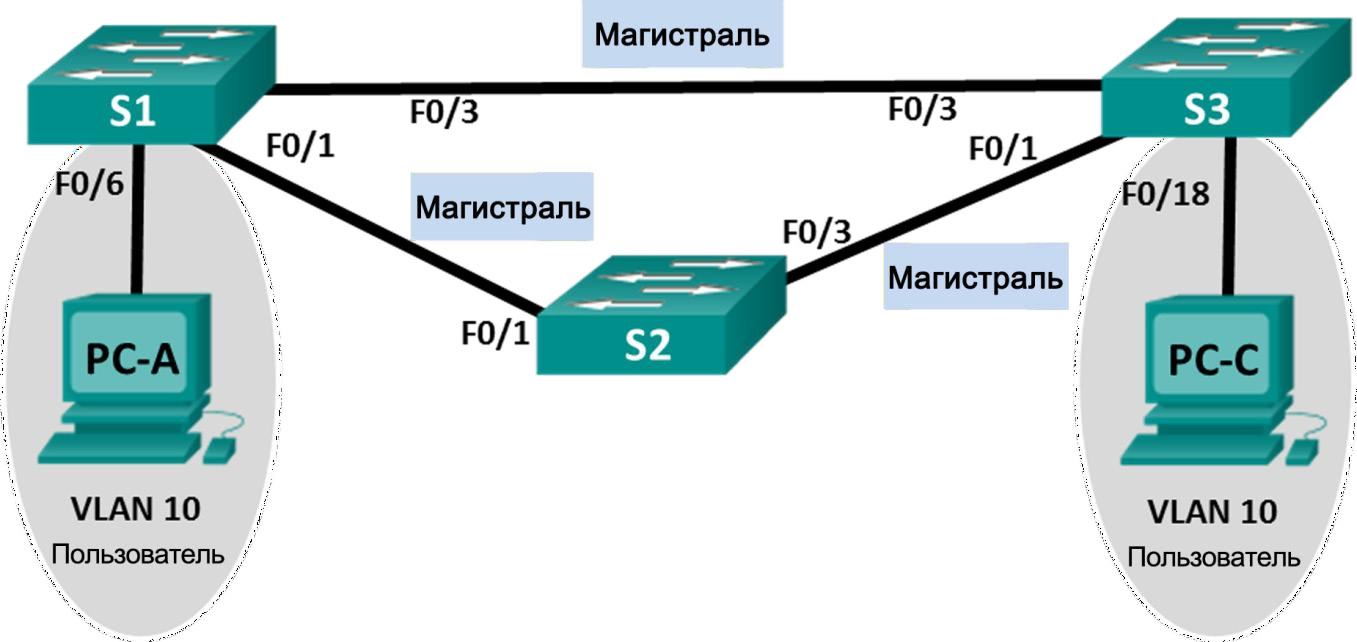


Настройка Rapid PVST+, PortFast и BPDU Guard

**Топология**



**Таблица адресации**

|  |  |  |  |
| --- | --- | --- | --- |
| **Устройство** | **Интерфейс** | **IP-адрес** | **Маска**  **подсети** |
| S1\_ФАМИЛИЯ | VLAN 99 | 192.168.X+1.11 | 255.255.255.0 |
| S2 | VLAN 99 | 192.168.X+1.12 | 255.255.255.0 |
| S3 | VLAN 99 | 192.168.X+1.13 | 255.255.255.0 |
| PC-A | NIC | 192.168.0.2 | 255.255.255.0 |
| PC-C | NIC | 192.168.0.3 | 255.255.255.0 |

**Назначения сети VLAN**

|  |  |
| --- | --- |
| **VLAN** | **Имя** |
| 10 | User\_ФАМИЛИЯ |
| 99 | Management |

**Задачи**

**Часть 1. Создание сети и настройка основных параметров устройства Часть 2. Настройка сетей VLAN, native VLAN и транковых каналов Часть 3. Настройка корневого моста и проверка сходимости PVST+**

**Часть 4. Настройка Rapid PVST+, PortFast, BPDU guard и проверка сходимости**

**Необходимые ресурсы**

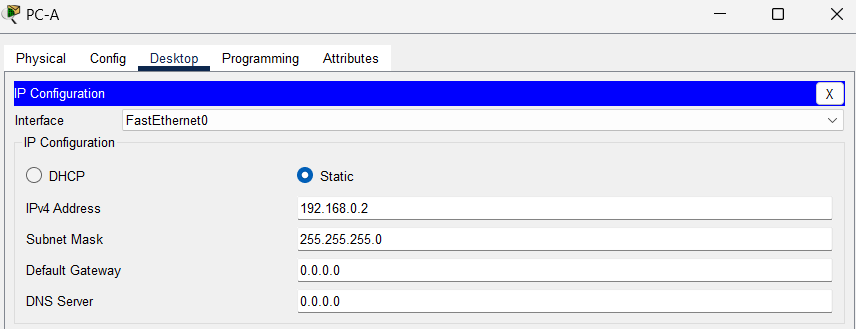
* 3 коммутатора (Cisco 2960 с операционной системой Cisco IOS 15.0(2) (образ lanbasek9) или аналогичная модель)
* 2 ПК (ОС Windows с программой эмуляции терминала, например, Tera Term)
* Консольные кабели для настройки устройств Cisco IOS через консольные порты
* Кабели Ethernet, расположенные в соответствии с топологией

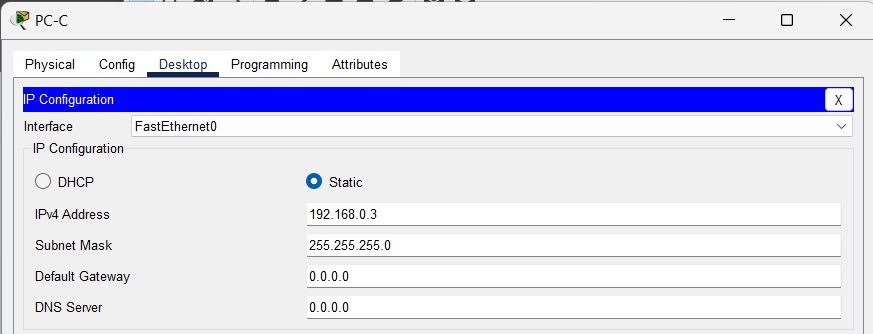
# Часть 1: Создание сети и настройка основных параметров устройства

В части 1 вы настроите топологию сети и такие базовые параметры, как IP-адреса интерфейсов, доступ к устройствам и пароли.

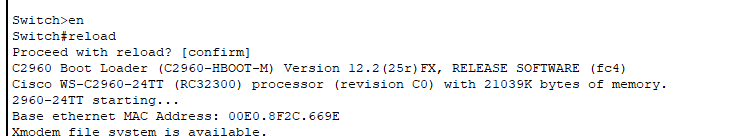
**Шаг 1: Создайте сеть согласно топологии.**

**Шаг 2: Настройте узлы ПК.**

****

****

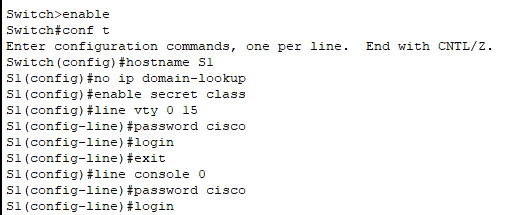
**Шаг 3: Выполните инициализацию и перезагрузку коммутаторов.**

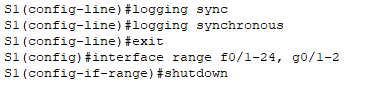
****

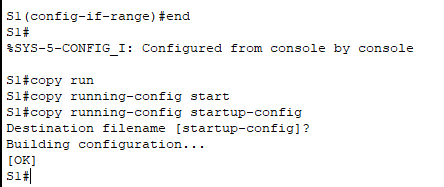
**Шаг 4: Настройте базовые параметры каждого коммутатора.**

1. Отключите поиск DNS.
2. Присвойте имена устройствам в соответствии с топологией.
3. Назначьте **cisco** в качестве пароля консоли и виртуального терминала VTY и включите запрос пароля при подключении.
4. Назначьте **class** в качестве зашифрованного пароля доступа к привилегированному режиму.
5. Настройте **logging synchronous**, чтобы сообщения от консоли не могли прерывать ввод команд.
6. Отключите все порты коммутатора.
7. Сохраните текущую конфигурацию в загрузочную конфигурацию.

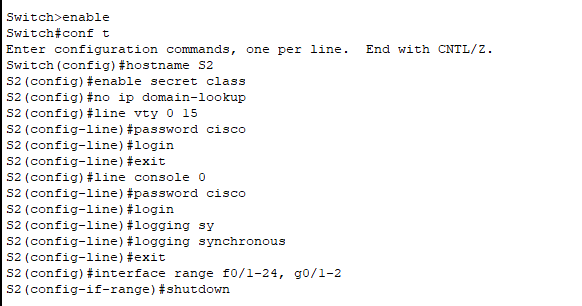
**Настройка коммутатора S1:**

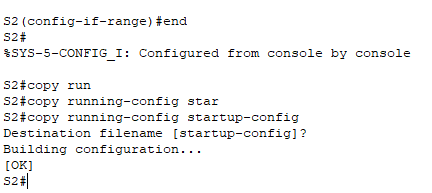
****

****

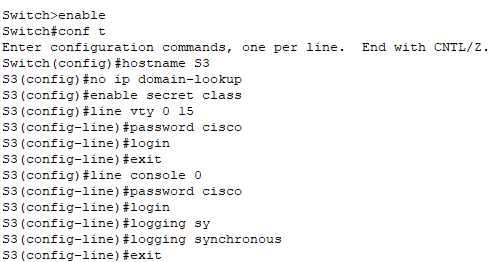
****

**Настройка коммутатора S2:**

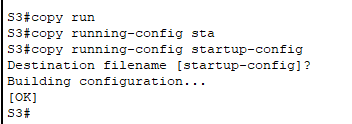
****

****

**Настройка коммутатора S3:**

****

****

****

# Часть 2: Настройка сетей VLAN, native VLAN и транковых каналов

В части 2 рассматриваются создание сетей VLAN, назначения сетям VLAN портов коммутатора, настройка транковых портов и изменение native VLAN для всех коммутаторов.

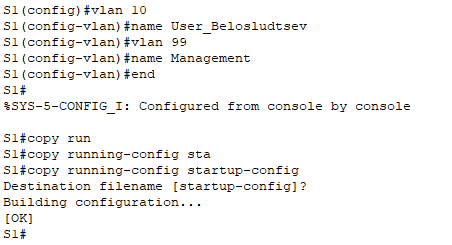
**Примечание**. Команды, необходимые для работы по части 2, указаны в Приложении А. Проверьте свои знания и попытайтесь настроить сети VLAN, сеть VLAN с нетегированным трафиком

и магистрали, не заглядывая в это приложение.

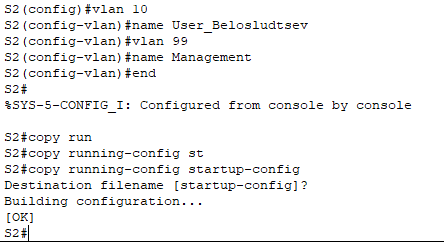
## Шаг 1: Создайте сети VLAN.

Используйте соответствующие команды, чтобы создать сети VLAN 10 и 99 на всех коммутаторах. Присвойте сети VLAN 10 имя **User\_ФАМИЛИЯ**, а сети VLAN 99 — имя **Management**.

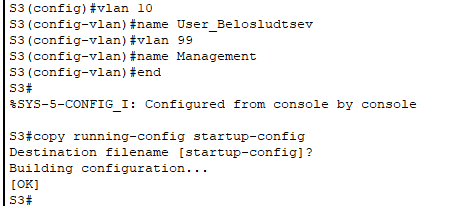
**Настройка коммутатора S1:**

****

**Настройка коммутатора S2:**

****

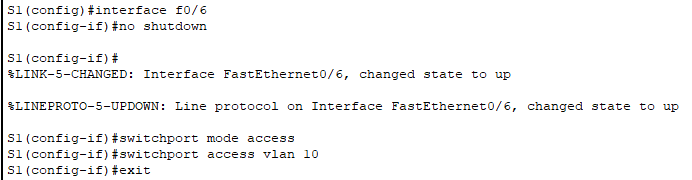
**Настройка коммутатора S3:**

****

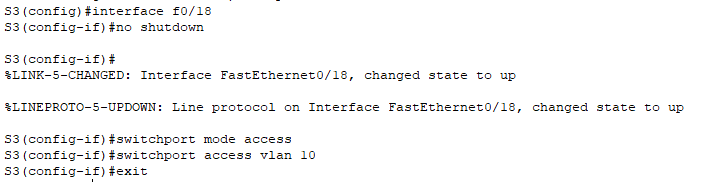
## Шаг 2: Переведите пользовательские порты в режим доступа и назначьте сети VLAN.

Для интерфейса F0/6 S1\_ФАМИЛИЯ и интерфейса F0/18 S3 включите порты, настройте их в качестве портов доступа и назначьте их сети VLAN 10.

**Настройка коммутатора S1:**



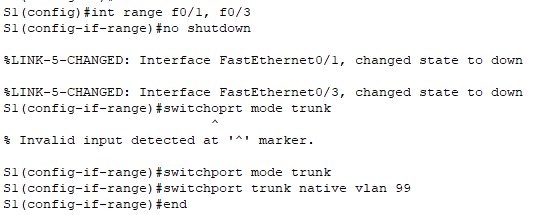
**Настройка коммутатора S3:**

****

## Шаг 3: Настройте транковые порты и назначьте их сети native VLAN 99.

Для портов F0/1 и F0/3 на всех коммутаторах включите порты, настройте их в качестве транковых и назначьте их сети native VLAN 99.

**Настройка коммутатора S1:**

****

**Настройка коммутатора S2:**

****

****

**Настройка коммутатора S3:**

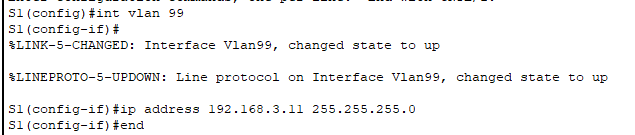
****

****

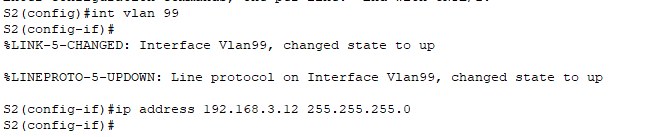
## Шаг 4: Настройте административный интерфейс на всех коммутаторах.

Используя таблицу адресации, настройте на всех коммутаторах административный интерфейс с соответствующим IP-адресом.

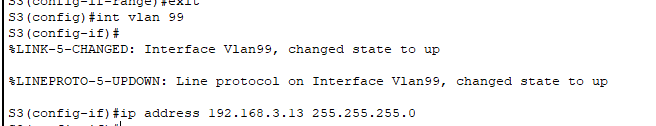
**Настройка коммутатора S1:**

****

**Настройка коммутатора S2:**

****

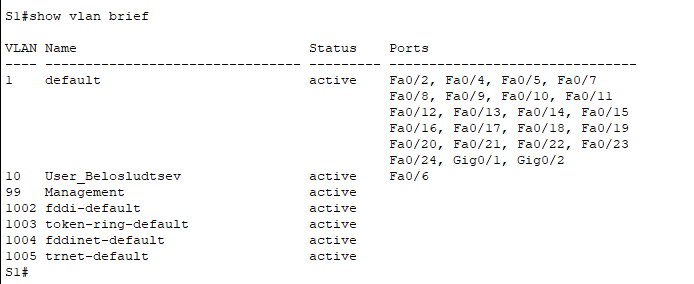
**Настройка коммутатора S3:**

****

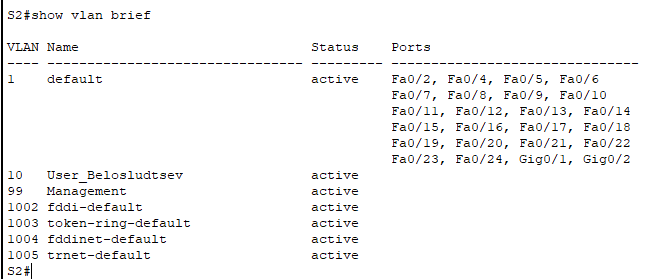
## Шаг 5: Проверка конфигураций и возможности подключения.

Используйте команду **show vlan brief** на всех коммутаторах, чтобы убедиться в том, что все сети VLAN внесены в таблицу VLAN и назначены правильные порты.

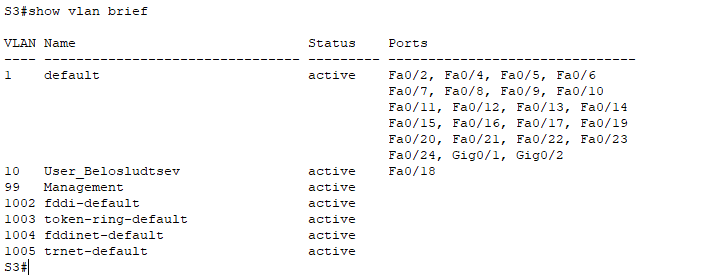
**Коммутатор S1:**

****

**Коммутатор S2:**

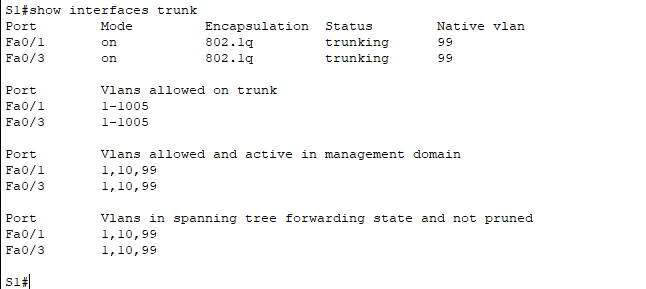
****

**Коммутатор S3:**

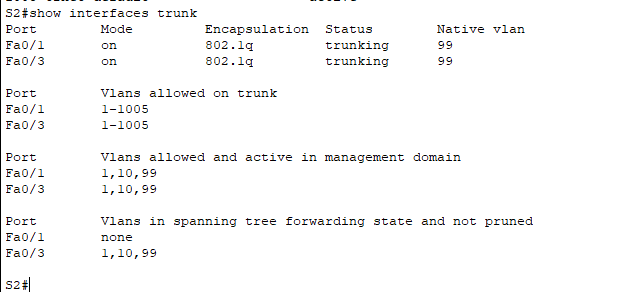
****

Используйте команду **show interfaces trunk** на всех коммутаторах для проверки магистральных интерфейсов.

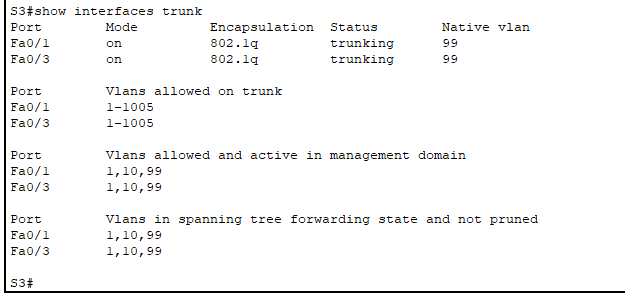
**Коммутатор S1:**

****

**Коммутатор S2:**

****

**Коммутатор S3:**

****

Используйте команду **show running-config** на всех коммутаторах, чтобы проверить все остальные конфигурации.

**Коммутатор S1:**

****

****

**Коммутатор S2:**

****

****

**Коммутатор S3:**

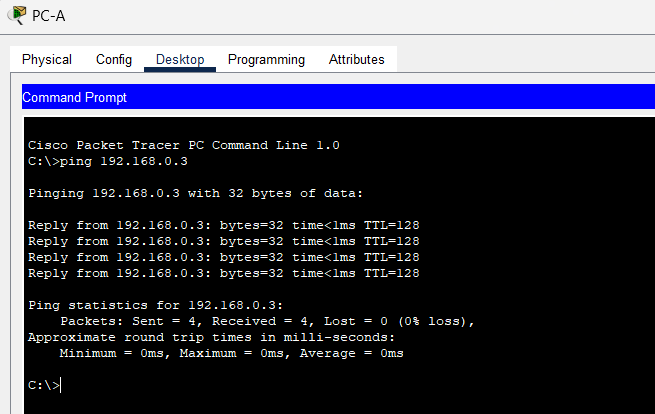
****

****

Какие настройки используются для режима протокола spanning-tree на коммутаторах Cisco?

Проверьте подключение между компьютерами PC-A и PC-C. Удалось ли получить ответ на эхо-запрос?

Если эхо-запрос выполнить не удалось, следует выполнять отладку до тех пор, пока проблема не будет решена.



# Часть 3: Настройка корневого моста и проверка сходимости PVST+

В части 3 вам предстоит определить корневой мост по умолчанию в сети, назначить основной

и вспомогательный корневые мосты и использовать команду **debug** для проверки сходимости PVST+.

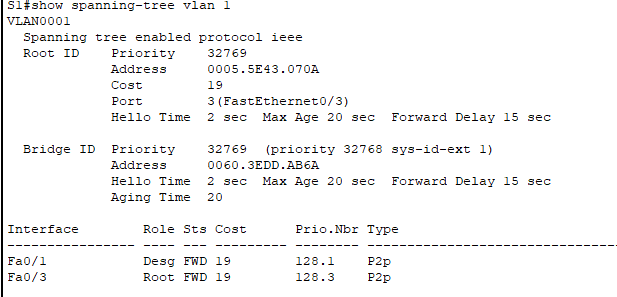
## Шаг 1: Определите текущий корневой мост.

С помощью какой команды пользователи определяют состояние протокола spanning-tree коммутатора Cisco Catalyst для всех сетей VLAN? Запишите команду в строке ниже.

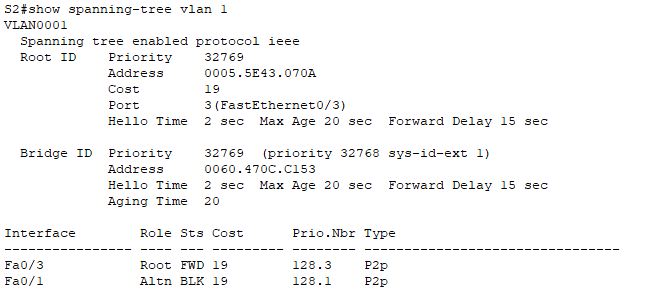
**show spanning-tree vlan 1**

Выполните команду на всех трех коммутаторах, чтобы ответить на следующие вопросы:

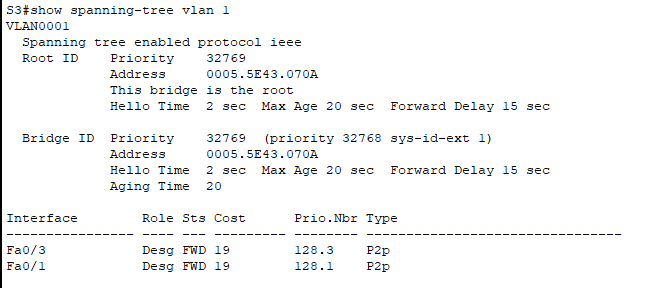
**Коммутатор S1:**



**Коммутатор S2:**

****

**Коммутатор S3:**



**Примечание**. На каждом коммутаторе доступно три экземпляра протокола spanning-tree. По умолчанию на коммутаторах Cisco используется конфигурация STP PVST+, которая позволяет создавать отдельный экземпляр протокола spanning-tree для каждой сети VLAN (VLAN 1 и все остальные настроенные пользователем сети VLAN).

Каков приоритет моста коммутатора S1\_ФАМИЛИЯ для сети VLAN 1?



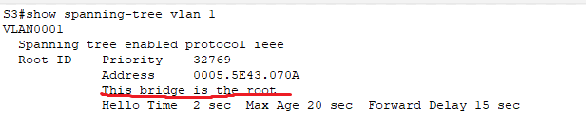
Каков приоритет моста коммутатора S2 для сети VLAN 1?



Каков приоритет моста коммутатора S3 для сети VLAN 1?



Какой коммутатор является корневым мостом?



Почему этот коммутатор выбран в качестве корневого моста?

**- Выбор делается на основе самого низкого MAC-адреса**

## Шаг 2: Настройте основной и вспомогательный корневые мосты для всех существующих сетей VLAN.

При выборе корневого моста (коммутатора) по MAC-адресу может образоваться условно оптимальная конфигурация. В этой лабораторной работе вам необходимо настроить коммутатор S2 в качестве корневого моста и коммутатор S1\_ФАМИЛИЯ — в качестве вспомогательного корневого моста.

1. Настройте коммутатор S2 в качестве основного корневого моста для всех существующих сетей VLAN. Запишите команду в строке ниже.

**spanning-tree vlan 1,10,99 root primary**

****

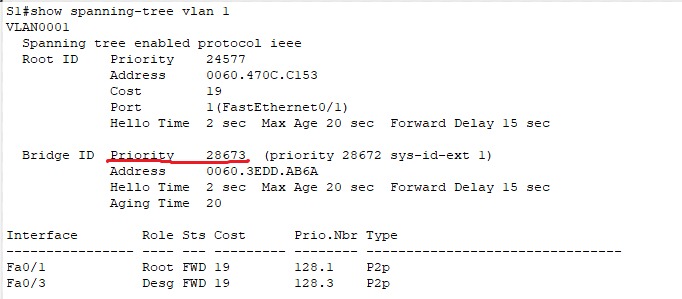
1. Настройте коммутатор S1\_ФАМИЛИЯ в качестве вспомогательного корневого моста для всех существующих сетей VLAN. Запишите команду в строке ниже.

**spanning-tree vlan 1,10,99 root secondary**

****

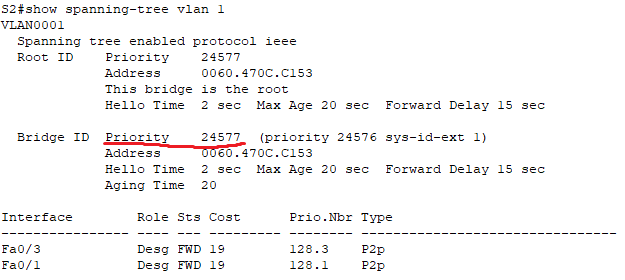
Используйте команду **show spanning-tree** для ответа на следующие вопросы:

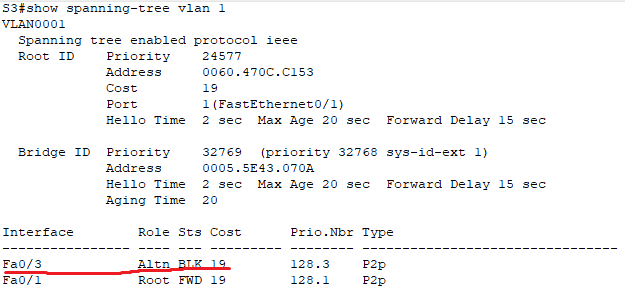
Какой приоритет моста используется для коммутатора S1\_ФАМИЛИЯ в сети VLAN 1?



Какой приоритет моста используется для коммутатора S2 в сети VLAN 1?

Какой интерфейс в сети находится в состоянии блокировки?





## Шаг 3: Измените топологию 2-го уровня и проверьте сходимость.

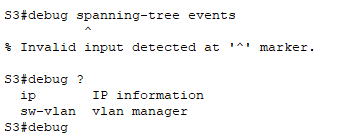
Чтобы проверить сходимость PVST+, необходимо создать изменение топологии 2-го уровня, используя команду **debug** для отслеживания событий протокола spanning-tree.

1. Выполните команду **debug spanning-tree events** в привилегированном режиме на коммутаторе S3.

**Примечание**. Прежде чем продолжить, исходя из выходных данных команды **debug** убедитесь, что все сети VLAN на интерфейсе F0/3 перешли в состояние пересылки, после чего используйте команду **no debug spanning-tree events**, чтобы остановить вывод данных командой **debug**.

Через какие состояния портов проходит каждая сеть VLAN на интерфейсе F0/3 в процессе схождения сети?

Используя временную метку из первого и последнего сообщений отладки STP, рассчитайте время (округляя до секунды), которое потребовалось для схождения сети. **Рекомендация**. Формат временной метки сообщений отладки: чч.мм.сс.мс



# Часть 4: Настройка Rapid PVST+, PortFast, BPDU Guard и проверка сходимости

В части 4 вам предстоит настроить Rapid PVST+ на всех коммутаторах. Вам необходимо будет настроить функции PortFast и BPDU guard на всех портах доступа, а затем использовать команду **debug** для проверки сходимости Rapid PVST+.

## Шаг 1: Настройте Rapid PVST+.

1. Настройте S1 для использования Rapid PVST+. Запишите команду в строке ниже.

**spanning-tree mode rapid-pvst**

****

1. Настройте коммутаторы S2 и S3 для Rapid PVST+.

**Коммутатор S2:**



**Коммутатор S3:**



1. Проверьте конфигурации с помощью команды **show running-config | include spanning-tree mode**.

**Коммутатор S1:**

****

**Коммутатор S2:**

****

**Коммутатор S3:**

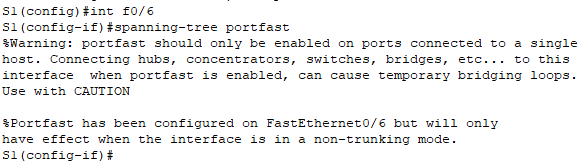
****

## Шаг 2: Настройте PortFast и BPDU Guard на портах доступа.

PortFast является функцией протокола spanning-tree, которая переводит порт в состояние пересылки сразу после его включения. Эту функцию рекомендуется использовать при подключении узлов, чтобы они могли начать обмен данными по сети VLAN немедленно, не дожидаясь протокола spanning-tree. Чтобы запретить портам, настроенным с использованием PortFast, пересылать кадры BPDU, которые могут изменить топологию протокола spanning-tree, можно включить функцию BPDU guard. После получения BPDU функция BPDU Guard отключает порт, настроенный с помощью функции PortFast.

1. Настройте F0/6 на S1\_ФАМИЛИЯ с помощью функции PortFast. Запишите команду в строке ниже.

**spanning-tree portfast**

****

1. Настройте F0/6 на S1\_ФАМИЛИЯ с помощью функции BPDU Guard. Запишите команду в строке ниже.

**spanning-tree bpduguard enable**

****

1. Глобально настройте все нетранковые порты на коммутаторе S3 с помощью функции PortFast. Запишите команду в строке ниже.

spanning-tree portfast default



1. Глобально настройте все нетранковые порты на коммутаторе S3 с помощью функции BPDU. Запишите команду в строке ниже.

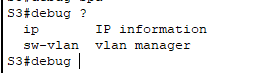
spanning-tree portfast bpduguard default



## Шаг 3: Проверьте сходимость Rapid PVST+.

1. Выполните команду **debug spanning-tree events** в привилегированном режиме на коммутаторе S3.
2. Измените топологию, отключив интерфейс F0/1 на коммутаторе S3.

Используя временную метку из первого и последнего сообщений отладки RSTP, рассчитайте время, которое потребовалось для схождения сети

.

**Вопросы для защиты теоретической части (глава 12)**

1. **Опишите преимущества беспроводной связи. Кратко охарактеризуйте основные типы беспроводной связи.**

* Гибкость и мобильность: Позволяет передавать данные без необходимости использования проводов, что обеспечивает свободу перемещения для устройств и пользователей.
* Удобство установки: Не требует сложной установки проводов, что упрощает развертывание сетей в различных местах.
* Экономия ресурсов: Сокращает расходы на проводную инфраструктуру, так как не требуется прокладка кабелей.
* Расширяемость: Позволяет легко добавлять новые устройства в сеть без необходимости расширения проводной инфраструктуры.

Основные типы беспроводной связи включают:

* Wi-Fi (беспроводные локальные сети): Используется для беспроводного подключения устройств к сети Интернет в домах, офисах, общественных местах и т.д.
* Bluetooth: Применяется для краткодистанционной связи между устройствами, такими как смартфоны, наушники, клавиатуры и другие периферийные устройства.
* Cellular (мобильная связь): Обеспечивает подключение к Интернету через мобильные сети с использованием сотовых телефонов, планшетов и других поддерживающих устройств.
* RFID (радиочастотная идентификация): Используется для идентификации и отслеживания объектов с помощью радиочастотных меток.
* NFC (ближняя беспроводная связь): Применяется для обмена данными на короткие дистанции, например, для бесконтактной оплаты или передачи информации между устройствами.
* Zigbee и Z-Wave: Протоколы, используемые для создания сетей умного дома и для управления различными устройствами в домашней автоматизации.

1. **В каких случаях используются технологии Bluetooth и спутниковая широкополосная связь? Для чего была разработана технология MIMO?**

Bluetooth используется для подключения периферийных устройств к компьютерам и смартфонам, обмена данными между мобильными устройствами, а также для управления умными устройствами.

Спутниковая широкополосная связь применяется для навигации (GPS) и глобальной коммуникации в удаленных или недоступных для проводной связи местах.

Технология MIMO разработана для увеличения пропускной способности, повышения надежности и улучшения покрытия беспроводных сетей.

1. **Какие роли может выполнять домашний беспроводной маршрутизатор? Для чего нужны беспроводные точки доступа?**

Домашний беспроводной маршрутизатор может выполнять следующие роли:

* Маршрутизация: Он направляет сетевой трафик между устройствами в локальной сети и внешней сетью, такой как Интернет.
* Беспроводной доступ: Обеспечивает беспроводное подключение устройств к сети через Wi-Fi.
* Безопасность: Может предоставлять функции защиты сети, такие как брандмауэр и шифрование данных.

Беспроводные точки доступа используются для расширения зоны покрытия беспроводной сети. Они позволяют увеличить диапазон действия Wi-Fi и обеспечивают более равномерное распределение сигнала в больших помещениях или на больших территориях.

1. **Назовите и охарактеризуйте категории точек доступа. Перечислите и опишите варианты антенн для беспроводных устройств.**

Категории точек доступа:

* Домашние: Для домашнего использования с базовыми функциями безопасности и ограниченным диапазоном покрытия.
* Бизнес: Для коммерческих помещений с расширенными функциями управления и большим диапазоном покрытия.
* Облачные: Управляемые через облачные сервисы для удаленного мониторинга и управления.

Варианты антенн:

* Омни-антенна: Равномерное покрытие во всех направлениях.
* Направленная антенна: Увеличение дальности сигнала в определенном направлении.
* Секторная антенна: Широкий угол покрытия.
* Панельная антенна: Узкий, но сильный сигнал в определенном направлении.
* Дисконаправленная антенна: Высокое усиление для связи на большие расстояния.

1. **Дайте характеристику режимам топологий беспроводной сети. В чем заключается разница между BSS и ESS?**

Характеристика режимов топологий беспроводной сети:

* Ad-hoc (IBSS - Independent Basic Service Set): Устройства соединяются непосредственно друг с другом без использования центральной точки доступа. Подходит для временных сетей или сетей с небольшим количеством устройств.
* Infrastructure (BSS - Basic Service Set): Сеть, в которой устройства соединены через центральную точку доступа (AP). Это основной способ создания беспроводных сетей, таких как Wi-Fi.

Разница между BSS и ESS:

* BSS (Basic Service Set): Это базовый элемент беспроводной инфраструктуры, состоящий из точки доступа и всех подключенных к ней устройств. BSS обеспечивает соединение между устройствами в пределах одной ячейки покрытия.
* ESS (Extended Service Set): Это объединение нескольких BSS через мосты или проводную сеть. ESS позволяет устройствам перемещаться между разными BSS внутри сети, обеспечивая непрерывное беспроводное соединение при перемещении пользователя.

1. **Опишите принцип работы беспроводного клиента при использовании метода CSMA/CA. В чем разница между пассивным и активным обнаружением точек доступа?**

Принцип работы беспроводного клиента с методом CSMA/CA:

CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance): Перед отправкой данных беспроводной клиент слушает канал на наличие активности. Если канал свободен, клиент начинает передачу данных. Если канал занят, клиент ждет случайное время и повторяет процесс.

Разница между пассивным и активным обнаружением точек доступа:

* Пассивное обнаружение точек доступа: Беспроводной клиент мониторит эфир на наличие сигналов от точек доступа без активной отправки запросов. Это более скрытый метод обнаружения, но требует длительного времени для поиска доступных сетей.
* Активное обнаружение точек доступа: Беспроводной клиент активно отправляет запросы на поиск сетей, отправляя запросы на частоты Wi-Fi-сетей. Это более быстрый метод обнаружения, но может быть более заметным для других устройств в сети.

1. **Опишите назначение протокола CAPWAP. Назовите основные рекомендации по установке точек доступа.**

Протокол CAPWAP (Control and Provisioning of Wireless Access Points) предназначен для управления и настройки беспроводными точками доступа (AP) в распределенных беспроводных сетях. Он обеспечивает следующие функции:

* Конфигурация и управление точками доступа: CAPWAP позволяет централизованно управлять настройками и обновлениями программного обеспечения для всех точек доступа в сети.
* Мониторинг и отладка: Протокол предоставляет возможности для мониторинга состояния и производительности точек доступа, а также для выявления проблем и их устранения.
* Безопасность: CAPWAP обеспечивает механизмы шифрования и аутентификации для защиты передаваемой информации и предотвращения несанкционированного доступа к устройствам.

Основные рекомендации по установке точек доступа включают:

* Выбор оптимального расположения: Разместите точку доступа в центре зоны покрытия, чтобы обеспечить равномерное покрытие всей области.
* Избегайте помех: Установите точку доступа вдалеке от других устройств, которые могут создавать помехи в беспроводном диапазоне, например, микроволновок или беспроводных телефонов.
* Настройка безопасности: Включите шифрование Wi-Fi (например, WPA2) и установите надежные пароли для защиты сети от несанкционированного доступа.
* Регулярное обновление ПО: Поддерживайте программное обеспечение точек доступа в актуальном состоянии, чтобы исправлять уязвимости и обеспечивать стабильную работу.
* Мониторинг производительности: Регулярно мониторьте производительность сети и точек доступа, чтобы быстро реагировать на проблемы и оптимизировать работу сети.

1. **Опишите основные угрозы при использовании беспроводных точек доступа. Какие бывают типы аутентификации в беспроводной связи?**

Основные угрозы при использовании беспроводных точек доступа включают:

* Несанкционированный доступ (Unauthorized Access): Злоумышленники могут попытаться подключиться к беспроводной сети без разрешения, используя украденные учетные данные или взломанные ключи безопасности.
* Перехват данных (Data Interception): Злоумышленники могут пытаться перехватывать передаваемую по беспроводной сети информацию, такую как личные данные, пароли или конфиденциальные документы.
* Атаки на сервисы (Service Attacks): К злоумышленникам могут быть направлены атаки, целью которых является нарушение работы беспроводной сети, например, атаки на отказ в обслуживании (DoS) или атаки на переполнение буфера (Buffer Overflow).
* Фальшивые точки доступа (Rogue Access Points): Злоумышленники могут размещать фальшивые точки доступа, которые пытаются подменить настоящие сети для перехвата трафика или кражи учетных данных.
* Атаки на службу аутентификации (Authentication Service Attacks): Злоумышленники могут атаковать службы аутентификации, чтобы получить несанкционированный доступ к сети или прервать ее работу.

Типы аутентификации в беспроводной связи включают:

* Открытая система (Open System): Все устройства могут подключиться к сети без аутентификации.
* WEP (Wired Equivalent Privacy): Устаревший протокол шифрования, который использует общий ключ для аутентификации и шифрования данных.
* WPA (Wi-Fi Protected Access): Более безопасный протокол, который использует персональные и предварительно распределенные ключи для шифрования данных.
* WPA2 (Wi-Fi Protected Access 2): Еще более безопасный протокол, который использует аутентификацию с помощью протокола EAP (Extensible Authentication Protocol) и AES (Advanced Encryption Standard) для шифрования данных.
* WPA3 (Wi-Fi Protected Access 3): Последняя версия протокола WPA, которая предлагает более надежную защиту с помощью более сложных методов шифрования и аутентификации.

1. **Для чего используется протокол RADIUS? Опишите методы аутентификации домашнего пользователя.**

Протокол RADIUS (Remote Authentication Dial-In User Service) используется для централизованной аутентификации, авторизации и учета пользователей, подключающихся к сети. Он часто применяется в корпоративных сетях, интернет-провайдерах и беспроводных сетях для обеспечения безопасного доступа.

Методы аутентификации домашнего пользователя включают:

* Использование пароля (Password-based authentication): Пользователь предоставляет идентификационное имя и пароль для проверки подлинности.
* Ключевые карты (Token-based authentication): Пользователь использует уникальный физический токен (например, смарт-карту или USB-ключ) для подтверждения своей личности.
* Биометрическая аутентификация (Biometric authentication): Пользователь использует биометрические данные (например, отпечаток пальца или распознавание лица) для проверки подлинности.
* Сертификаты (Certificate-based authentication): Пользователь использует цифровой сертификат для аутентификации, который был выдан доверенным центром сертификации.