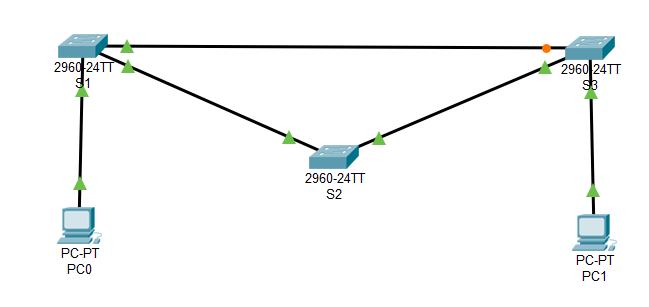
Практическая работа №8. Настройка Rapid PVST+, PortFast и BPDU Guard

## Топология

****

**Таблица адресации**

|  |  |  |  |
| --- | --- | --- | --- |
| **Устройство** | **Интерфейс** | **IP-адрес** | **Маска подсети** |
| S1\_ Shestakov | VLAN 99 | 192.168.28.11 | 255.255.255.0 |
| S2 | VLAN 99 | 192.168.28.12 | 255.255.255.0 |
| S3 | VLAN 99 | 192.168.28.13 | 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\_Shestakov |
| 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.

Изображение выглядит как текст, снимок экрана, Шрифт, число

Автоматически созданное описание Изображение выглядит как текст, документ, снимок экрана

Автоматически созданное описание

# 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**.

### 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.

Изображение выглядит как текст, снимок экрана, линия

Автоматически созданное описание

### 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.

Изображение выглядит как текст, снимок экрана

Автоматически созданное описание

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

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

### 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.

Изображение выглядит как текст, снимок экрана, программное обеспечение, линия

Автоматически созданное описание

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

Изображение выглядит как текст, программное обеспечение, снимок экрана

Автоматически созданное описание

# 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.

Изображение выглядит как текст, снимок экрана, программное обеспечение, число

Автоматически созданное описание

### 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 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.

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

Изображение выглядит как текст, снимок экрана, программное обеспечение, число

Автоматически созданное описание

### 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.

a. 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**.

Изображение выглядит как текст, Шрифт, снимок экрана, белый

Автоматически созданное описание

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

Изображение выглядит как текст, снимок экрана, Шрифт, линия

Автоматически созданное описание

### 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.

Изображение выглядит как текст, Шрифт, снимок экрана, белый

Автоматически созданное описание

**Ответы на контрольные вопросы**

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

WLAN делает возможной мобильность в домашней и деловой среде. Беспроводная инфраструктура может адаптироваться к быстро меняющимся потребностям и технологиям.

**4 типа беспроводной связи:**

1. **Беспроводные персональные сети (WPAN)** – используют маломощные передатчики для сетей ближнего действия, обычно от 20 до 30 футов (от 6 до 9 метров). Устройства на базе Bluetooth и ZigBee обычно используются в WPAN. WPAN основаны на стандарте 802.15 и частоте 2,4 ГГц.
2. **Беспроводные локальные сети (WLAN)** – использует передатчики для покрытия сети среднего размера, обычно до 100 метров. Беспроводные локальные сети подходят для использования дома, в офисе и даже в кампусе. Сети WLAN основаны на стандарте 802.11 и частоте 2,4 ГГц или 5 ГГц.
3. **Беспроводные MAN (WMAN)** – использует передатчики для предоставления услуг беспроводной связи в большой географической зоне. WMAN подходят для обеспечения беспроводного доступа к столичному городу или конкретному району. WMAN используют определенные лицензированные частоты.
4. **Беспроводные глобальные сети (WWANs)** – использует передатчики для обеспечения покрытия в обширной географической области. WWAN подходят для национальных и глобальных коммуникаций. WWAN также используют определенные лицензированные частоты.
5. **В каких случаях используются технологии Bluetooth и спутниковая широкополосная связь? Для чего была разработана технология MIMO?**

**Bluetooth** – стандарт IEEE 802.15 WPAN, использующий процесс сопряжения устройств для связи на расстоянии до 100 м. Его можно найти в устройствах «умный дом», аудиоподключениях, автомобилях и других устройствах, требующих подключения на небольшом расстоянии.

**Спутниковая широкополосная связь** – обеспечивает сетевой доступ к удаленным объектам посредством использования направленной спутниковой антенны, которая ориентирована на определенный геостационарный спутник на орбите Земли. Как правило, эта технология отличается более высокой стоимостью и к тому же требует обеспечения прямой видимости. Обычно это дороже и требует четкого обзора. Как правило, он используется сельскими домовладельцами и предприятиями, где нет кабеля и DSL.

Некоторые из более новых стандартов, которые передают и принимают на более высоких скоростях, требуют, чтобы точки доступа (AP) и беспроводные клиенты имели несколько антенн, использующих технологию множественного входа и множественного выхода (**MIMO**). MIMO использует несколько антенн в качестве передатчика и приемника для улучшения характеристик связи. Может поддерживаться до четырех антенн.

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

Беспроводной маршрутизатор служит как:

* Точка доступа – обеспечивает беспроводной доступ 802.11a/b/g/n/ac.
* Коммутатор – обеспечивает четырехпортовый полнодуплексный Ethernet-коммутатор 10/100/1000 для подключения проводных устройств
* Маршрутизатор – обеспечивает шлюз по умолчанию для подключения к другим сетевым инфраструктурам, таким как Интернет.

Точки беспроводного доступа необходимы для предоставления выделенного беспроводного доступа для пользовательских устройств.

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

Точки доступа могут быть автономными и управляемыми контроллером.

**Автономные точки доступа** – это автономные устройства, настроенные с использованием интерфейса командной строки или графического интерфейса. Автономные AP полезны в ситуациях, когда в организации требуется только пара AP.

**AP на основе контроллера** – эти устройства не требуют начальной настройки и часто называются облегченными точками доступа (LAP). LAP используют протокол облегченной точки доступа (LWAPP) для связи с контроллером WLAN (WLC). Точки доступа, управляемые контроллером, рекомендуется использовать в случаях, когда в сети требуется много точек доступа. Поскольку больше AP добавлено, каждый AP автоматически настраивается и управляется WLC.

**Варианты антенн для беспроводных устройств:**

* **Всенаправленные антенны** обеспечивают 360-градусный охват и идеальны в домах, открытых офисных помещениях, конференц-залах и вне помещений.
* **Направленные антенны** фокусируют радиосигнал в заданном направлении. Это усиливает сигнал к и от точки доступа в направлении, на которое указывает антенна. Это обеспечивает более сильный уровень сигнала в одном направлении и пониженный уровень сигнала во всех других направлениях.
* Несколько выходов (**MIMO антенна**) использует несколько антенн для увеличения доступной полосы пропускания для беспроводных сетей IEEE 802.11n/ac/ax. Для увеличения пропускной способности можно использовать до восьми передающих и принимающих антенн.

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

Режимы топологии беспроводной сети:

* **Ad hoc Режим** используется, когда два устройства подключаются по беспроводной сети в одноранговой (P2P) манере без использования точек доступа или беспроводных маршрутизаторов.
* **Инфраструктурный режим** – это когда беспроводные клиенты соединяются через беспроводной маршрутизатор или точку доступа, например, в WLAN. Точки доступа подключаются к сетевой инфраструктуре с помощью проводной системы распределения, например, Ethernet.
* **Режим модема (**использование мобильного телефона в качестве точки доступа в Интернет) – смартфон или планшет с сотовым доступом к данным включен для создания личной точки доступа. Точка беспроводного доступа является временным краткосрочным решением, благодаря которому смартфон может обеспечивать сервисы беспроводной связи Wi-Fi-маршрутизатора. Другие устройства могут подключаться и проверять подлинность со смартфоном для использования интернет-соединения.

Режим инфраструктуры определяет два строительных блока топологии: базовый набор услуг (BSS) и расширенный набор услуг (ESS).

**Базовый набор сервисов** **(BSS)** состоит из одной точки доступа, которая взаимодействует со всеми связанными беспроводными клиентами.

**Расширенный набор сервисов (ESS)** – это объединение двух или более BSS, связанных между собой проводным DS. Когда одна BSS обеспечивает недостаточное покрытие, две или более BSS могут быть объединены через общую систему распределения (DS) в ESS.

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

WLAN используют многостанционный доступ с контролем несущей и предотвращение коллизий (CSMA/CA) в качестве метода определения того, как и когда отправлять данные в сеть. Беспроводной клиент делает следующее:

1. Прослушивает канал, чтобы увидеть, не занят ли он, что означает, что он чувствует, что в данный момент на канале нет другого трафика. Канал также называется несущей.
2. Отправляет сообщение о готовности к отправке (RTS) в точку доступа для запроса выделенного доступа к сети.
3. Получает сообщение очистки для отправки (CTS) от точки доступа, предоставляющей доступ к отправке.
4. Если беспроводной клиент не получает сообщение CTS, он ожидает случайное количество времени, прежде чем перезапустить процесс.
5. После того, как он получает CTS, он передает данные.
6. Все передачи подтверждены. Если беспроводной клиент не получает подтверждение, он предполагает, что произошло столкновение, и перезапускает процесс.

В **пассивном режиме** AP открыто объявляет о своей услуге, периодически отправляя кадры широковещательного маяка, содержащие SSID, поддерживаемые стандарты и настройки безопасности. Основная цель маяка состоит в том, чтобы позволить беспроводным клиентам узнавать, какие сети и точки доступа доступны в данной области. Это позволяет беспроводным клиентам выбирать, какую сеть и точку доступа использовать.

В **активном режиме** беспроводные клиенты должны знать имя SSID. Беспроводной клиент инициирует процесс путем отправки по широковещательной рассылке кадра запроса поиска на несколько каналов. Запрос поиска содержит имя SSID и сведения о поддерживаемых стандартах. AP, настроенные с SSID, отправят ответ на запрос, который включает SSID, поддерживаемые стандарты и параметры безопасности. Активный режим может понадобиться в том случае, если для беспроводного маршрутизатора или точки доступа настроен запрет широковещательной рассылки кадров сигнала.

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

**CAPWAP** - это стандартный протокол IEEE, который позволяет WLC управлять несколькими точками доступа и WLAN. CAPWAP также отвечает за инкапсуляцию и пересылку клиентского трафика WLAN между AP и WLC.

При планировании местоположения точек доступа важна приблизительная круговая зона покрытия, но есть несколько дополнительных рекомендаций:

* Если точки доступа должны использовать существующие кабельные системы, или присутствуют расположения, где нельзя разместить точки доступа, следует отметить эти места на карте;
* Обратите внимание на все потенциальные источники помех, которые могут включать микроволновые печи, беспроводные видеокамеры, флуоресцентные лампы, детекторы движения или любое другое устройство, использующее диапазон 2,4 ГГц.
* Точки доступа следует размещать выше физических препятствий;
* По возможности размещать точки доступа вертикально рядом с потолком в центре каждой зоны;
* Размещать AP в тех местах, где будут находиться пользователи.

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

Беспроводные сети особенно подвержены следующим угрозам:

* Перехват данных - беспроводные данные должны быть зашифрованы для предотвращения их перехвата.
* Беспроводные нарушители - неавторизованные пользователи, пытающиеся получить доступ к сетевым ресурсам, могут быть предотвращены с помощью эффективных методов аутентификации.
* Атаки типа «отказ в обслуживании» (DoS) - Доступ к услугам WLAN может быть скомпрометирован случайно или злонамеренно. Существуют различные решения в зависимости от источника атаки DoS.
* Вредоносные точки доступа - Несанкционированные точки доступа, установленные благонамеренными пользователями или в злонамеренных целях, можно обнаружить с помощью программного обеспечения для управления.

**Типы аутентификации в беспроводной связи:**

1. Открытая аутентификация. Рабочая станция делает запрос аутентификации, в котором присутствует только MAC-адрес клиента. Точка доступа отвечает либо отказом, либо подтверждением аутентификации.
2. Аутентификация с общим ключом. Необходимо настроить статический ключ шифрования алгоритма WEP.
3. Wi-Fi Protected Access (WPA). Существуют два варианта аутентификации: с помощью RADIUS сервера (WPA-Enterprise) и с помощью предустановленного ключа (WPA-PSK).
4. Wi-Fi Protected Access2 (WPA2, 802.11i). В качестве основного шифра был выбран стойкий блочный шифр AES.
5. Cisco Centralized Key Managment (CCKM). Вариант аутентификации от фирмы CISCO. Поддерживает роуминг между точками доступа.
6. **Для чего используется протокол RADIUS? Опишите методы аутентификации домашнего пользователя.**

Протокол RADIUS используется для аутентификации, авторизации и учёта пользователей в сетях. Он предоставляет стандартизированный метод для проверки подлинности и предоставления доступа к сетевым ресурсам.

Домашние маршрутизаторы обычно имеют два варианта аутентификации: WPA и WPA2.