAN на транковых каналах.
- Проверьте состояние транковых портов на коммутаторах при помощи команды **show interfaces trunk**.

- Если все причины, по которым не совпадают IP-адреса, были устранены, а устройства до сих пор не могут установить связь, проверьте, **настроена ли VLAN на коммутаторе**.
- Примените команду **switchport trunk allowed vlan** для определения, каким VLAN разрешено отправлять кадры через транковый канал.



Практические рекомендации по проектированию VLAN

Указания по проектированию VLAN

- Переместите все порты из VLAN1 и назначьте их неиспользуемой VLAN.
- Отключите все неиспользуемые порты коммутатора.
- Разделите трафик управления и трафик пользовательских данных.
- Измените VLAN управления на VLAN, отличную от VLAN1. Сделайте то же самое для native VLAN.
- Убедитесь, что к коммутатору могут подключаться для конфигурирования только устройства из VLAN управления.
- На коммутаторе должны быть разрешены только SSH-подключения.
- Отключите функцию автосогласования на транковых портах.
- Не используйте режимы **switchport mode dynamic auto** и **switchport mode dynamic desirable**.

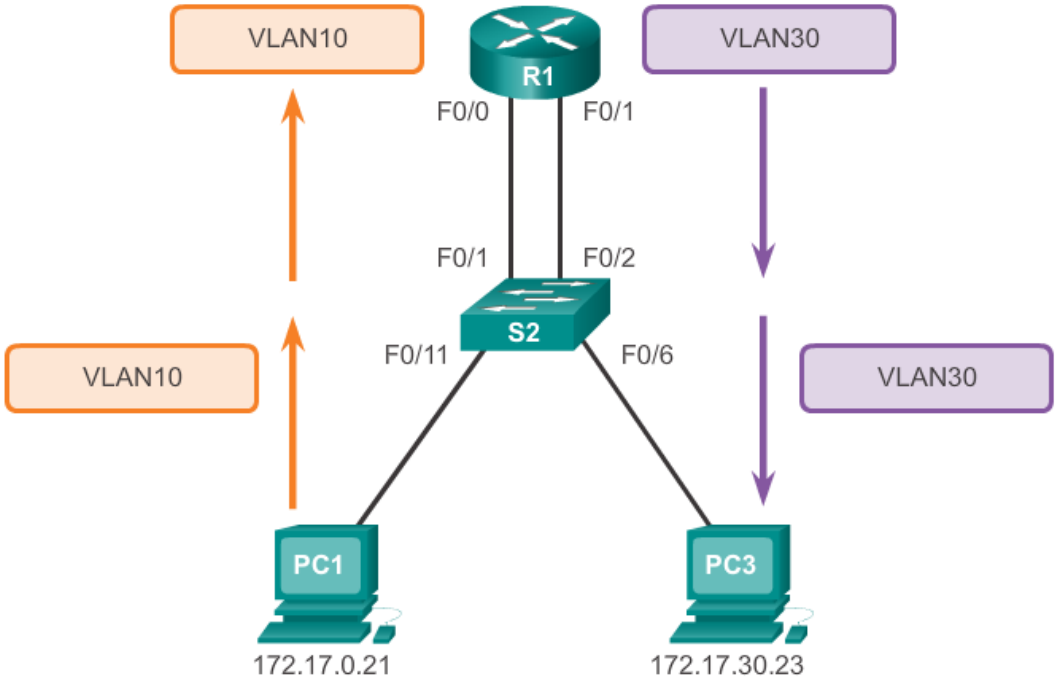
МОСКОВСКИЙ АВИАЦИОННЫЙ ИНСТИТУТ | НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

Маршрутизация между сетями VLAN

Коммутация, маршрутизация и беспроводная связь

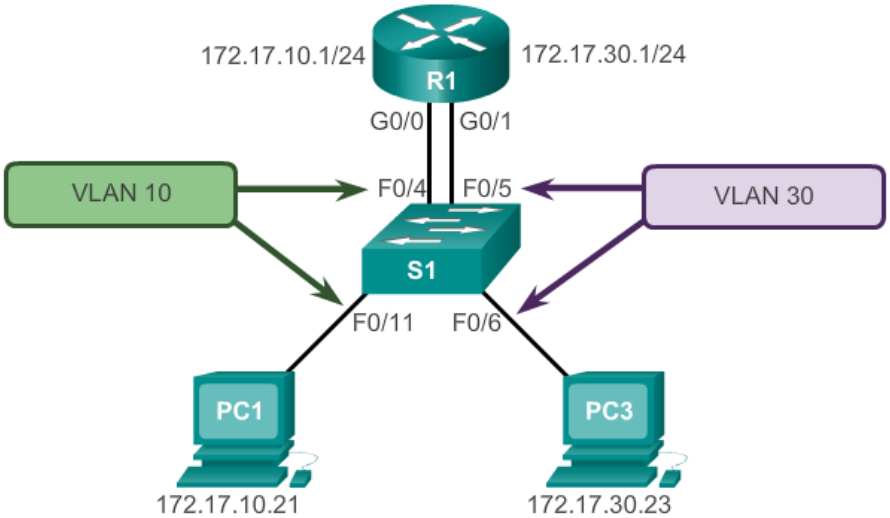
Что такое маршрутизация между VLAN

- Коммутаторы уровня 2 не могут пересылать трафик между VLAN без помощи маршрутизатора.
- Маршрутизация между VLAN — это процесс пересылки сетевого трафика из одной VLAN в другую с помощью маршрутизатора.



Устаревший метод маршрутизации между VLAN

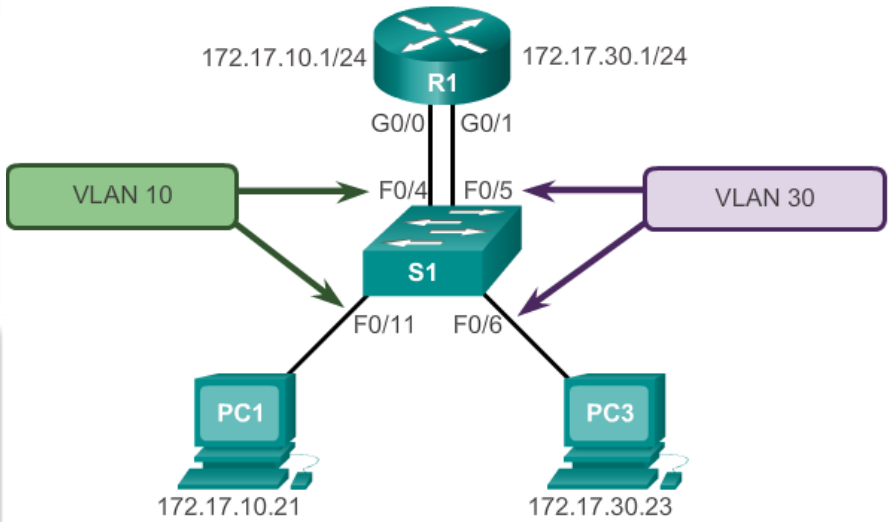
- В прошлом действующие маршрутизаторы использовались для маршрутизации между VLAN.
- Каждая VLAN была подключена к отдельному физическому интерфейсу маршрутизатора.
- Пакеты поступали на маршрутизатор через один интерфейс, маршрутизировались и покидали маршрутизатор через другой интерфейс.
- Поскольку интерфейсы маршрутизатора были подключены к VLAN и имели IP-адреса из общего с соответствующей VLAN адресного пространства, достигалась маршрутизация между VLAN.
- Это простое решение, однако едва ли имеющее возможности масштабирования. Крупные сети с большим количеством VLAN потребовали бы огромного количества интерфейсов маршрутизаторов.



Настройка маршрутизации между VLAN по устаревшему методу

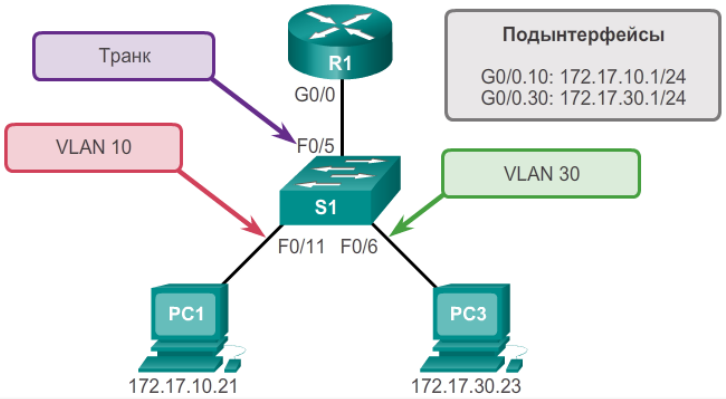
```
S1(config)# vlan 10
S1(config-vlan)# vlan 30
S1(config-vlan)# interface f0/11
S1(config-if)# switchport access vlan 10
S1(config-if)# interface f0/4
S1(config-if)# switchport access vlan 10
S1(config-if)# interface f0/6
S1(config-if)# switchport access vlan 30
S1(config-if)# interface f0/5
S1(config-if)# switchport access vlan 30
S1(config-if)# end
*Mar 20 01:22:56.751: %SYS-5-CONFIG_I: Configured from console by
console
S1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

```
R1(config)# interface g0/0
R1(config-if)# ip address 172.17.10.1 255.255.255.0
R1(config-if)# no shutdown
*Mar 20 01:42:12.951: %LINK-3-UPDOWN: Interface GigabitEthernet0/0,
changed state to up
*Mar 20 01:42:13.951: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0, changed state to up
R1(config-if)# interface g0/1
R1(config-if)# ip address 172.17.30.1 255.255.255.0
R1(config-if)# no shutdown
*Mar 20 01:42:54.951: %LINK-3-UPDOWN: Interface GigabitEthernet0/1,
changed state to up
*Mar 20 01:42:55.951: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to up
R1(config-if)# end
R1# copy running-config startup-config
```



Маршрутизация между VLAN с использованием конфигурации router-on-a-stick «маршрутизатор на палочке» (ROS)

- Один из физических интерфейсов маршрутизатора настраивается в качестве транкового порта 802.1Q. Теперь этот порт может распознавать метки VLAN.
- Затем создаются логические подынтерфейсы. По одному подынтерфейсу для каждой VLAN
- Каждый подынтерфейс настраивается с IP-адресом, полученным от той VLAN, которую он представляет.
- Участники (узлы) VLAN настраиваются для использования адреса подынтерфейса в качестве шлюза по умолчанию.
- Используется только один из физических интерфейсов маршрутизатора.




```
S1(config)# vlan 10
S1(config-vlan)# vlan 30
S1(config-vlan)# interface f0/5
S1(config-if)# switchport mode trunk
S1(config-if)# end
S1#
```

```
R1(config)# interface g0/0.10
R1(config-subif)# encapsulation dot1q 10
R1(config-subif)# ip address 172.17.10.1 255.255.255.0
R1(config-subif)# interface g0/0.30
R1(config-subif)# encapsulation dot1q 30
R1(config-subif)# ip address 172.17.30.1 255.255.255.0
R1(config)# interface g0/0
R1(config-if)# no shutdown
*Mar 20 00:20:59.299: %LINK-3-UPDOWN: Interface GigabitEthernet0/0,
 changed state to down
*Mar 20 00:21:02.919: %LINK-3-UPDOWN: Interface GigabitEthernet0/0,
 changed state to up
*Mar 20 00:21:03.919: %LINEPROTO-5-UPDOWN: Line protocol on
 changed state to down
*Mar 20 00:21:02.919: %LINK-3-UPDOWN: Interface GigabitEthernet0/0,
 changed state to up
*Mar 20 00:21:03.919: %LINEPROTO-5-UPDOWN: Line protocol on
 Interface GigabitEthernet0/0, changed state to up
```

Конфигурация ROS

Проверка подынтерфейсов и маршрутизации

```
R1# show vlans
<выходные данные опущены>
Virtual LAN ID:  10 (IEEE 802.1Q Encapsulation)

  vLAN Trunk Interface:   GigabitEthernet0/0.10

  Protocols Configured:  Address:     Received:   Transmitted:
          IP             172.17.10.1         11              18
<выходные данные опущены>
Virtual LAN ID:  30 (IEEE 802.1Q Encapsulation)

  vLAN Trunk Interface:   GigabitEthernet0/0.30

  Protocols Configured:  Address:     Received:   Transmitted:
          IP             172.17.30.1         11               8
<выходные данные опущены>
```

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP,M - mobile,
       B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF,
       IA - OSPF inter area
       N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1,
       L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default,
       U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP,
       l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

   172.17.0.0/16 is variably subnetted, 4 subnets, 2 masks
C      172.17.10.0/24 is directly connected, GigabitEthernet0/0.10
L      172.17.10.1/32 is directly connected, GigabitEthernet0/0.10
C      172.17.30.0/24 is directly connected, GigabitEthernet0/0.30
L      172.17.30.1/32 is directly connected, GigabitEthernet0/0.30
```

- Возможность доступа к устройствам в удалённых VLAN можно проверить с помощью команды **ping**. VLAN отправляет эхо-запрос ICMP на адрес назначения. Когда узел получает эхо-запрос ICMP, он отправляет эхо-ответ ICMP.
- Команда **tracert** — полезный инструмент для подтверждения существования пути между двумя устройствами.

Маршрутизация между VLAN через многоуровневый коммутатор 3 уровня

- Многоуровневые коммутаторы могут выполнять функции коммутаторов уровня 2 и уровня 3. Маршрутизаторы больше не требуются
- Каждая VLAN, настроенная на коммутаторе, представляет собой SVI (виртуальный интерфейс коммутатора).
- SVI выступают как интерфейсы уровня 3.
- Коммутатор понимает протокольные блоки данных на сетевом уровне и, следовательно, может маршрутизировать их между SVI, подобно тому как это делает маршрутизатор.
- При использовании многоуровневого коммутатора трафик маршрутизируется внутри коммутатора.
- Такое решение легко масштабируется.

МОСКОВСКИЙ АВИАЦИОННЫЙ ИНСТИТУТ | НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

Избыточность LAN

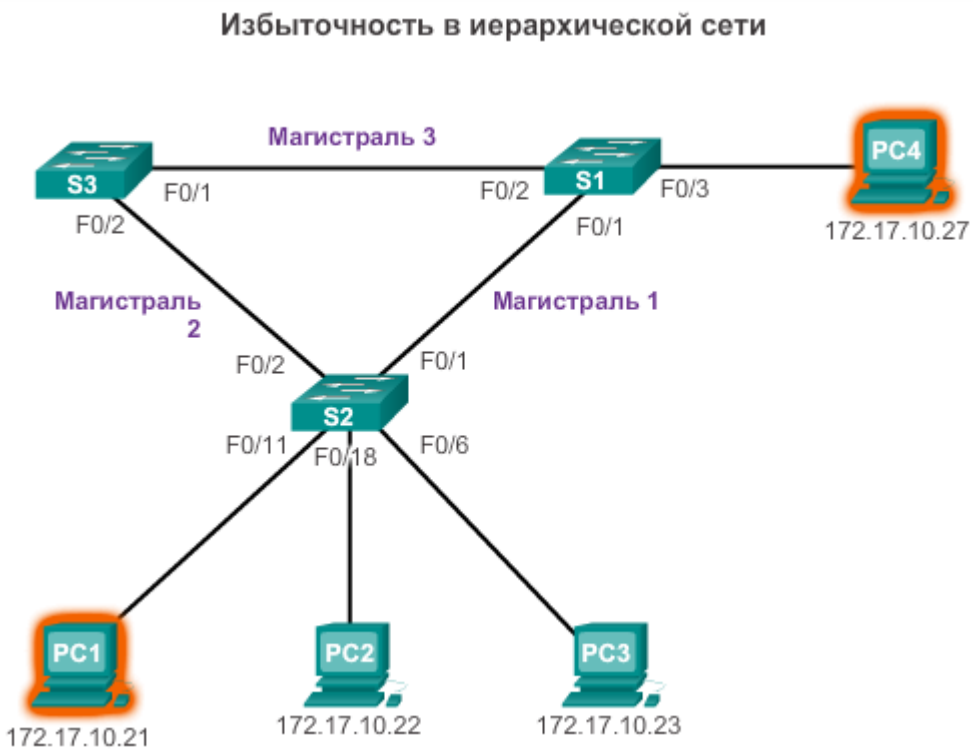
Коммутация, маршрутизация и беспроводная связь

Избыточность 1 и 2 уровней модели OSI

1. PC1 взаимодействует с PC4 через избыточную топологию сети.

2. Когда в сетевом канале между S1 и S2 происходит сбой, путь между PC1 и PC4 автоматически корректируется, чтобы компенсировать сбой, через S3.

3. Если сетевое соединение между S1 и S2 восстановлено, путь повторно корректируется для маршрутизации трафика непосредственно от S2 к S1 для его доставки на PC4.



Понятие протокола Spanning Tree

Избыточность 1 и 2 уровней модели OSI

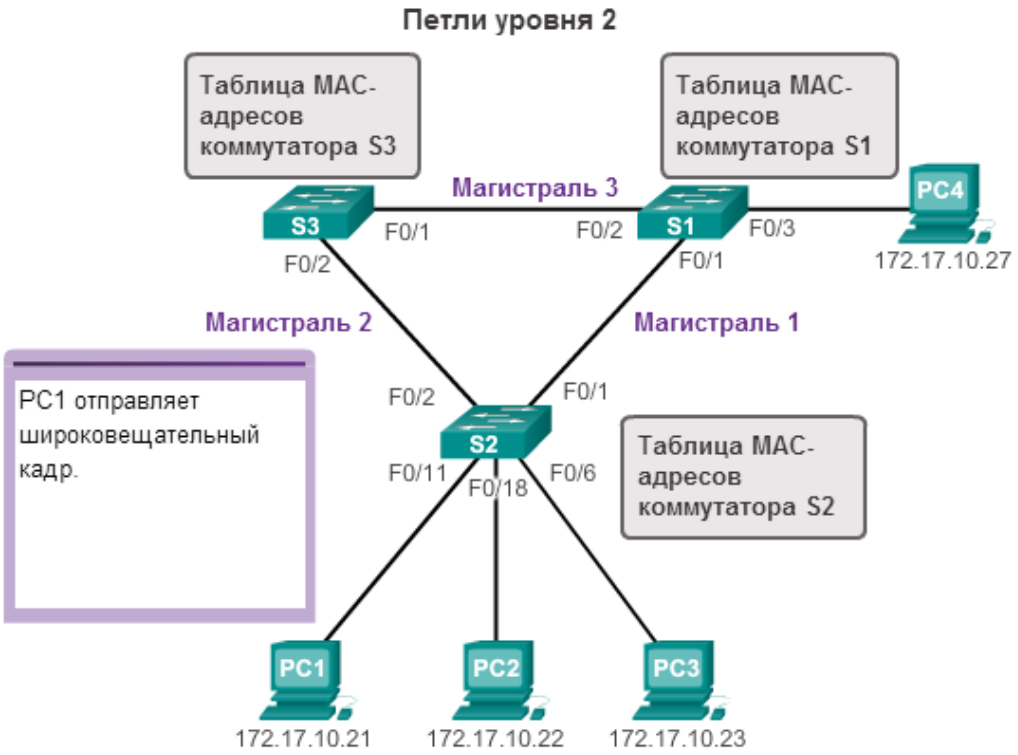
Ключевые факторы, учитываемые при реализации избыточности:

- **Нестабильность базы данных MAC-адресов**. Нестабильность содержимого таблицы MAC-адресов возникает из-за создания копий одного кадра, полученных на разных портах коммутатора. Если коммутатор использует все ресурсы для преодоления последствий нестабильности таблицы MAC-адресов, эффективность пересылки данных может быть снижена.

- **Широковещательные штормы**. Без использования надлежащего процесса предотвращения петель каждый из коммутаторов может бесконечно выполнять широковещательную рассылку. Обычно такую ситуацию называют широковещательным штормом.

- **Множественная передача кадров**. На станции назначения могут доставляться несколько копий одноадресных кадров. Многие протоколы предполагают получение только одной копии каждого передаваемого блока. Прием нескольких копий одного кадра может привести к неустранимым ошибкам.

Нестабильность базы данных MAC-адресов



1. PC1 отправляет широковещательный кадр на S2. S2 принимает широковещательный кадр и обновляет свою таблицу MAC-адресов.

2. Поскольку этот кадр — широковещательный, S2 пересылает кадр из всех портов, включая Магистраль 1 и Магистраль 2. Когда широковещательный кадр поступает на S3 и S1, их таблицы MAC-адресов обновляются относительно PC1.

3. Поскольку этот кадр является широковещательным, S3 и S1 пересылают кадр из всех портов, за исключением исходного входного порта. S3 отправляет широковещательный кадр с PC1 на S1. S1 отправляет широковещательный кадр с PC1 на S3. Все коммутаторы обновляют свою таблицу MAC-адресов с учетом неправильного порта PC1.

4. Все коммутаторы снова пересылают широковещательный кадр из всех портов, за исключением входного порта. Это приводит к тому, что оба коммутатора пересылают кадр на S2.

5. Когда S2 получает широковещательные кадры от S3 и S1, таблица MAC-адресов снова обновляется, в этот раз с учетом последней записи, полученной от двух других коммутаторов.

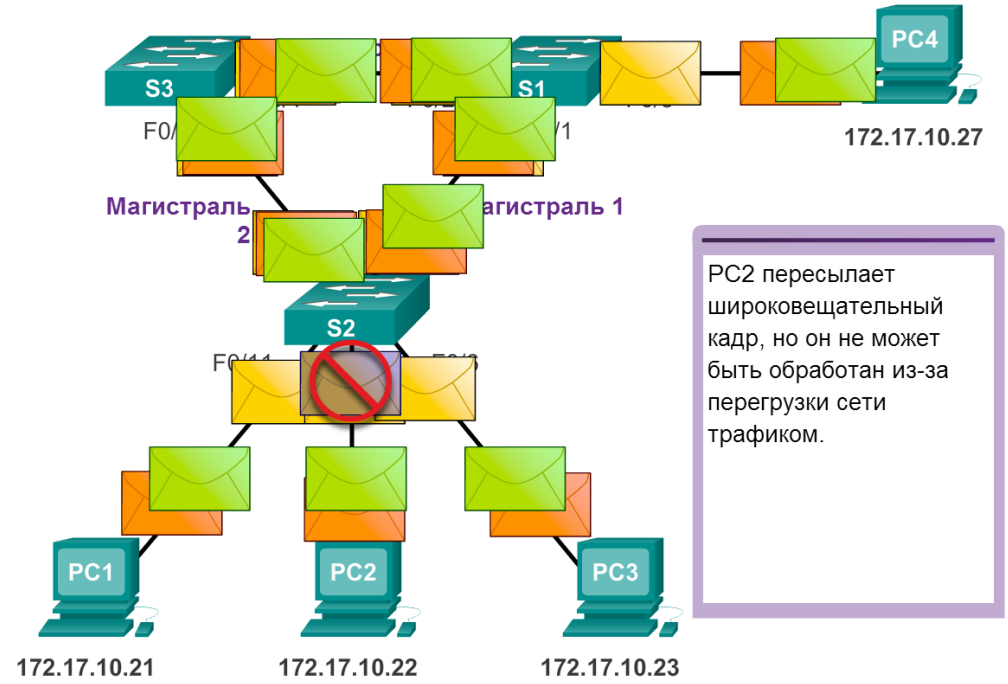
Этот процесс повторяется до тех пор, пока **петля** не будет прервана путем физического отключения соединений, вызывающих ее, или отключения питания одного из коммутаторов в петле.

Понятие протокола Spanning Tree

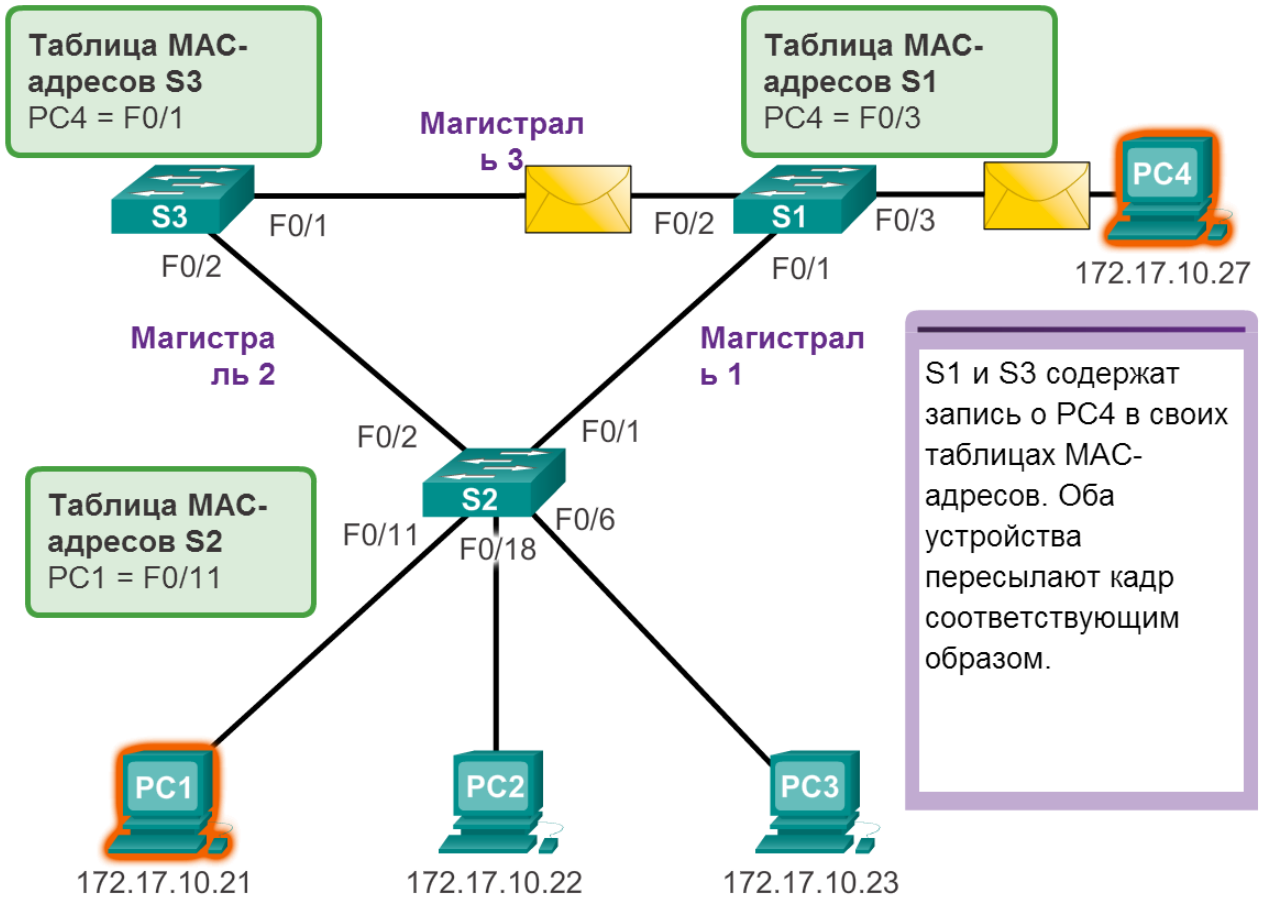
Широковещательный шторм

- Широковещательный шторм возникает в случае, когда в петлю на 2 уровне попадает столько кадров широковещательной рассылки, что при этом **потребляется вся доступная полоса пропускания**. Соответственно, **для легитимного трафика нет доступной полосы пропускания**, и сеть становится недоступной для обмена данными. Когда сеть полностью насыщена трафиком широковещательной рассылки, который циклически передается между коммутаторами, **новый трафик отбрасывается коммутатором**, поскольку он не в состоянии его обработать. Описанная ситуация — **эффективный отказ в обслуживании**.

- Поскольку устройства, подключенные к сети, регулярно отправляют кадры широковещательной рассылки, например, **ARP-запросы**, **широковещательный шторм может возникать за считанные секунды**. В результате при возникновении петли коммутируемая сеть быстро выходит из строя. **Широковещательный шторм неизбежен в сети, где возникла петля**.



Дублирование одноадресных кадров



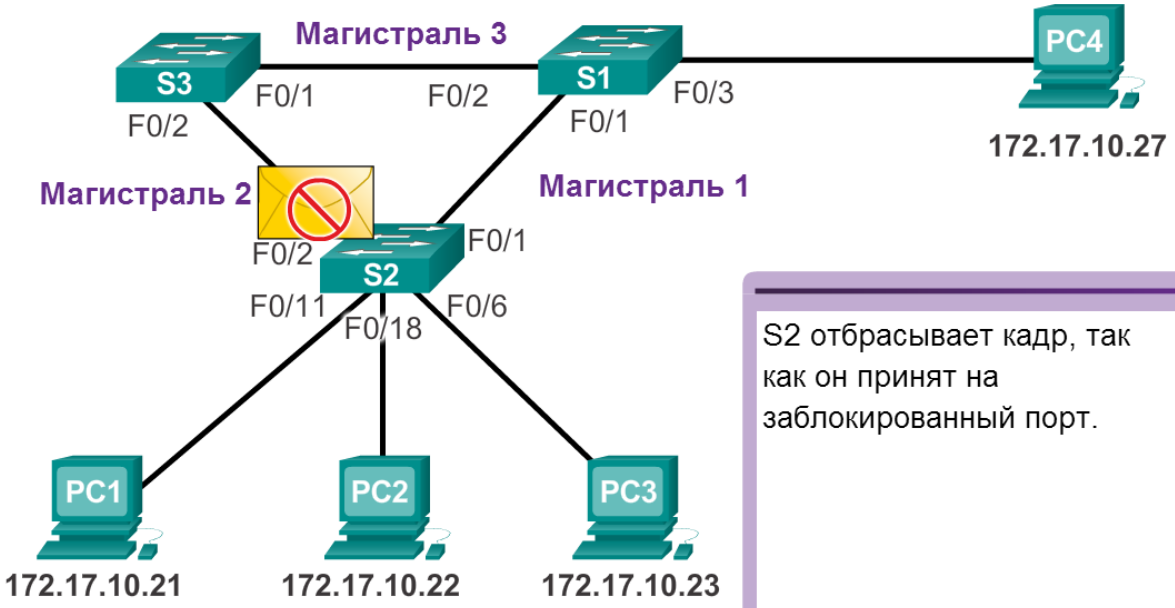
1. PC1 отправляет кадр одноадресной рассылки для PC4.
2. S2 не содержит в своей таблице MAC-адресов записи для PC4, поэтому выполняет лавинную рассылку этого кадра из всех портов коммутатора, пытаясь найти PC4.
3. Кадр поступает на коммутаторы S1 и S3.
4. S1 содержит в таблице MAC-адресов записи для PC4, поэтому он отправляет кадр на PC4.
5. S3 также содержит в таблице MAC-адресов запись для PC4, поэтому отправляет кадр одноадресной рассылки на S1.
6. S1 принимает дублированный кадр и отправляет его на PC4.
7. Таким образом, PC4 принимает два одинаковых кадра.

Принцип работы STP

Алгоритм Spanning Tree

- Протокол STP обеспечивает **наличие только одного логического пути** между всеми узлами назначения в сети путем намеренного **блокирования резервных путей**, которые могли бы вызвать петлю.
- **Порт считается заблокированным, когда заблокирована отправка и прием данных на этот порт.** К таким данным не относятся кадры BPDU, которые используются протоколом STP для предотвращения петель.
- Физические пути по-прежнему используются для обеспечения избыточности, однако эти пути отключены в целях предотвращения петель.
- **Если путь потребуется для компенсации неисправности сетевого кабеля или коммутатора, протокол STP повторно рассчитывает пути и снимает блокировку с требуемых портов**, чтобы разрешить активацию избыточного пути.

Алгоритм Spanning Tree



S2 отбрасывает кадр, так как он принят на заблокированный порт.

1. PC1 отправляет широковещательную рассылку в сеть.

2. S2 настроен с использованием протокола STP, и для порта F0/2 задано состояние блокировки. Состояние блокировки запрещает использование портов для пересылки данных пользователей, предотвращая, таким образом, возникновение петли. S2 пересылает кадр широковещательной рассылки из всех портов коммутатора, за исключением порта источника PC1 и порта F0/2 для Магистраль 2.

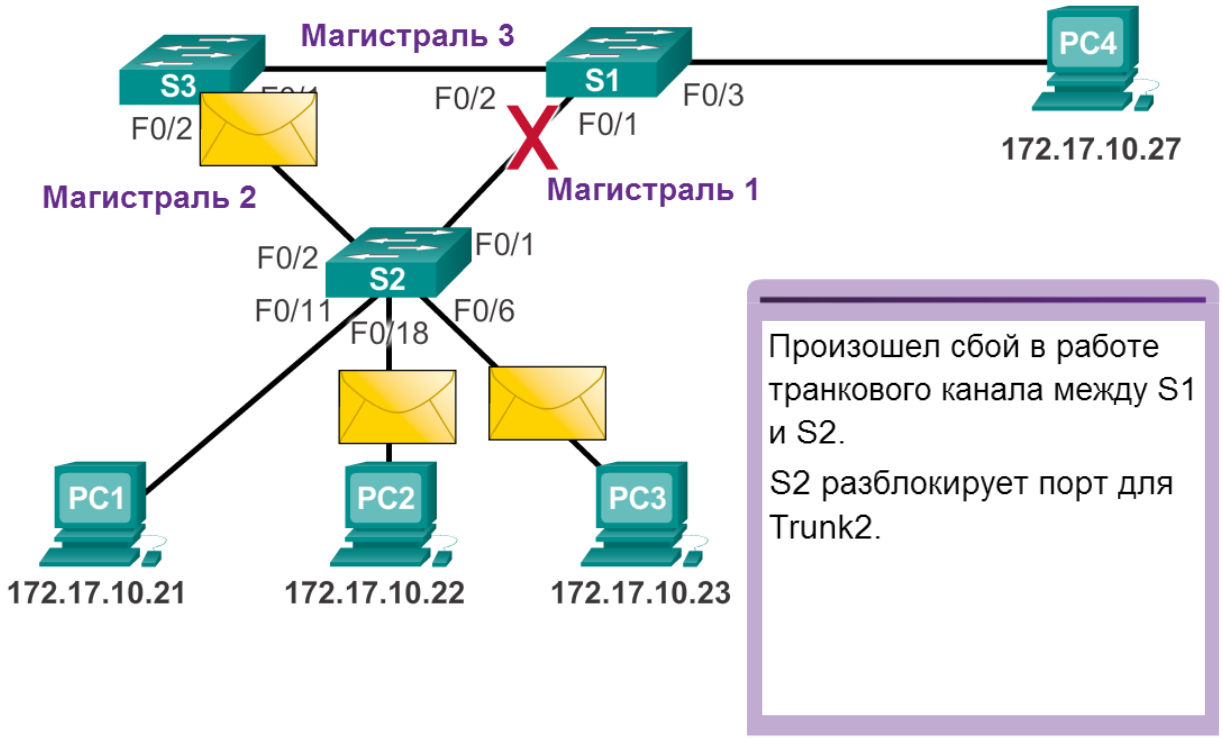
3. S1 принимает кадр широковещательной рассылки и пересылает его из всех портов коммутатора на PC4 и S3.

4. S3 пересылает кадр из порта F0/2 в Магистраль 2, и S2 отбрасывает кадр, т.к. он принят на заблокированный порт.

Возникновение петли 2 уровня предотвращено.

Принцип работы STP

Алгоритм Spanning Tree



Произошел сбой в работе транкового канала между S1 и S2.

S2 разблокирует порт для Trunk2.

S2 снимает блокировку с предварительно заблокированного порта для Магистраль 2 и разрешает передачу трафика широковещательной сети по альтернативному пути, обеспечивая дальнейший обмен данными. Если этот канал снова работает, выполняется повторное схождение протокола STP, а порт на S2 снова блокируется.

Принцип работы STP

Spanning Tree Алгоритм (STA): роли портов

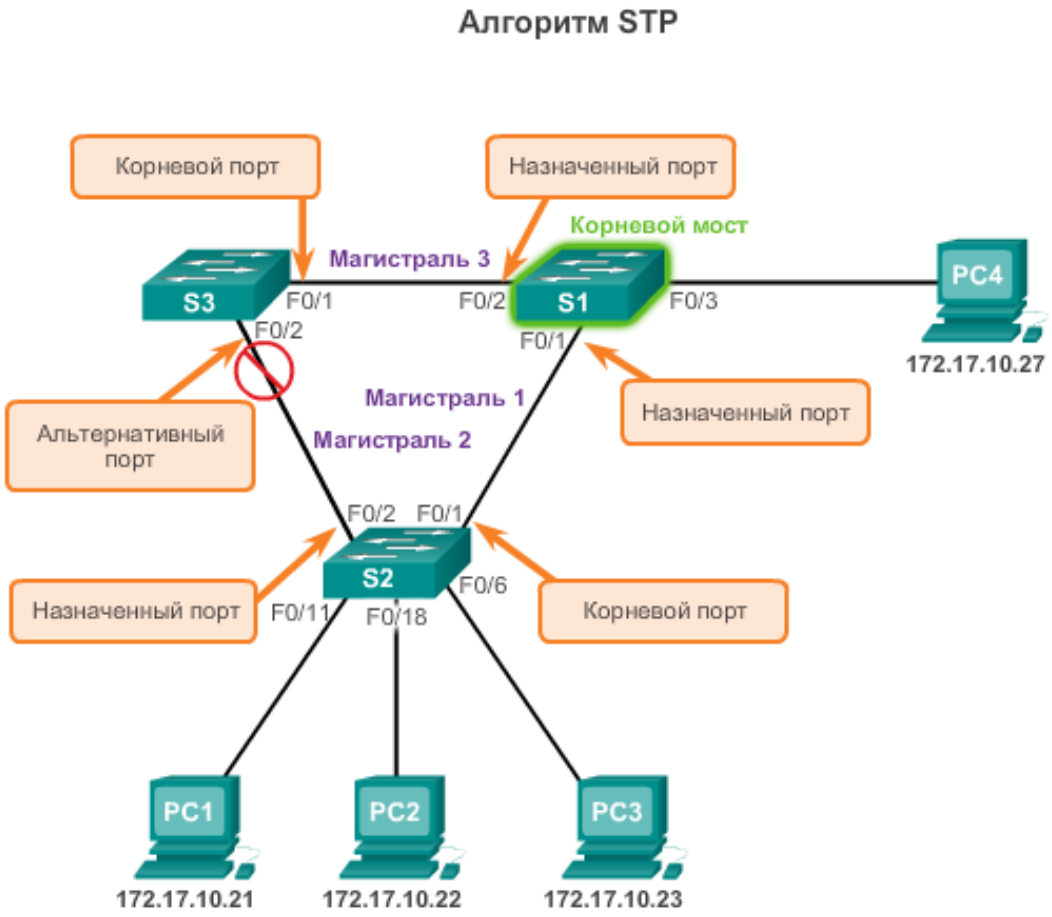
STA назначает один из коммутаторов в качестве корневого моста и использует его как точку привязки для расчёта всех путей. Все коммутаторы, участвующие в STP, обмениваются кадрами BPDU, чтобы определить, какой коммутатор имеет самое низкое значение идентификатора моста (BID) в сети. **Коммутатор с наименьшим значением BID автоматически становится корневым мостом для расчётов STA.**

Корневые порты – порты коммутаторов, ***находящиеся максимально близко к корневому мосту.*** Корневые порты выбираются для каждого коммутатора отдельно.

Назначенные порты — все некорневые порты, которым, тем не менее, разрешено пересылать трафик по сети. Назначенные порты выбираются для каждого транкового канала отдельно***. Если на одном конце транка находится корневой порт, то на другом — назначенный. Все порты на корневом мосте являются назначенными портами.***

Альтернативные и резервные порты – альтернативные и резервные порты настраиваются в состояние блокировки во избежание возникновения петель. Альтернативные порты выбираются только на транковых каналах, где ни один из концов не является корневым портом.

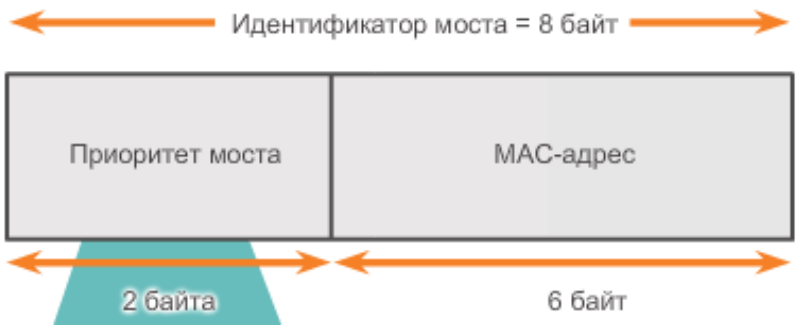
Отключенные порты –порт коммутатора, питание которого отключено.

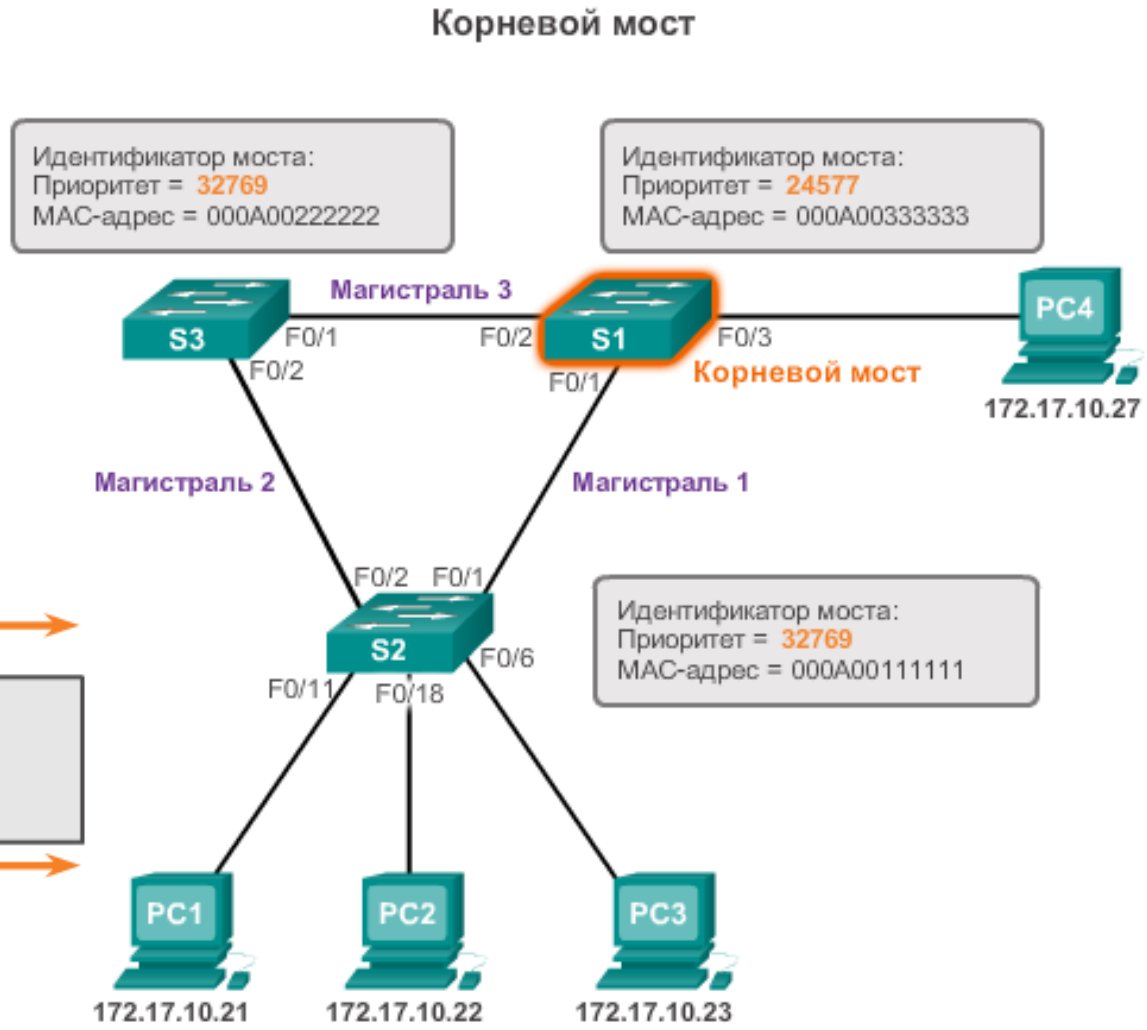


Принцип работы STP

Алгоритм Spanning Tree: Корневой мост

Коммутаторы начинают рассылать кадры BPDU **с интервалом в 2 секунды**. Эти BPDU содержат идентификатор BID коммутатора и идентификатор корневого моста. Если идентификатор корневого моста полученного кадра BPDU имеет меньшее значение, чем идентификатор корневого моста на принимающем коммутаторе, то принимающий коммутатор обновляет свой идентификатор корневого моста, указывая смежный коммутатор в качестве корневого моста.

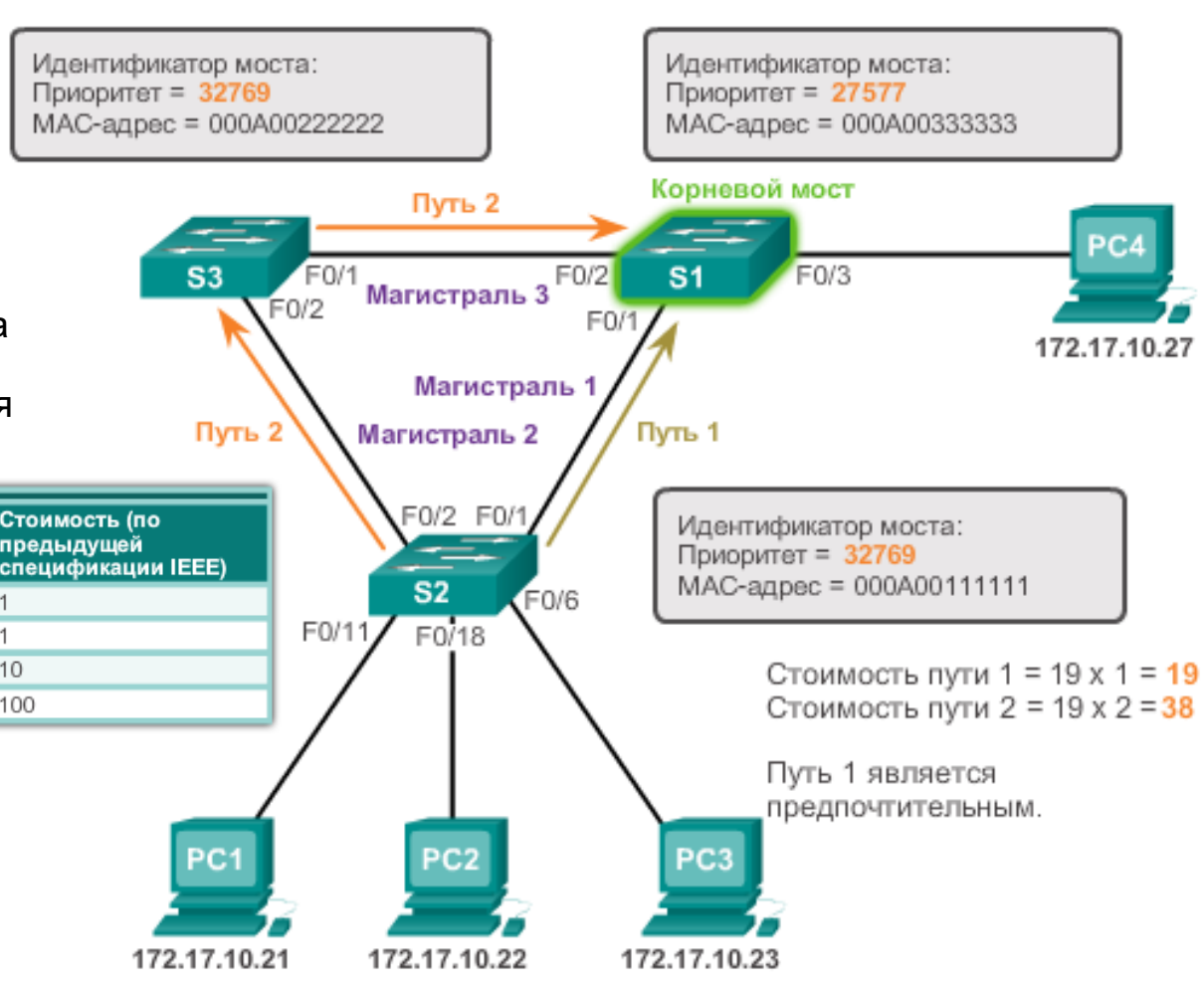




Алгоритм Spanning Tree: Стоимость пути

STA определяет оптимальные пути к корневому мосту от всех некорневых коммутаторов суммированием значений стоимости отдельных портов на пути.
Стоимость портов определяется скоростью работы порта.
Пути с наименьшей стоимостью становятся предпочтительными, а все остальные избыточные пути блокируются для предотвращения возникновения петли.

Скорость канала	Стоимость (по изменённой спецификации IEEE)	Стоимость (по предыдущей спецификации IEEE)
10 Гбит/с	2	1
1 Гбит/с	4	1
100 Мбит/с	19	10
10 Мбит/с	100	100



Принцип работы STP

Алгоритм Spanning Tree: Стоимость пути

Чтобы настроить стоимость порта интерфейса, введите команду **spanning-tree cost** *value* в режиме конфигурации интерфейса. Это значение может находиться в диапазоне между 1 и 200 000 000.

Чтобы восстановить значение стоимости порта по умолчанию 19, введите команду режима конфигурации интерфейса **no spanning-tree cost**.

Чтобы проверить стоимость порта и стоимость пути к корневому мосту, введите команду **show spanning-tree**

Настроить стоимость порта

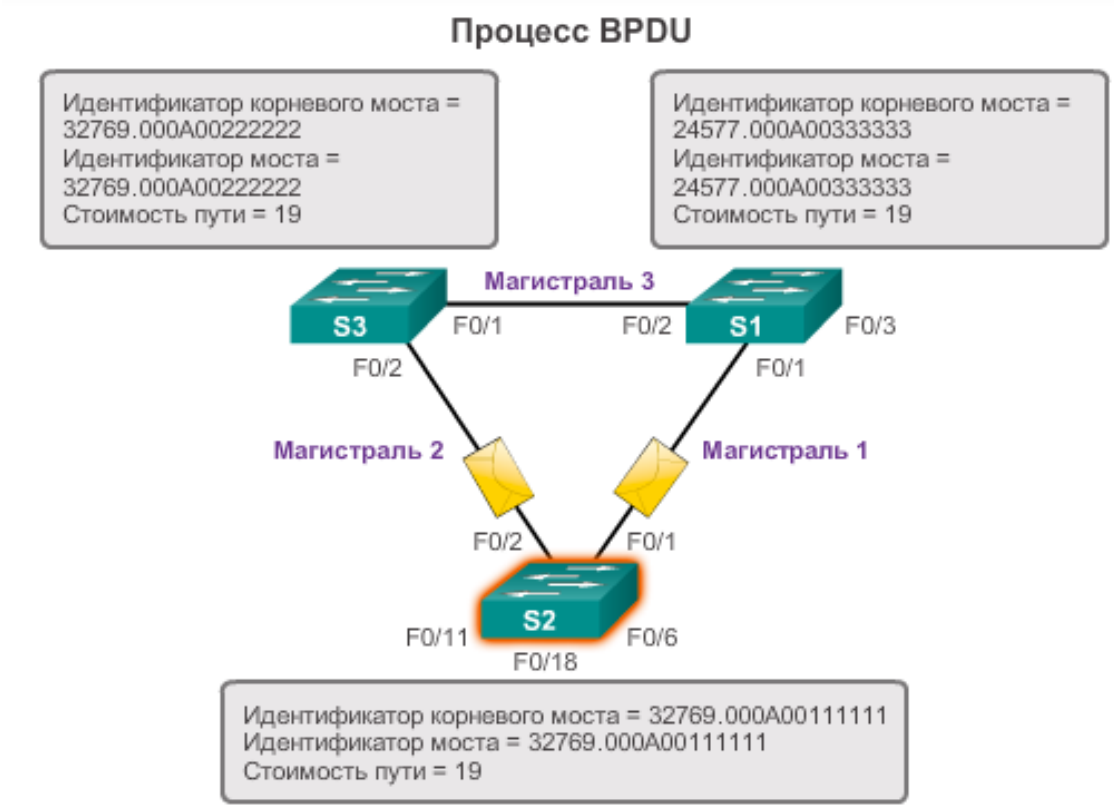
```
S2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)# interface f0/1
S2(config-if)# spanning-tree cost 25
S2(config-if# end
S2#
```

Сбросить стоимость порта

```
S2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)# interface f0/1
S2(config-if)# no spanning-tree cost
S2(config-if)# end
S2#
```

Принцип работы STP

Распространение и процесс BPDU



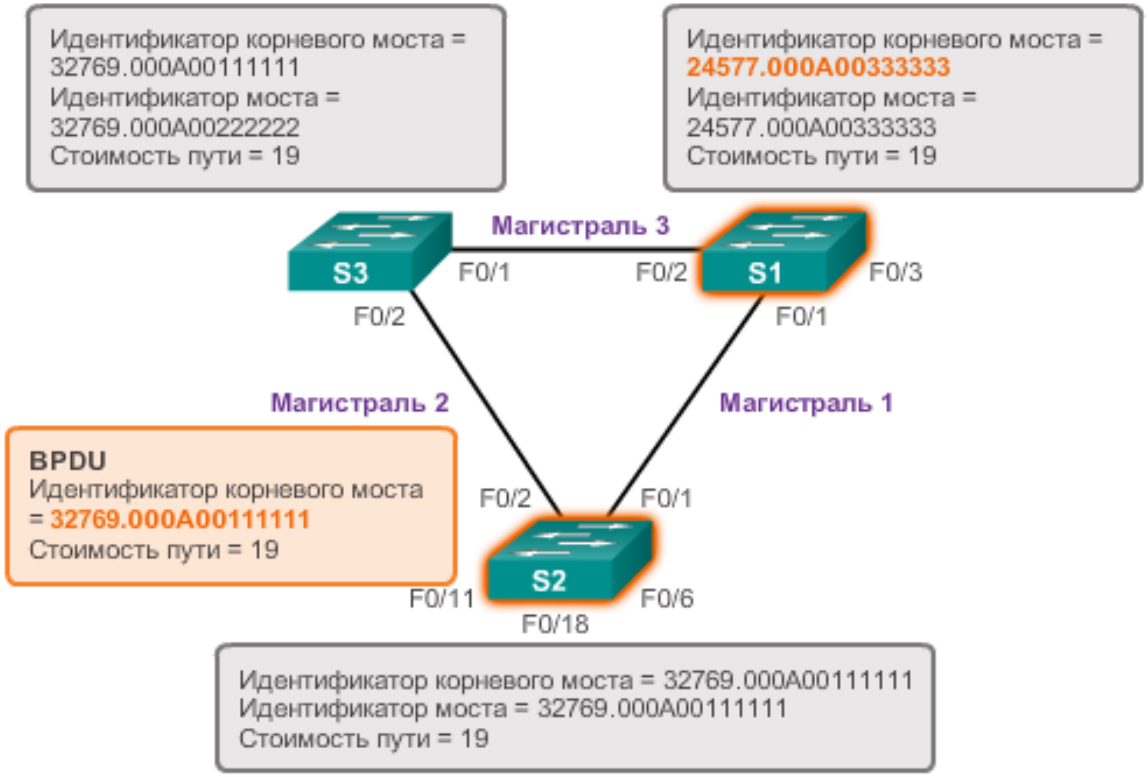
Изначально все коммутаторы считают, что они являются корневыми мостами. S2 пересылает кадры BPDU из всех портов коммутатора. Кадр BPDU содержит идентификатор моста и идентификатор корневого моста для S2, указывая, что это корневой мост.

Распространение и процесс BPDU

S3 сравнивает полученный идентификатор корневого моста с собственным и определяет S2 как более низкое значение идентификатора корневого моста. S3 обновляет свой идентификатор корневого моста до значения идентификатора корневого моста S2.Теперь S3 считает S2 корневым мостом. S3 обновляет стоимость пути до значения 19, так как BPDU получен на порт Fast Ethernet.

Принцип работы STP

Распространение и процесс BPDU



Когда S1 сравнивает свой идентификатор корневого моста с тем, который был получен в кадре BPDU от S2, он определяет локальный идентификатор корневого моста как более низкое значение и удаляет BPDU из S2. S1 все еще считает себя корневым мостом.

Принцип работы STP

Распространение и процесс BPDU

S3 пересылает кадры BPDU из всех портов коммутатора. Кадр BPDU содержит идентификатор корневого моста S2, указывая, что это корневой мост.

Принцип работы STP

Распространение и процесс BPDU

S2 сравнивает полученный корневой идентификатор BPDU с собственным и определяет, что эти идентификаторы совпадают. S2 продолжает считать себя корневым мостом в сети. S2 не обновляет стоимость пути.

Принцип работы STP

Распространение и процесс BPDU

S1 сравнивает полученный корневой идентификатор BPDU со своим собственным и определяет, что его собственный идентификатор имеет меньшее значение. S1 продолжает считать себя корневым мостом в сети. S1 не обновляет стоимость пути.

Принцип работы STP

Распространение и процесс BPDU

S1 пересылает кадры BPDU из всех портов коммутатора. Кадр BPDU содержит идентификатор моста и идентификатор корневого моста для S1, указывая, что это корневой мост.

Принцип работы STP

Распространение и процесс BPDU

S3 сравнивает полученный идентификатор корневого моста с собственным и определяет S1 как более низкое значение идентификатора корневого моста. S3 обновляет свой идентификатор корневого моста до значения идентификатора корневого моста S1. S3 теперь считает S1 корневым мостом. S3 обновляет стоимость пути до значения 19, поскольку BPDU получен на порт Fast Ethernet.

Распространение и процесс BPDU

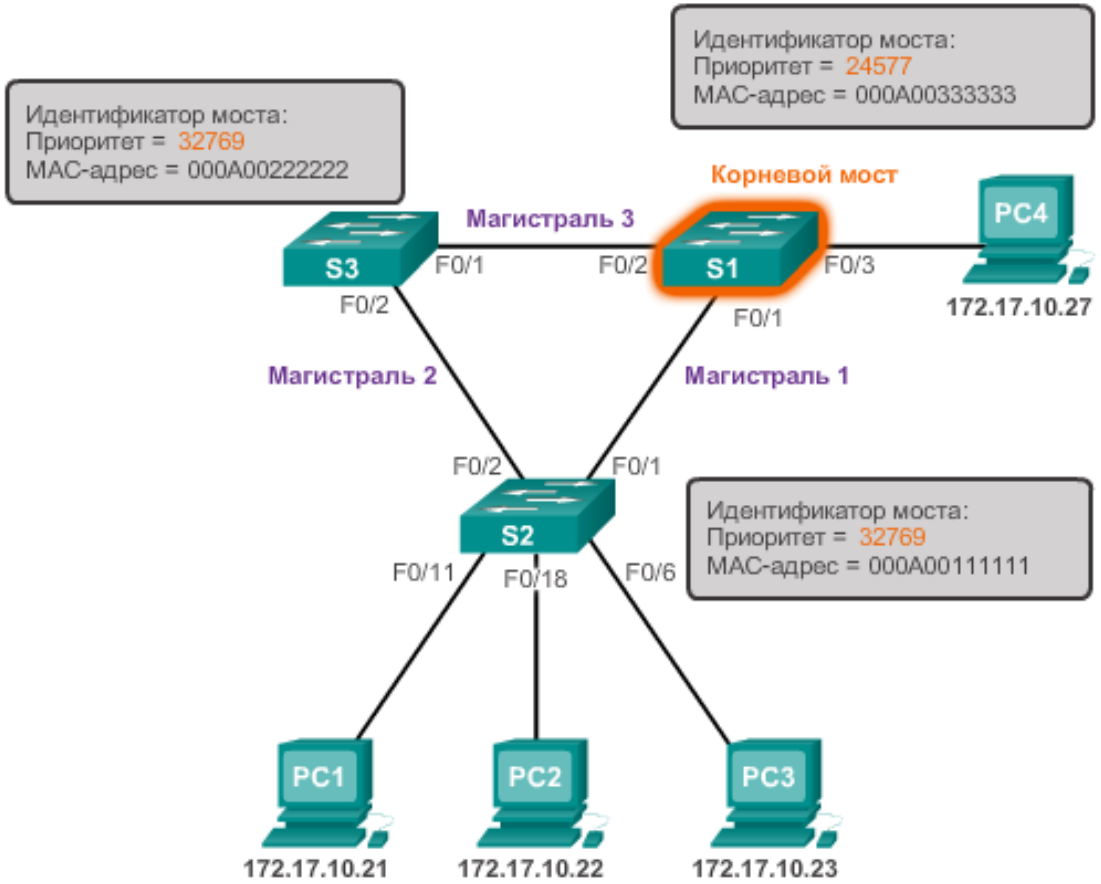
S2 сравнивает полученный идентификатор корневого моста с собственным и определяет S1 как более низкое значение идентификатора корневого моста. S2 обновляет свой идентификатор корневого моста до значения идентификатора корневого моста S1. S2 теперь считает S1 корневым мостом. S2 обновляет стоимость пути до значения 19, поскольку BPDU получен на порт Fast Ethernet.

Расширенный идентификатор VLAN

Сведения о сети VLAN включены в кадр BPDU с помощью расширенного идентификатора системы. Если пользовательские VLAN не установлены, то по умолчанию установлена VLAN 1 и расширенный идентификатор системы равен 1.

Принцип работы STP

Приоритет моста



По умолчанию для всех коммутаторов Cisco используется значение приоритета 32768. Значения варьируются в диапазоне от 0 до 61440 с шагом в 4096. Допустимые значения приоритета: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344 и 61440. Все остальные значения отклоняются. Приоритет моста 0 имеет преимущество по сравнению со всеми остальными значениями приоритета моста.

Типы протоколов STP

Список протоколов STP

Типы протоколов STP

- **802.1D-1998:** устаревший стандарт передачи данных в режиме моста и STP.
  - **CST:** допускает использование только одного экземпляра связующего дерева для всей сети с мостовым соединением независимо от количества сетей VLAN.
- **PVST+:** усовершенствованный корпорацией Cisco протокол STP, обеспечивающий отдельный экземпляр связующего дерева 802.1D для каждой сети VLAN, настроенной в сети.
- **802.1D-2004:** обновленный стандарт передачи данных в режиме моста и STP.
- **802.1w (RSTP):** повышает сходимость по протоколу STP 1998 за счёт добавления ролей в порты и усовершенствования обмена данными BPDU.
- **Rapid PVST+:** усовершенствованный корпорацией Cisco протокол RSTP, использующий PVST+.
- **802.1s (MSTP):** сопоставляет несколько сетей VLAN в пределах одного экземпляра связующего дерева.

Типы протоколов STP

Характеристики протоколов STP

Протокол	Стандарт	Требуемые ресурсы	Сходимость	Расчёт дерева
STP	802.1D	Низкая	Медленная	Все сети VLAN
PVST+	Cisco	Высокая	Медленная	На VLAN
RSTP	802.1w	Средняя	Быстрая	Все сети VLAN
Rapid PVST+	Cisco	Очень высокая	Быстрая	На VLAN
MSTP	802.1s, Cisco	Средняя или высокая	Быстрая	На экземпляр

Рассмотрим протоколы PVST+ и Rapid PVST+.

PVST+

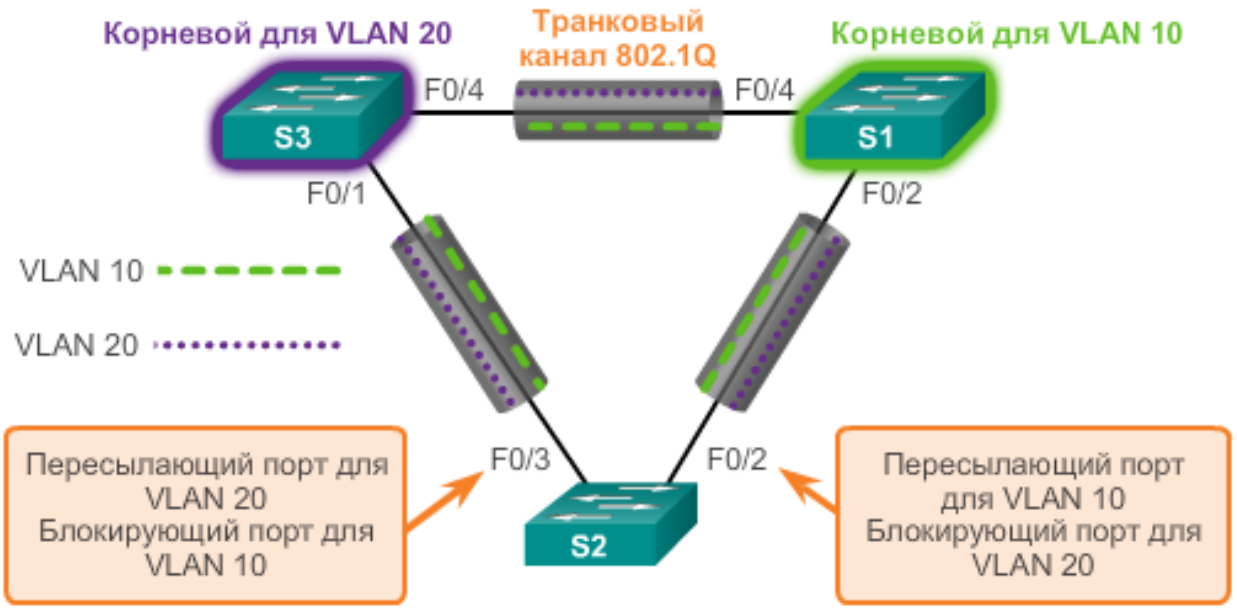
Обзор PVST+

- Корпорация Cisco разработала протокол PVST+ таким образом, чтобы сеть могла использовать независимый экземпляр реализации стандарта IEEE 802.1D **для каждой сети VLAN в пределах сети**.
- **PVST+ позволяет одному транковому порту на коммутаторе блокировать отдельную сеть VLAN, не блокируя при этом остальные сети VLAN**. PVST+ можно использовать для распределения нагрузки на 2 уровне.
- Поскольку все сети VLAN используют отдельный экземпляр STP, коммутаторам в среде PVST+ **требуется больший объём ресурсов ЦП и полосы пропускания BPDU**, чем в стандартной реализации CST протокола STP.

Обзор PVST+

Сети под управлением PVST+ имеют **следующие характеристики**:

- Поддерживается оптимальное распределение нагрузки.
- Поддержка одного экземпляра протокола spanning-tree для каждой сети VLAN может привести к значительному необоснованному потреблению ресурсов ЦП для всех коммутаторов в сети.



Порт F0/3 на коммутаторе S2 является портом, обеспечивающим передачу данных для сети VLAN 20, а порт F0/2 на коммутаторе S2 — для сети VLAN 10. Для этого нужно настроить коммутаторы таким образом, чтобы один был выбран в качестве корневого моста для половины сетей VLAN в пределах сети, а второй — в качестве корневого моста для оставшихся сетей VLAN. Коммутатор S3 является корневым мостом для VLAN 20, а S1 является корневым мостом для VLAN 10. Несколько корневых мостов STP в одной сети VLAN позволяют увеличить объём избыточности в сети.

PVST+

Работа протокола PVST+

Для обеспечения логической беспетлевой топологии сети для каждой сети VLAN в коммутируемой сети протокол PVST+ выполняет четыре действия:

1. Выбор одного корневого моста: только один коммутатор может выступать в роли корневого моста (для данной сети VLAN). Корневой мост — это коммутатор с наименьшим значением идентификатора моста. Все порты на корневом мосту являются назначенными (в частности, отсутствуют корневые порты).
2. Выбор корневого порта на каждом некорневом мосту: протокол STP устанавливает один корневой порт на каждом некорневом мосту. Корневой порт является путем с наименьшей стоимостью от некорневого моста к корневому мосту, указывая оптимальный путь к корневому мосту. Как правило, корневые порты находятся в режиме пересылки.
3. Выбор назначенного порта в каждом сегменте: в каждом канале протокол STP устанавливает один выделенный порт. Назначенный порт выбирается на коммутаторе, который предоставляет маршрут с наименьшей стоимостью к корневому мосту. Как правило, назначенные порты находятся в режиме пересылки и выполняют пересылку трафика для сегмента.
4. Остальные порты в коммутируемой сети являются альтернативными: альтернативные порты, как правило, остаются в состоянии блокировки, что позволяет логически разорвать петлевую топологию. Когда порт находится в состоянии блокировки, он не пересылает трафик, но по-прежнему может обрабатывать полученные сообщения BPDU.

PVST+

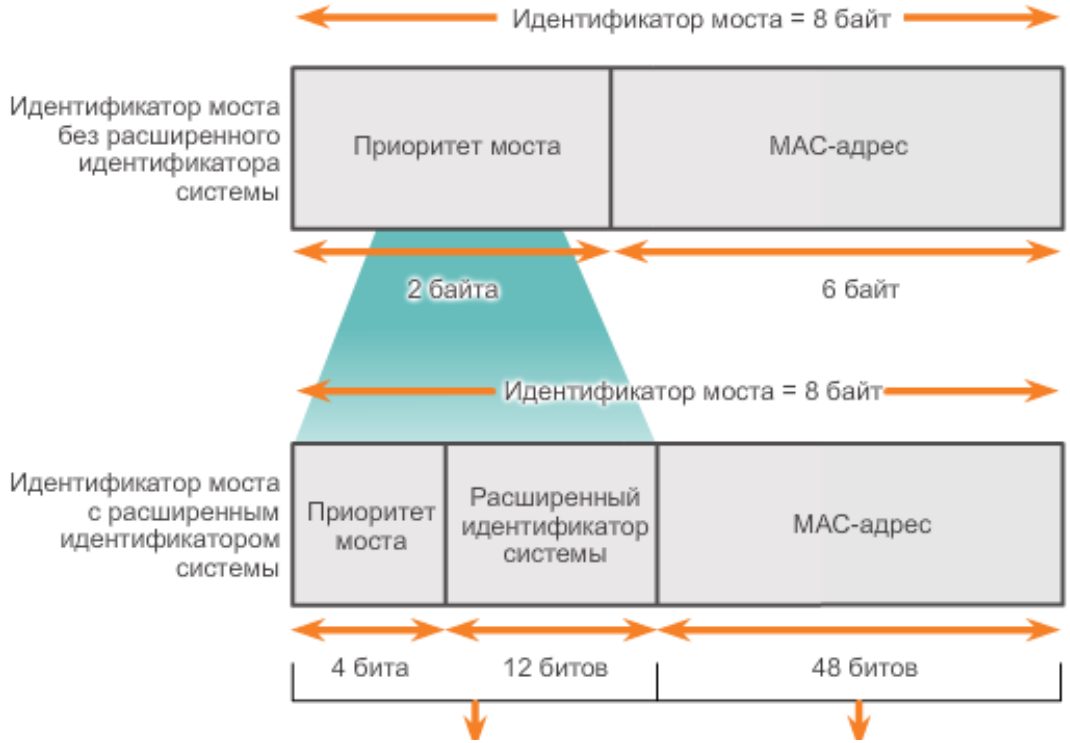
Состояние портов протокола PVST+

	Состояние порта				
Операция разрешена	**Блокировка:** порт является альтернативным и не участвует в пересылке кадров. Порт принимает кадры BPDU, чтобы определить местоположение и идентификатор корневого моста, а также роли порта, выполняемые каждым из портов коммутатора в конечной активной топологии STP.	**Прослушивание:** прослушивание пути к корневому мосту. Протокол STP определил, что порт может участвовать в пересылке кадров в соответствии с кадрами BPDU, которые коммутатор принял до этого момента. На этом этапе порт коммутатора не только принимает кадры BPDU, но также передает свои собственные кадры BPDU и сообщает смежным коммутаторам о том, что порт коммутатора готовится к участию в активной топологии.	**Обучение:** изучение MAC-адресов. На этапе подготовки к пересылке кадров порт начинает заполнять таблицу MAC-адресов.	**Пересылка:** порт считается частью активной топологии. Он пересылает кадры данных, отправляет и принимает кадры BPDU.	**Отключен:** порт 2 уровня не участвует в протоколе spanning-tree и не пересылает кадры. Отключенное состояние устанавливается в том случае, если порт коммутатора отключен администратором.
Может получать и обрабатывать BPDU	да	да	да	да	нет
Может пересылать кадры данных, полученные на интерфейс	нет	нет	нет	да	нет
Может пересылать кадры данных, полученные из другого интерфейса	нет	нет	нет	да	нет
Может получать данные MAC-адресов	нет	нет	да	да	нет

PVST+

Расширенный идентификатор системы PVST+

- В среде PVST+ расширенный идентификатор коммутатора обеспечивает уникальный идентификатор BID для каждого коммутатора в каждой из сетей VLAN.
- Например, сеть VLAN 2 будет использовать идентификатор BID по умолчанию 32770 (приоритет 32768 плюс расширенный идентификатор системы 2). Если приоритет не задан, коммутаторы будут использовать одинаковое значение приоритета по умолчанию, и выбор корневого моста для каждой сети VLAN будет выполняться на основе MAC-адреса.

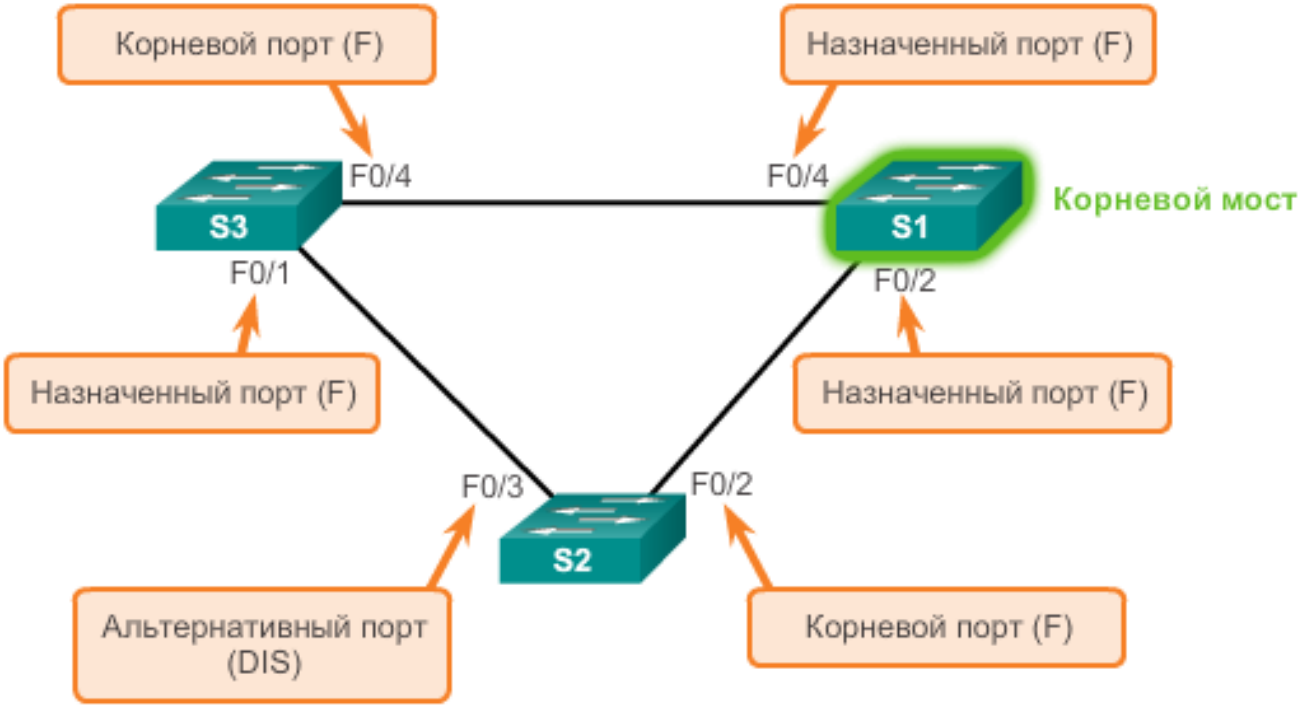


Описание Rapid PVST+

- RSTP является предпочтительным протоколом, позволяющим избежать возникновения петель 2 уровня в коммутируемой сети.
- В Rapid PVST+ **для каждой сети VLAN запускается самостоятельный экземпляр протокола RSTP**.
- RSTP поддерживает новый тип порта: **альтернативный порт в состоянии отбрасывания**.
- В протоколе RSTP **нет состояния блокирования порта**. Протокол RSTP определяет следующие состояния портов: **отбрасывание, изучение или пересылка**.
- RSTP (802.1w) заменяет STP (802.1D), сохраняя при этом обратную совместимость
- RSTP сохраняет тот же формат BPDU, за исключением того, что **в поле версии установлено значение 2**, что указывает на протокол RSTP, а **поле флагов задействует все 8 бит**.

Описание Rapid PVST+

В сети под управлением RSTP S1 является корневым мостом с двумя назначенными портами в состоянии пересылки.
RSTP поддерживает новый тип порта: порт F0/3 на коммутаторе S2 является альтернативным портом в состоянии отбрасывания.



Rapid PVST+

RSTP BPDU

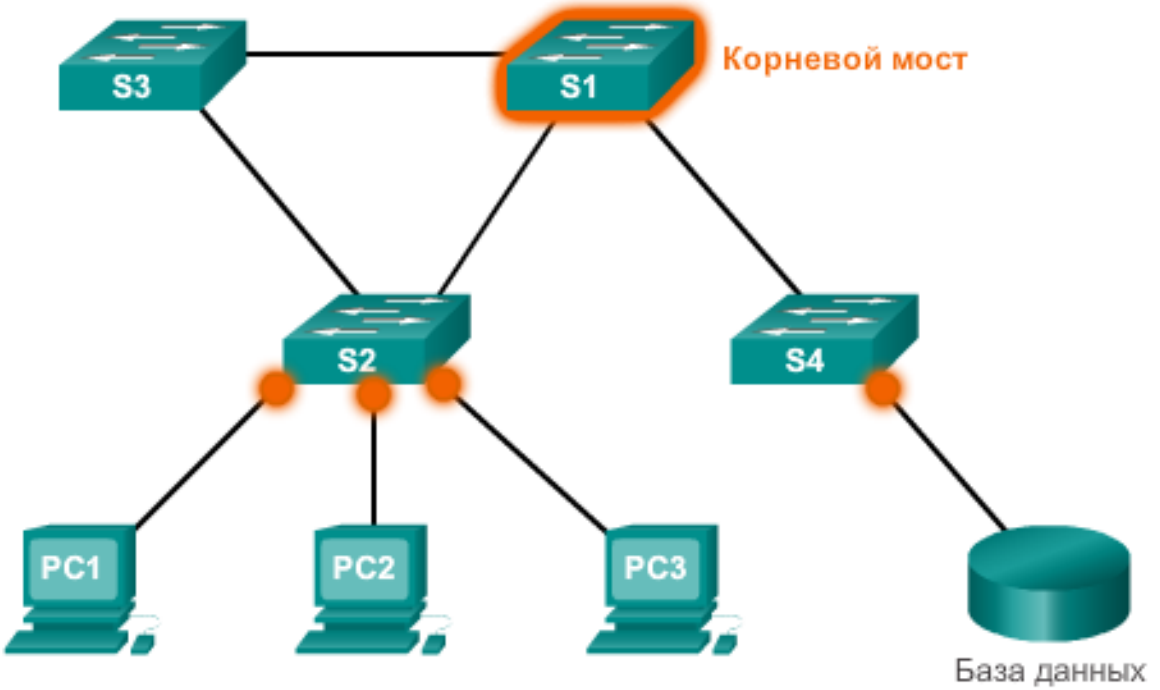
RSTP версия 2 BPDU

Поле	Длина байт
Идентификатор протокола=0x0000	2
Идентификатор версии протокола=0x02	1
Тип BPDU=0X02	1
Флаги	1
Идентификатор корневого моста	8
Стоимость корневого пути	4
Идентификатор моста	8
Идентификатор порта	2
Возраст сообщения	2
Максимальный возраст	2
Время приветствия	2
Задержка при пересылке	2

Поле флага

Бит поля	Бит
Изменение топологии	0
Предложение	1
Роль порта Неизвестный порт Альтернативный или резервный порт Корневой порт Назначенный порт	2-3 00 01 10 11
Обучение	4
Пересылка	5
Соглашение	6
Подтверждение изменения топологии	7

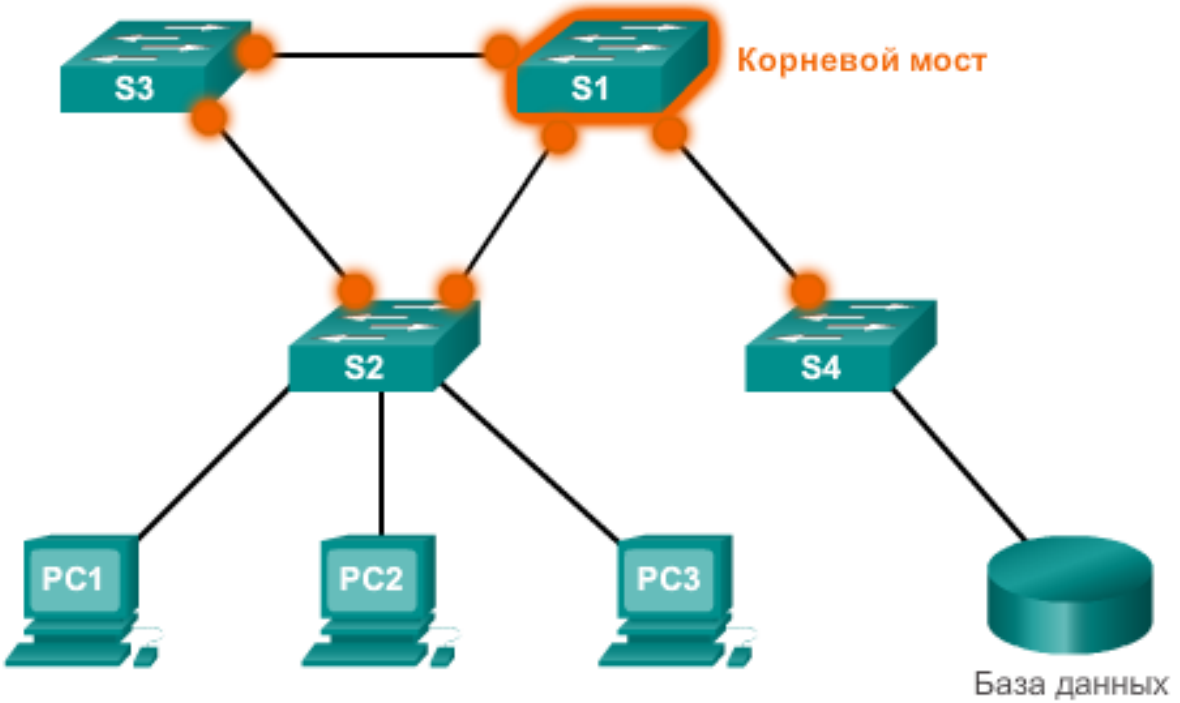
Пограничный порт



Пограничные порты

- Никогда не будет подключен к коммутатору
- Немедленно переходит в режим пересылки
- Функционирует аналогично порту, настроенному с использованием Cisco PortFast
- На коммутаторе Cisco, настроенном с помощью команды **`spanning-tree portfast`**

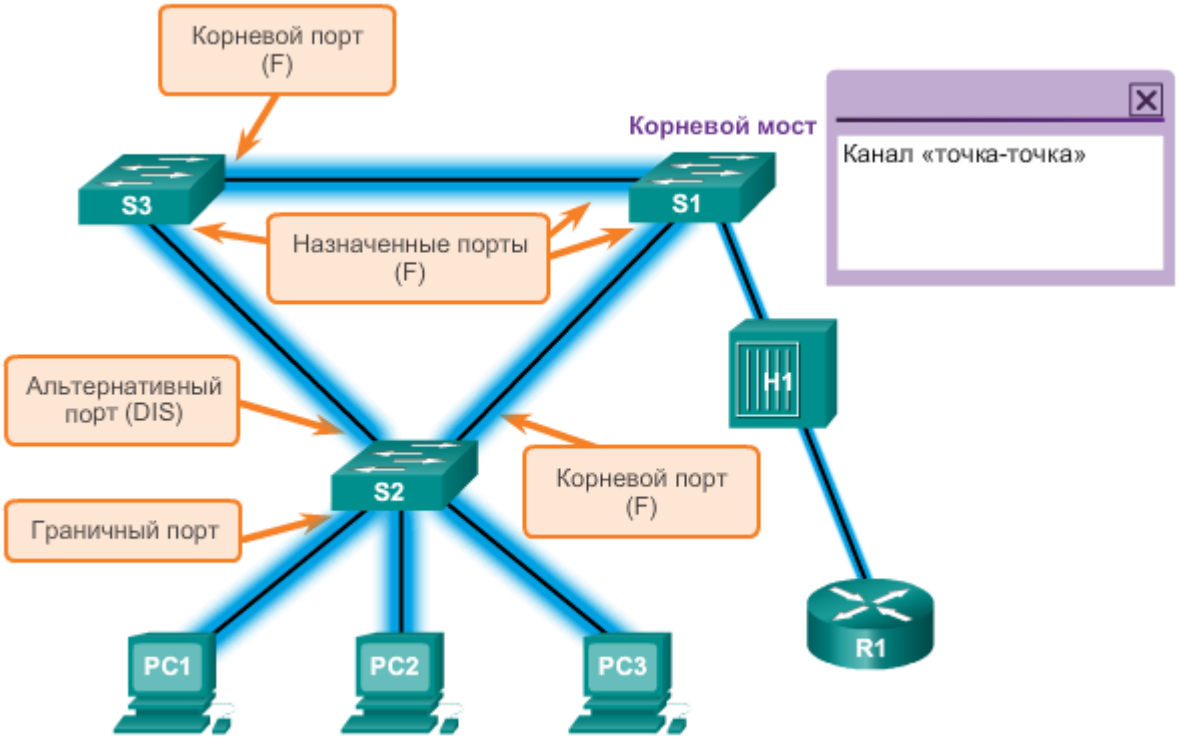
Неграничный порт



Неграничные порты

Порты, которые могут быть соединены с другими устройствами коммутации и не должны быть настроены как граничные порты.

Типы каналов

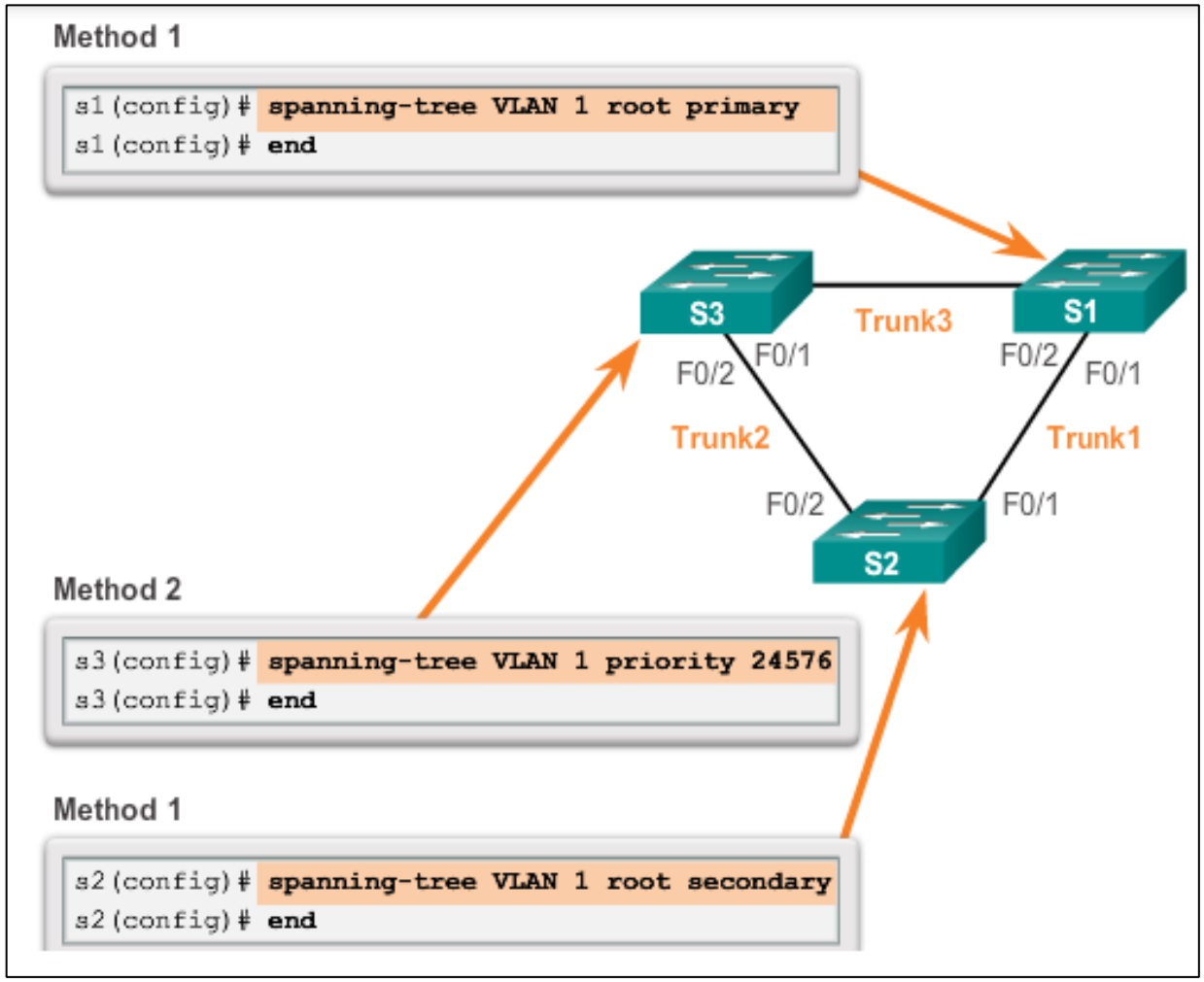


В зависимости от того, какие устройства подключены к каждому из портов, можно выделить два различных типа каналов:

Точка-точка: порт, работающий в полнодуплексном режиме; как правило, соединяет два коммутатора и является кандидатом на быстрый переход в состояние пересылки.

Общий: порт, работающий в полудуплексном режиме; соединяет коммутатор с концентратором, объединяющим несколько устройств.

Настройка и проверка идентификатора моста



Метод 1

Коммутатор S1 назначен в качестве основного корневого моста с помощью команды **spanning-tree vlan 1 root primary**, а коммутатор S2 в качестве вспомогательного корневого моста с помощью команды **spanning-tree vlan 1 root secondary**. Альтернативный коммутатор становится корневым мостом в случае отказа основного корневого моста.

Метод 2

Настроить значение приоритета порта также можно с помощью команды глобального режима конфигурации **spanning-tree vlan** *vlan-id* **priority** *value*. Значение приоритета настраивается с шагом в 4096 в диапазоне от 0 до 61440.

В этом примере коммутатору S3 присвоено значение приоритета моста 24576 с помощью команды **spanning-tree vlan 1 priority 24576**.

Конфигурация PVST+

Настройка и проверка идентификатора моста

```
S3# show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    24577
              Address     00A.0033.3333
              This bridge is the root
              Hello Time  2 sec Max Age 20 sec Forward Delay 15 sec
  Bridge ID   Priority    24577  (priority  24576  sys-id-ext  1)
              Address     000A.0033.3333
              Hello Time  2 sec Max Age 20 sec Forward Delay 15 sec
              Aging Time  300

Interface      Role    Sts    Cost      Prio.Nbr       Type
-------------  -----   ----   -----     ----------     ------
Fa0/1          Desg    FWD    4         128.1          p2p
Fa0/2          Desg    FWD    4         128.2          p2p
S3#
```

Для коммутатора задан приоритет 24576. Также обратите внимание, что коммутатор назначен в качестве корневого моста для экземпляра протокола spanning-tree.

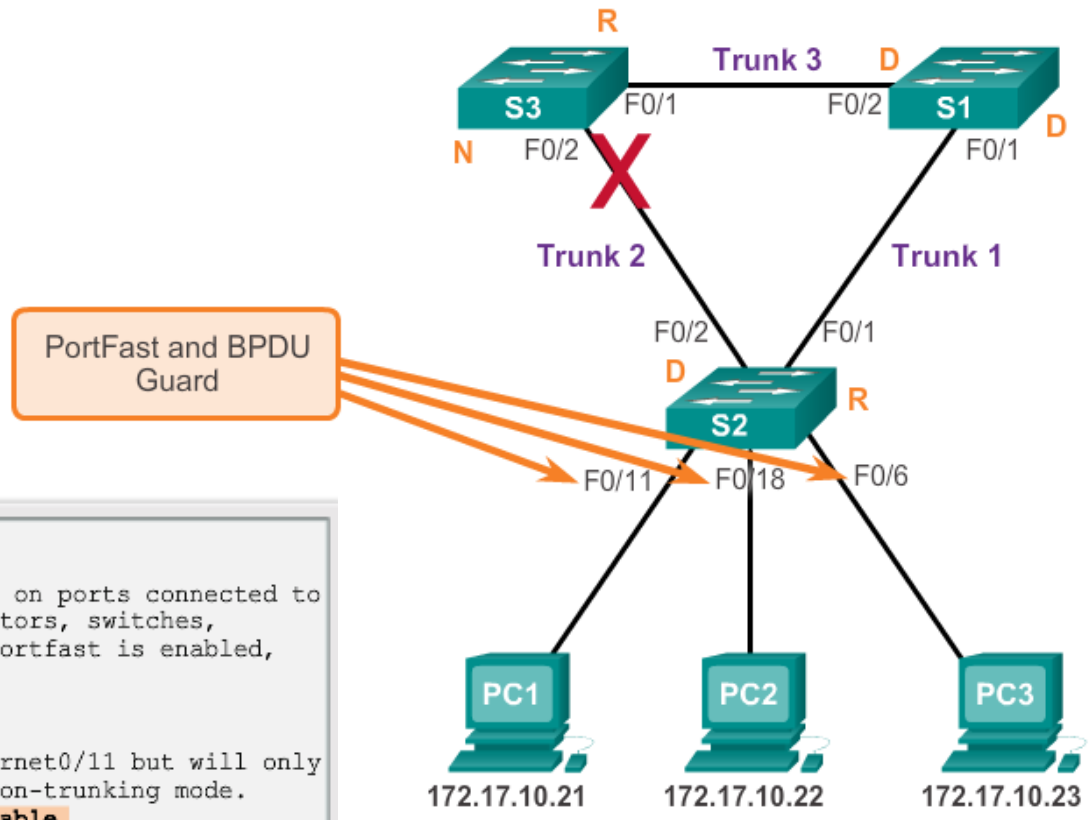
Конфигурация PVST+

PortFast и BPDU Guard

- Если порт коммутатора настроен с помощью функции **PortFast**, то такой порт сразу переходит из состояния блокировки в состояние пересылки, минуя состояния прослушивания и получения данных.
- Когда функция **BPDU guard** включена, она переводит порт в состояние *отключения из-за ошибки* при получении BPDU. Это позволяет выключить порт.

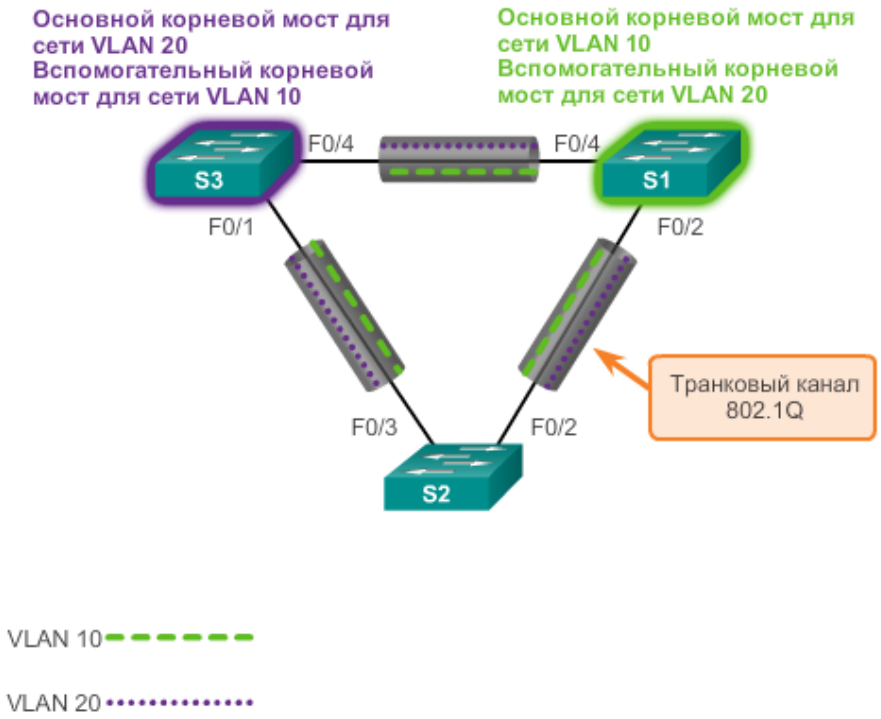
```
S2(config)# interface FastEthernet 0/11
S2(config-if)# spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to
a single host. Connecting hubs, concentrators, switches,
bridges, etc... to this interface  when portfast is enabled,
can cause temporary bridging loops.
 Use with CAUTION

%Portfast has been configured on FastEthernet0/11 but will only
 have effect when the interface is in a non-trunking mode.
S2(config-if)# spanning-tree bpduguard enable
S2(config-if)# end
```



Конфигурация PVST+

Распределение нагрузки PVST+



Для назначения корневого моста, можно установить самое низкое значение приоритета протокола spanning-tree на каждом коммутаторе, чтобы этот коммутатор был выбран в качестве основного моста для связанной с ним сети VLAN.

```
S3(config)# spanning-tree vlan 20 root primary
```

Эта команда принудительно назначает S3 основным корневым мостом для сети VLAN 20.

```
S3(config)# spanning-tree vlan 10 root secondary
```

Эта команда принудительно назначает S3 вспомогательным корневым мостом для сети VLAN 10.

```
S1(config)# spanning-tree vlan 10 root primary
```

Эта команда принудительно назначает S1 основным корневым мостом для сети VLAN 10.

```
S1(config)# spanning-tree vlan 20 root secondary
```

Эта команда принудительно назначает S1 вспомогательным корневым мостом для сети VLAN 20.

```
S3(config)# spanning-tree vlan 20 priority 4096
```

Эта команда задает для приоритета S3 самое низкое допустимое значение. В результате S3, скорее всего, станет основным корневым мостом для сети VLAN 20.

```
S1(config)# spanning-tree vlan 10 priority 4096
```

Эта команда задает для приоритета S1 самое низкое допустимое значение. В результате S1, скорее всего, станет основным корневым мостом для сети VLAN

Распределение нагрузки PVST+

Команда **show spanning-tree active** позволяет отобразить сведения о конфигурации протокола spanning-tree только для активных интерфейсов. Выходные данные относятся к S1, настроенному с помощью PVST+.

```
S1# show spanning-tree active

<выходные данные опущены>

VLAN0010
   Spanning tree enabled protocol ieee
   Root ID     Priority    4106
               Address     0019.aa9e.b000
               This bridge is the root
               Hello Time  2 sec Max Age 20 sec Forward Delay 15 sec
   Bridge ID   Priority    4106  (priority 4096 sys-id-ext 10)
               Address     0019.aa9e.b000
               Hello Time  2 sec Max Age 20 sec Forward Delay 15 sec
               Aging Time  300

Interface        Role    Sts    Cost      Prio.Nbr       Type
---------------- ------  ----   -------   ----------     ------
Fa0/2            Desg    FWD    19         128.2         p2p
Fa0/4            Desg    FWD    19         128.4         p2p

<выходные данные опущены>
```

4096+10=4106

Конфигурация PVST+

Распределение нагрузки PVST+

```
S1# show running-config
Building configuration...

Current configuration : 1595 bytes
!
version 12.2
 <выходные данные опущены>
!
spanning-tree mode pvst
spanning-tree extend system-id
spanning-tree vlan 1 priority 24576
spanning-tree vlan 10 priority 4096
spanning-tree vlan 20 priority 28672
!
 <выходные данные опущены>
```

Приоритет для сети VLAN 10 равен 4096, что является наименьшим из значений приоритета для трех соответствующих сетей VLAN.

Rapid PVST+ Configuration

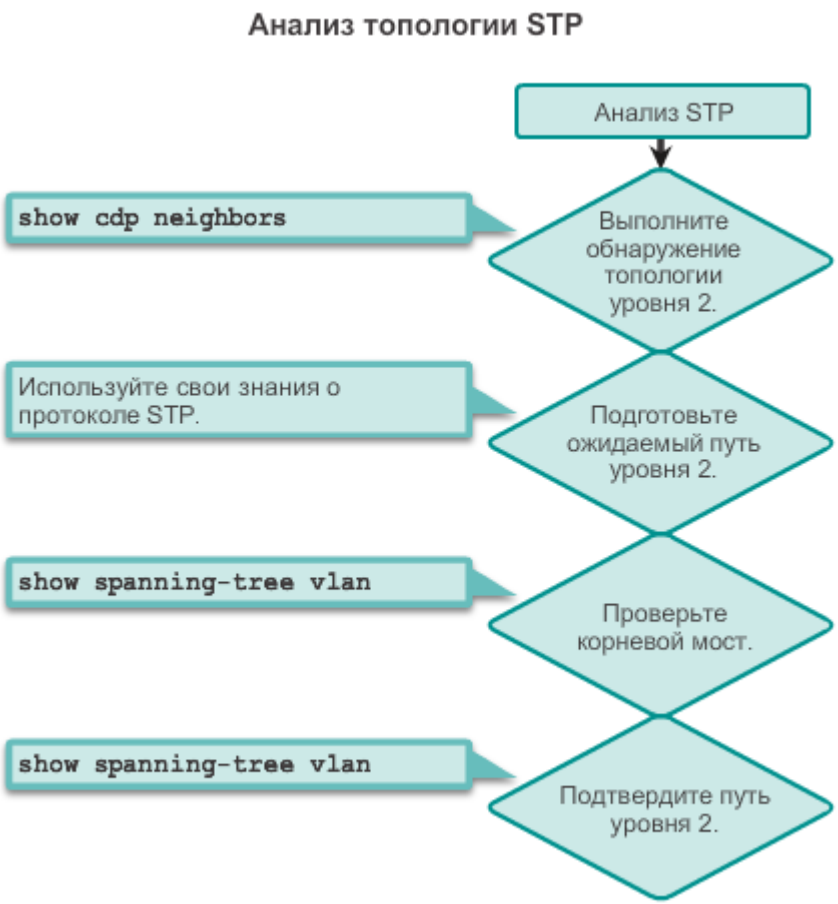
Spanning Tree Mode

В большинстве случаев разница между настройкой PVST+ и Rapid PVST+ заключается в команде **spanning-tree mode rapid-pvst**.

```
S1# configure terminal
S1(config)# spanning-tree mode rapid-pvst
S1(config)# interface f0/2
S1(config-if)# spanning-tree link-type point-to-point
S1(config-if)# end
S1# clear spanning-tree detected-protocols
```

Синтаксис команд Cisco IOS	
Войдите в режим глобальной конфигурации.	`configure terminal`
Настройте режим spanning-tree протокола Rapid PVST+.	`spanning-tree mode rapid-pvst`
Перейдите в режим конфигурации интерфейса и укажите интерфейс, который необходимо настроить. Допустимые интерфейсы содержат физические порты, сети VLAN и агрегированные каналы.	`interface` *interface-id*
Укажите, что канал для данного порта принадлежит к типу «точка-точка».	`spanning-tree link-type point-to-point`
Вернитесь в привилегированный режим EXEC.	`end`
Очистите все обнаруженные STP.	`clear spanning-tree detected-protocols`

Анализ топологии STP



Для анализа топологии STP выполните следующие действия:

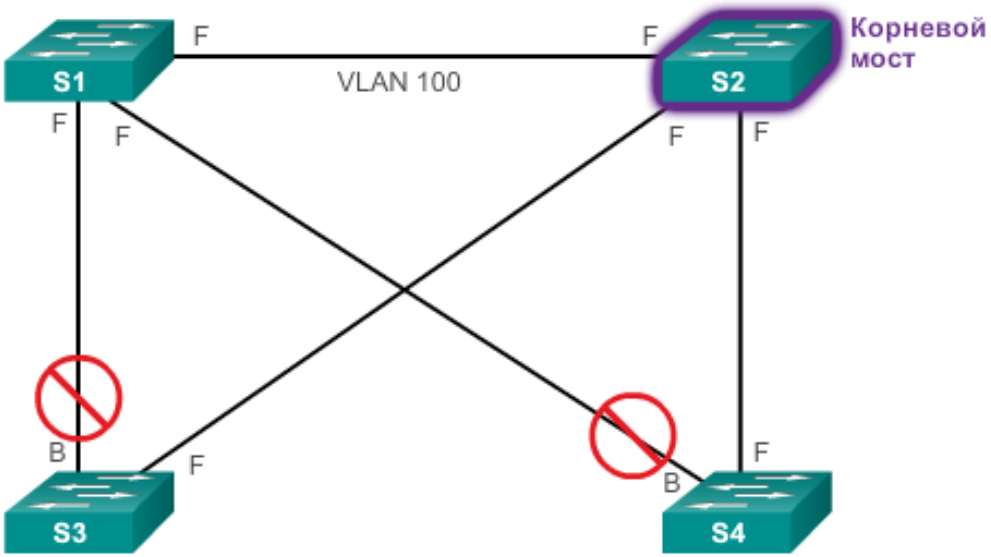
Шаг 1. Обнаружение топологии 2 уровня. Используйте сетевую документацию (если есть) или команду **show cdp neighbors** для обнаружения топологии 2 уровня.

Шаг 2. После обнаружения топологии 2 уровня используйте сведения об STP для определения ожидаемого пути 2 уровня. Необходимо знать, какой коммутатор является корневым мостом.

Шаг 3. Чтобы определить, какой коммутатор является корневым мостом, используйте команду **show spanning-tree vlan**.

Шаг 4. Используйте команду **show spanning-tree vlan** для всех коммутаторов, чтобы выяснить, какие порты находятся в состоянии блокировки или пересылки и подтвердить ожидаемый путь 2 уровня.

Анализ топологии STP



Устранение проблемы с STP:

- Чтобы исправить сбой протокола spanning-tree, можно вручную удалять избыточные каналы из коммутируемой сети (физически или через конфигурацию), пока из топологии не будут устранены все петли.
- Перед восстановлением избыточных каналов следует определить и устранить причину сбоя протокола spanning-tree.

Во многих сетях оптимальная топология STP определяется в рамках проекта сети, после чего реализуется посредством операций с приоритетом STP и значениями стоимости. Могут возникать ситуации, когда STP не учитывается в проекте сети и при ее реализации, либо STP был учтен или реализован до того, как сеть была существенно расширена или изменена. В таких ситуациях важно уметь анализировать фактическую топологию STP в работающей сети.

По большей части устранение неисправностей заключается в сравнении фактического состояния сети с ее ожидаемым состоянием и выявлении несоответствий, которые помогают в определении и решении проблемы. Сетевой специалист должен уметь проверять коммутаторы и определять фактическую топологию, а также понимать, какой должна быть топология протокола spanning-tree.