

(встал и стоит) Ачо



соглы

парковка
курсов

Прак №1

Вопросы:

1. Укажите последовательность загрузки коммутатора. Что позволяет сделать включенная функция auto-MDIX?

1. Во-первых, коммутатор загружает программу самотестирования при включении питания (POST), хранящуюся в ПЗУ. POST проверяет ЦП подсистемы. Программа тестирует ЦП, оперативную динамическую память (DRAM) и часть флеш-устройств, составляющих файловую систему флеш-памяти.
2. После этого на коммутаторе запускается программное обеспечение начального загрузчика. Начальный загрузчик — это небольшая программа, которая хранится в ПЗУ и запускается сразу после успешного завершения проверки POST.
3. Начальный загрузчик выполняет низкоуровневую инициализацию ЦП. Он инициализирует регистры ЦП, которые контролируют физическую память, количество памяти и скорость.
4. Затем программа запускает файловую систему флеш-памяти на материнской плате.
5. Наконец, начальный загрузчик находит и загружает образ операционной системы IOS по умолчанию и передаёт ей управление коммутатором.

Включённая функция auto-MDIX позволяет использовать любой тип кабеля для подключения к другим устройствам, а интерфейс автоматически настраивается для успешного взаимодействия. На новых маршрутизаторах и коммутаторах Cisco эту функцию включает команда режима конфигурации интерфейса **mdix auto**. При использовании функции auto-MDIX на интерфейсе скорость интерфейса и дуплексный режим должны быть настроены в режим **auto**, чтобы функция работала должным образом.

2. Дайте характеристику протоколам SSH и Telnet, указав принципиальную разницу между ними. Какой порт и протокол транспортного уровня используется при работе с SSH и Telnet?

Telnet — это стандартный протокол TCP / IP для службы виртуальных терминалов.

SSH — это сетевой протокол, который широко используется для удаленного доступа и управления устройством.

Telnet уязвим для атак на безопасность, а SSH помогает преодолеть многие проблемы безопасности Telnet

Telnet использует порт 23, который был разработан специально для локальных сетей, тогда как SSH по умолчанию работает на порту 22.

Telnet передает данные в виде простого текста, а в SSH данные отправляются в зашифрованном формате по защищенному каналу.

Telnet подходит для частных сетей. С другой стороны, SSH подходит для публичных сетей.

3. Дайте характеристику интерфейса loopback маршрутизатора. Какие задачи можно выполнить с помощью функции истории команд?

Интерфейс loopback — это логический интерфейс внутри маршрутизатора. Он не назначается физическому порту, поэтому его нельзя подключить к другому устройству. Он считается программным интерфейсом, который автоматически переводится в состояние up (активен) во время работы маршрутизатора.

Используется в основном для тестирования передачи данных от обслуживающего центра коммутации, проверки работы коммутационных кабелей и теста обратной петли, когда сигнал посылается и возвращается отправителю по всем коммуникационным каналам.

С помощью функции истории команд можно

- устанавливать размер буфера истории команд;
- повторно обращаться к командам;
- отключать функцию ведения истории команд.

4. Какая информация содержится в таблице MAC-адресов коммутатора?

Опишите алгоритм заполнения таблицы MAC-адресов в случае отсутствия записей в таблице.

В таблице MAC-адресов содержится информация о номере интерфейса, типе MAC-адреса (динамический [запись о нём хранится временно и если этот адрес не встречается в принятых пакетах длительное время, то удаляется из таблицы] или статический [настраивается пользователем вручную, имеет высший приоритет, не стираются и не перезаписываются из таблицы]) и портах к которым подключены устройства

По мере того, как коммутатор узнает отношение портов к устройствам, он создает таблицу MAC-адресов или таблицу ассоциативной памяти (CAM).

1. Коммутатор получает кадр от компьютера PC 1 на порте Port 1.
2. Коммутатор проверяет MAC-адрес источника и сравнивает его с таблицей MAC-адресов.

Если адрес не содержится в таблице MAC-адресов, он сопоставляет MAC-адрес источника компьютера PC 1 с входным портом (Port 1) в таблице MAC-адресов.

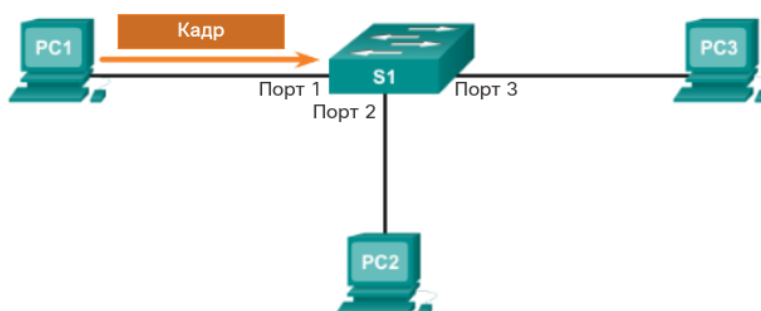
Если таблица MAC-адресов уже содержит запись для этого адреса источника, она сбрасывает таймер. Обычно запись MAC-адреса хранится в течение пяти минут.

3. После записи информации об адресе источника коммутатор проверяет MAC-адрес назначения.

Если адрес назначения не содержится в таблице MAC-адресов или представляет собой широковещательный MAC-адрес, на что указывают все F, коммутатор рассылает кадр на все порты, за исключением входного.

4. Устройство назначения (PC 3) отвечает кадром индивидуальным кадром, адресованным PC 1.
5. Коммутатор вводит MAC-адрес источника компьютера PC 3 и номер порта входного порта в таблицу адресов. Адрес назначения кадра и его соответствующий выходной порт находятся в таблице MAC-адресов.
6. Теперь коммутатор может пересылать кадры между устройствами источника и назначения без лавинной рассылки, потому что в таблице MAC-адресов есть записи, которые идентифицируют соответствующие порты.

Таблицы MAC-адресации и MAC-адресов коммутатора



5. Дайте характеристику способам пересылки на коммутаторе. При каком режиме коммутации возможна пересылка недопустимых кадров и почему?

Коммутаторы используют один из двух способов пересылки для коммутации данных между сетевыми портами:

- Коммутация с промежуточным хранением (store-and-forward)
- Сквозная коммутация (cut-through)

Коммутация с
промежуточным
хранением



Сквозная
коммутация



Коммутатор с промежуточным хранением получает кадр целиком и вычисляет циклический избыточный код (CRC). Если значение CRC правильное, коммутатор ищет адрес назначения, по которому и будет определяться исходящий интерфейс. Затем кадр перенаправляется к правильному порту.

Коммутатор со сквозной коммутацией пересылает данный кадр до его полного получения. Поэтому, как минимум, адрес назначения кадра должен быть прочтен раньше, чем кадр можно будет перенаправить.

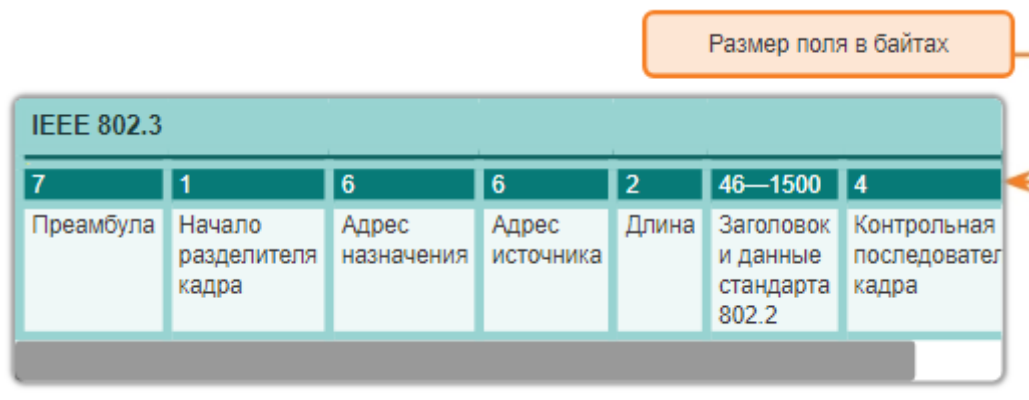
CRC использует математическую формулу, основанную на количестве бит (единиц) в кадре, что позволяет определить наличие ошибок в полученном кадре. После подтверждения целостности кадра он перенаправляется через соответствующий порт к узлу назначения. Если же в кадре обнаружена ошибка, коммутатор отбросит его

Сквозная коммутация не отбрасывает большинство недопустимых кадров. Коммутатор со сквозной коммутацией может принимать решение о пересылке сразу после нахождения MAC-адреса назначения кадра в своей таблице MAC-адресов. Коммутатору не нужно ждать остальной части кадра, поступающей через входной порт, прежде чем принять решение о пересылке.

Описания способов пересылки кадров коммутатора приведены в таблице. Нажмите на поля Store-and-Forward (с промежуточным хранением) или Cut-Through (сквозной режим), чтобы сопоставить способы пересылки с описаниями.

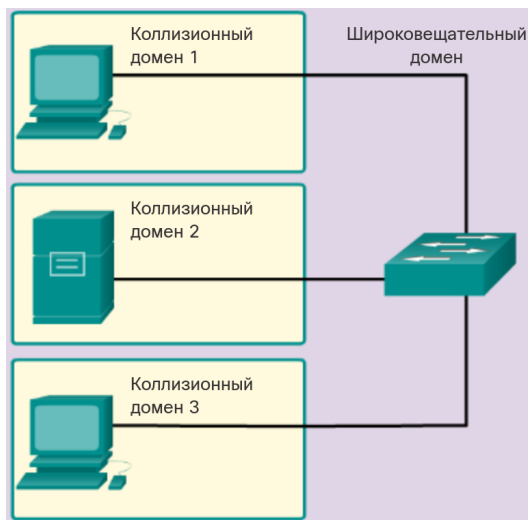
	Режим с промежуточным хранением	Сквозной режим
1. Буферизирует кадры, пока коммутатор не получит весь кадр.	✓	
2. Проверяет кадр на наличие ошибок, прежде чем выпустить его из портов коммутатора; если кадр получен не полностью, коммутатор отбрасывает его.	✓	
3. Перед выпуском кадров из портов коммутатор не выполняет проверку кадров на наличие ошибок.		✓
4. Отличный способ для сохранения полосы пропускания в сети.	✓	
5. Сетевой адаптер (NIC) назначения отбрасывает все неполные кадры с помощью этого способа пересылки кадров.		✓
6. Это более быстрый метод коммутации, но может повлечь за собой больше ошибок в целостности данных, поэтому может потребоваться больше пропускной способности.		✓

6. Перечислите и охарактеризуйте основные поля заголовка канального уровня. Дайте определение понятию "домен коллизии".



- Преамбула (Preamble). Состоит из 8 байтов. Первые семь содержат одну и ту же циклическую последовательность битов (10101010), которая хорошо подходит для синхронизации приемопередатчиков. Последний (Start-of-frame-delimiter, SFD), 1 байт (10101011), служит меткой начала информационной части кадра. Это поле не учитывается при определении длины кадра и не рассчитывается в контрольной сумме.
- MAC-адрес получателя (Destination Address, DA).
- MAC-адрес отправителя (Source Address, SA). Первый бит всегда равен нулю.
- Поле длины либо тип данных (Length/Type, L/T). Два байта, которые содержат явное указание длины (в байтах) поля данных в кадре или указывают на тип данных. Ниже, в описании LLC будет показано, что возможно простое автоматическое распознавание разных типов кадров.
- Данные (Data). Полезная нагрузка кадра, данные верхних уровней OSI. Может иметь длину от 0 до 1500 байт.
- Для корректного распознавания коллизий необходим кадр не менее чем из 64 байт. Если поле данных менее 46 байт, то кадр дополняется полем заполнения (Padding).
- Контрольная сумма (Frame Check Sequence, FCS). 4 байта, которые содержит контрольную сумму всех информационных полей кадра. Вычисление выполняется по алгоритму CRC-32 отправителем и добавляется в кадр. После приема кадра в буфер, приемник выполняет аналогичный расчет. В случае расхождения результата вычислений, предполагается ошибка при передаче, и кадр уничтожается.

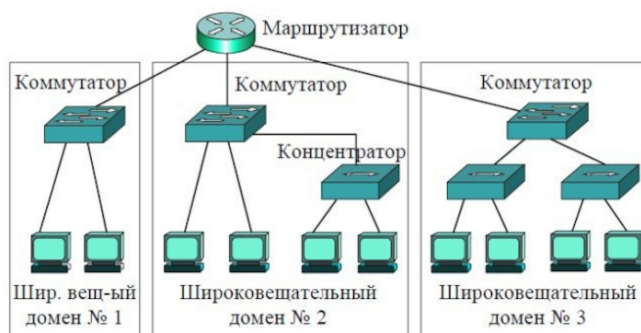
Домен коллизии - часть сети Ethernet, все узлы которой конкурируют за общую разделяемую среду передачи и, следовательно, каждый узел которой может создать коллизию с любым другим узлом этой части сети.



7. Дайте определение понятию "широковещательный домен". Какое устройство позволяет сегментировать домен широковещательной рассылки и почему?

Широковещательный домен это участок сети, в котором все узлы могут передавать данные друг другу с помощью широковещания на канальном уровне сетевой модели OSI.

С широковещательным штормом может бороться только маршрутизатор, который делит сеть на **широковещательные домены**, т.е. отдельные сети.



Устройства, ограничивающие широковещательный домен — маршрутизаторы, работающие на третьем, сетевом уровне модели OSI. Маршрутизаторы сегментируют сети на широковещательные домены, что позволяет исключить перегрузку всех устройств в сети, связанную с обработкой широковещательных пакетов.

При передаче информации между хостами, находящимися в одном широковещательном домене, проблем не возникает.

8. Опишите поведение коммутатора, который получает широковещательный кадр.

передача кадра на все порты, за исключением порта, на который поступил кадр

Какие механизмы/характеристики коммутаторов позволяют снизить нагрузку на сеть?

Полнодуплексная связь повышает производительность и снижает нагрузку коммутируемой LAN, позволяя передавать и получать данные в обоих направлениях. При этом кадры не могут столкнуться друг с другом так как используют два разных канала в сетевой кабеле.

Скорость фильтрации и продвижения кадров - это ещё две основные характеристики производительности коммутатора, которые могут помочь уменьшить перегрузку сети.

Скорость фильтрации определяет скорость, с которой коммутатор выполняет следующие этапы обработки кадров: прием кадра в свой буфер, просмотр адресной

таблицы с целью нахождения порта для адреса назначения кадра, уничтожение кадра, так как его порт назначения совпадает с портом-источником.

Скорость продвижения определяет скорость, с которой коммутатор выполняет следующие этапы обработки кадров: прием кадра в свой буфер, просмотр адресной таблицы с целью нахождения порта для адреса назначения кадра, передача кадра в сеть через найденный по адресной таблице порт назначения.

9. Какова цель буферизации кадров на коммутаторе?

При буферизации кадров присутствует возможность проверить их по контрольной сумме на наличие ошибок и, при обнаружении отбросить кадр. Также с помощью внутреннего буфера обеспечивается внутреннее хранение в тех случаях, когда невозможно немедленно передать кадр на выходной порт. Чем больше объем буферной памяти, тем менее вероятны потери кадров.

Опишите поведение коммутатора, если на одном из его портов был получен кадр с MAC-адресом назначения, которого нет в таблице MAC-адресов. (см. вопрос 4 подпункт 3)

10. Опишите основные шаги по настройке протокола SSH. Опишите поведение коммутатора, который получает кадр многоадресной рассылки.

Шаг 1. Проверка поддержки протокола SSH. (`show ip ssh`)

Шаг 2. Настройка домена IP. (`ip domain-name имя_домена`)

Шаг 3. Создание пар ключей RSA. (`crypto key generate rsa`)

Шаг 4. Настройка аутентификации пользователя. (`username имя_пользователя secret password`)

Шаг 5. Настройка каналов vty (`transport input ssh, login local`)

Шаг 6. Включите SSH версии 2. (`ip ssh version 2`)

Когда коммутатор 2-го уровня получает многоадресный трафик, он начинает передавать кадры через все порты, т.к. не находит записи о MAC-адресе в своей таблице коммутации. Это противоречит основному назначению коммутатора, которое заключается в ограничении трафика и передаче его только тем портам, к которым подключены получатели.

Управление многоадресной рассылкой на коммутаторе 2-го уровня может быть выполнено двумя способами.

Первый способ заключается в создании статических таблиц коммутации для портов, к которым не подключены подписчики многоадресных групп. Это позволяет ограничить многоадресный трафик и передавать его только через те порты, к которым подключены узлы-подписчики. Однако этот способ не позволяет динамически отслеживать добавление или исключение членов из многоадресной группы.

Вторым способом, позволяющим решить проблему лавинной передачи (flooding) многоадресных пакетов и динамически отслеживать состояние подписки узлов, является функция IGMP Snooping (IGMP-прослушивание).

11. Дайте определение понятиям "карликовый кадр" и "гигантский кадр". Как получить доступ в начальный загрузчик (режим восстановления) коммутатора?

- **Карликовые кадры (runt frames)** — кадры Ethernet, размер которых не превышает минимально разрешенные 64 байта. Карликовые кадры чаще всего бывают вызваны неисправностью сетевой платы, но могут быть обусловлены и другими причинами, например чрезмерно высоким числом коллизий.
- **Гигантские кадры (giants)** — кадры Ethernet, размер которых превышает максимальную длину кадра. Наличие гигантских кадров вызвано теми же причинами, что и наличие карликовых.

Начальная настройка параметров коммутатора Восстановление после сбоя системы

Загрузчик предоставляет доступ к коммутатору, если операционная система не может быть использована из-за отсутствия или повреждения системных файлов. Загрузчик имеет командную строку, которая обеспечивает доступ к файлам, хранящимся во флэш-памяти. Доступ в начальный загрузчик можно получить через консольное подключение, выполнив следующие действия:

Шаг 1. Подключите ПК через консольный кабель к консольному порту коммутатора. Настройка программы эмуляции терминала и подключение ПК к консольному порту

Шаг 2. Отсоедините кабель питания коммутатора.

Step 3. Повторно подключите шнур питания к коммутатору и в течение 15 секунд нажмите и удерживайте кнопку Mode, пока индикатор системы все еще мигает зеленым цветом.

Step 4. Продолжайте нажимать кнопку «Режим», пока системный светодиод не станет желтым, а затем сплошным зеленым; затем отпустите кнопку «Режим».

Step 5. В эмуляторе терминала на ПК появится запрос switch: начального загрузчика.

Командная строка начального загрузчика поддерживает команды для форматирования файловой флеш-системы, переустановки операционной системы и восстановления утерянного или забытого пароля. Например, команду `dir` можно использовать для просмотра списка файлов в указанном каталоге, как показано на рисунке.

© Cisco или Партнеры, 2016 г. Все права защищены.
Конфиденциальная информация Cisco

8

12. Дайте общую характеристику светодиодным индикаторам коммутатора. Что произойдет, что коммутатор получит «карликовый» или «гигантский» кадр?

Начальная настройка параметров коммутатора

Светодиодные индикаторы коммутатора



Системный индикатор показывает, есть ли питание системы и функционирует ли она должным образом.

Индикатор RPS. Индикатор резервного источника питания (RPS), который указывает состояние этой источника.

Индикатор состояния порта (STAT): зеленый цвет указывает, что выбран режим состояния порта, который является значением по умолчанию. Статус порта может быть понятен светом, связанным с каждым портом.

Светодиодный индикатор дуплекса порта (DUPLX):зеленый цвет указывает, что выбран режим дуплекса порта. Дуплекс порта может быть понятен светом, связанным с каждым портом.

Индикатор скорости порта (SPEED):зеленый цвет указывает, что выбран режим скорости порта. Скорость порта может быть понята светом, связанным с каждым портом.

Power over Ethernet LED (PoE):Присутствует, если коммутатор поддерживает PoE. Указывает состояние PoE портов коммутатора.

Кнопка Mode используется для перемещения между различными режимами — STAT, DUPLX, SPEED и PoE

Что происходит с «карликовыми кадрами», получаемыми коммутатором Cisco Ethernet?

*****кадры возвращаются на сетевое устройство-отправитель**

13. Перечислите 4 различных параметра фильтрации выходных данных для коммутатора и приведите примеры их применения. Каким способом можно указать количество отображаемых строк в консоли при наборе команды, которая выводит несколько экранов выходных данных?

`show` | параметр и выражение фильтрации

- **section** — показать целый раздел, который начинается с заданного фильтра.
- **include** — включить все строки выходных данных, которые соответствуют заданному фильтру.

- **exclude** — исключить все строки выходных данных, которые соответствуют заданному фильтру.
- **begin** — показать все строки выходных данных от конкретного места, начиная с линии, которая соответствует заданному фильтру

Пример: `show ip interface brief | include up`

Для указания количества отображаемых строк используйте команду **terminal length**. Значение 0 (ноль) позволяет просмотреть выходные данные без приостановки в процессе вывода данных на экран.

Прак №2

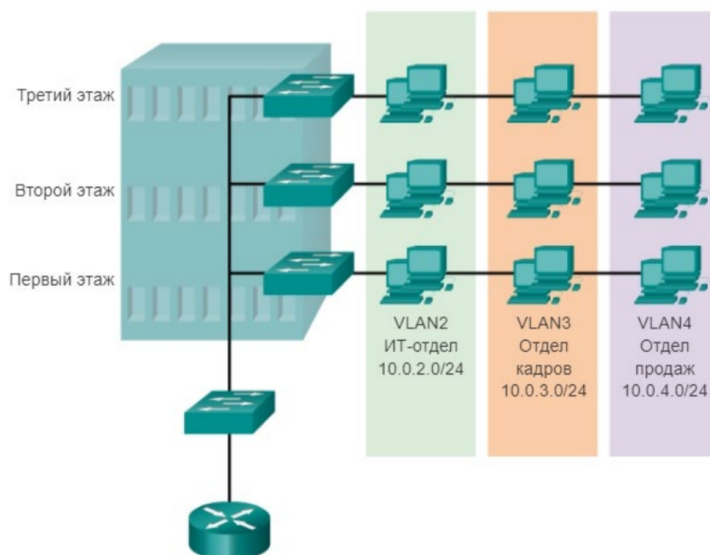
Вопросы:

1. Дайте определение понятию VLAN. В каких случаях порт коммутатора может быть назначен более чем одной сети VLAN?

Сети VLAN позволяют сгруппировать устройства внутри локальной сети. Группа устройств в пределах сети VLAN взаимодействует так, будто устройства подключены с помощью одного провода. Сети VLAN основываются не на физических, а на логических подключениях. Устройства в пределах сети VLAN работают таким образом, будто находятся в собственной независимой сети, даже если делят одну общую инфраструктуру с другими VLAN. Сеть VLAN создаёт логический широковещательный домен, который может охватывать несколько физических сегментов LAN. Если устройство в одной сети VLAN передаёт широковещательный кадр Ethernet, то этот кадр получают все устройства в рамках этой VLAN, устройства же в других сетях VLAN этот кадр не получают.

Каждый порт коммутатора может быть назначен только одной сети VLAN (за исключением порта, подключённого к IP-телефону или к другому коммутатору).

Определение групп виртуальной локальной сети (VLAN)



2. Назовите основные преимущества технологии VLAN. Дайте характеристику сети VLAN 1.

Преимущества:

- **Безопасность:** группы, обладающие уязвимыми данными, отделены от остальной части сети, благодаря чему снижается вероятность утечки конфиденциальной информации.
- **Снижение расходов:** благодаря экономии на дорогих обновлениях сетевой инфраструктуры и более эффективному использованию имеющейся полосы пропускания и восходящих каналов происходит снижение расходов.

- **Повышение производительности:** разделение однородных сетей 2-го уровня на несколько логических рабочих групп (широковещательных доменов) уменьшает количество лишнего сетевого трафика и повышает производительность.
- **Уменьшенные широковещательные домены:** разделение сети на сети VLAN уменьшает количество устройств в широковещательном домене.
- **Повышение производительности ИТ-отдела:** сети VLAN упрощают управление сетью, поскольку пользователи с аналогичными требованиями к сети используют одну и ту же сеть VLAN. Также ИТ-специалистам легче определять функцию сети VLAN, назначая ей соответствующее имя.
- **Упрощенное управление проектами и приложениями:** сети VLAN объединяют пользователей и сетевые устройства для соответствия деловым или географическим требованиям сети. Управление проектом и работа на прикладном уровне упрощены благодаря использованию разделения функций.

VLAN 1 поддерживает все функции любой сети VLAN, однако её нельзя переименовать или удалить. По умолчанию весь управляющий трафик 2-го уровня связан с сетью VLAN 1.

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	fdi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fdinet-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.

3. Дайте определение сети VLAN для данных. Каково назначение сети Native VLAN и какой она имеет номер по умолчанию?

Виртуальная локальная сеть для данных — это сеть VLAN, которая настроена специально для передачи трафика, генерируемого пользователем. Сеть VLAN, передающая голосовой трафик или трафик управления, не является сетью VLAN для передачи данных. Рекомендуется отделять голосовой и управляющий трафик от трафика данных. VLAN для передачи данных иногда называют пользовательской сетью VLAN. Сети VLAN для данных используются для разделения сети на группы пользователей или устройств.

Сеть native VLAN назначена транковому порту 802.1Q. Транковые порты — это каналы между коммутаторами, которые поддерживают передачу трафика, связанного с более чем одной сетью VLAN. Транковый порт 802.1Q поддерживает трафик, поступающий от нескольких VLAN (тегированный трафик), а также трафик, который поступает не от VLAN (нетегированный трафик). Тегированным называется трафик, для которого в исходный заголовок кадра Ethernet вставлен 4-байтовый тег, определяющий сеть VLAN, к которой относится этот кадр. Транковый порт 802.1Q размещает нетегированный трафик в сети native VLAN, которой по умолчанию является VLAN 1.

4. Дайте определение управляющей VLAN. Каково назначение управляющей VLAN и какой она имеет номер по умолчанию?

Управляющая VLAN — это любая сеть VLAN, настроенная 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, благодаря чему коммутатором можно управлять через протоколы

HTTP, Telnet, SSH или SNMP. Поскольку в исходной настройке коммутатора Cisco VLAN 1 является сетью VLAN по умолчанию, VLAN 1 не следует использовать в качестве управляющей VLAN.

5. Назовите определение магистрального канала (транка). Между какими устройствами можно организовать транковый канал?

Транк — это канал типа «точка-точка» между двумя сетевыми устройствами, который поддерживает более одной сети VLAN. Транк виртуальных сетей расширяет сети VLAN по всей сети. Cisco поддерживает стандарт IEEE 802.1Q для координации транков в интерфейсах Fast Ethernet, Gigabit Ethernet и 10-Gigabit Ethernet.

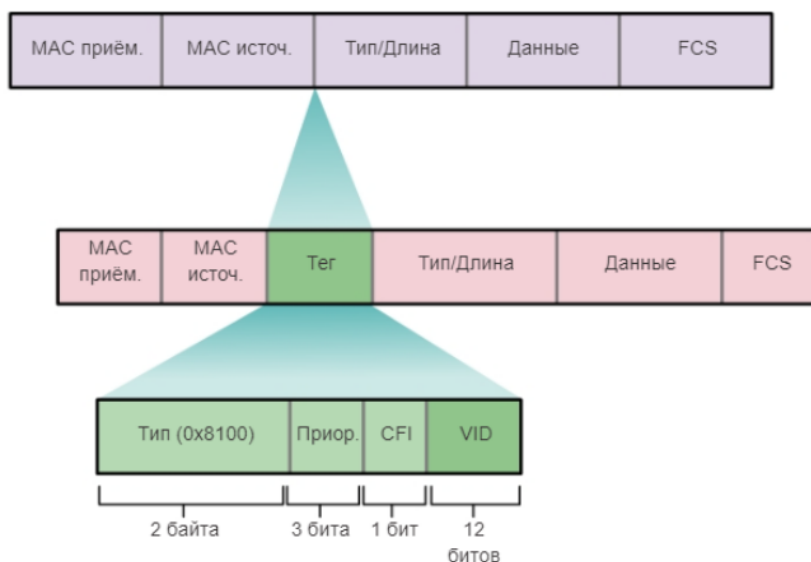
Транк может также использоваться между сетевым устройством и сервером или другим устройством, оснащённым соответствующим сетевым адаптером с поддержкой 802.1Q. По умолчанию на транковом порте коммутатора Cisco Catalyst поддерживаются все сети VLAN.

6. Опишите механизм тегирования трафика. Перечислите диапазоны VLAN на коммутаторах.

Стандартный заголовок кадра Ethernet не содержит информацию о VLAN, к которой относится кадр. Поэтому, когда кадры Ethernet размещаются в транковом канале, необходимо добавить информацию о сетях VLAN, которым они принадлежат. Этот процесс называется тегированием и выполняется с помощью заголовка IEEE 802.1Q, указанного в стандарте IEEE 802.1Q.

Когда коммутатор получает кадр через порт, настроенный в режиме доступа и назначенный сети VLAN, коммутатор добавляет в заголовок кадра метку VLAN, заново вычисляет FCS и отправляет тегированный кадр из транкового порта.

Поля в кадре Ethernet 802.1Q



Тегирование голосовой VLAN



7. Охарактеризуйте VLAN стандартного и расширенного диапазона. Опишите основные шаги по настройке транкового канала.

Виртуальные локальные сети стандартного диапазона	Сети VLAN расширенного диапазона
Используются в малых и средних сетях предприятий и организаций.	Позволяют операторам связи расширять свою инфраструктуру для большого числа клиентов.
Определяются идентификатором VLAN от 1 до 1005.	Некоторым крупным международным корпорациям нужны идентификаторы VLAN расширенного диапазона.
Идентификаторы от 1002 до 1005 зарезервированы для сетей VLAN Token Ring и FDDI.	Определяются идентификатором VLAN от 1006 до 4094.
Идентификаторы 1 и идентификаторы от 1002 до 1005 создаются автоматически и не могут быть удалены.	Конфигурации сетей не записываются в файл vlan.dat.
Конфигурации хранятся в файле базы данных VLAN под именем vlan.dat.	Поддерживают меньше функций VLAN, чем сети VLAN стандартного диапазона.
Протокол VTP (транковый протокол VLAN), помогающий управлять конфигурациями VLAN между коммутаторами, может распознавать и хранить только сети VLAN стандартного диапазона.	По умолчанию сохраняются в файл текущей конфигурации.
	Протокол VTP не распознаёт сети VLAN расширенного диапазона.

Задача	Команда IOS
Войдите в режим глобальной настройки.	Switch# configure terminal
Войдите в режим конфигурации интерфейса.	Switch(config)# interface interface-id
Установите порт в режим постоянной магистрали.	Switch(config-if)# switchport mode trunk
Установите в качестве VLAN с нетегированным трафиком сеть, отличную от VLAN 1.	Switch(config-if)# switchport trunk native vlan vlan-id
Укажите список сетей VLAN, которым разрешен доступ в магистральный канал.	Switch(config-if)# switchport trunk allowed vlan vlan-list
Вернитесь в привилегированный режим.	Switch(config-if)# end

8. Опишите назначение протокола DTP. В каких случаях стоит отключать протокол DTP и почему?

Протокол DTP позволяет коммутаторам автоматически согласовывать магистральные соединения с соседним устройством. Он действует только по принципу сквозного подключения между устройствами сети.

Некоторые межсетевые устройства могут пересылать кадры DTP неправильно, из-за чего могут возникнуть ошибки конфигурации. Чтобы этого избежать, отключите DTP на интерфейсах коммутатора Cisco, который подключён к устройствам, не поддерживающим DTP.

9. Опишите основные режимы протокола DTP, в которых может находиться интерфейс. Какие режимы протокола DTP смогут образовать магистраль с интерфейсом, настроенным на динамический автоматический режим?

Switch(config)# switchport mode { access | dynamic { auto | desirable } | trunk }

Параметр	Описание
access	Режим постоянного доступа и согласовывает преобразование соседнего канала в канал доступа
dynamic auto	Будет становиться интерфейсом магистрали, если соседний интерфейс установлен в транк или режим desirable
dynamic desirable	Активно стремится стать магистралью путем переговоров с другими auto или desirable интерфейсами
trunk	режим постоянного транкинга и согласовывает преобразование соседнего канала в trunk

	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	Ограниченные возможности подключения
Access	Access	Access	Ограниченные возможности подключения	Access

10. Каким образом можно изменить принадлежность порта сети VLAN? Что необходимо сделать перед удалением какой-либо сети VLAN и почему?

Если порт доступа коммутатора неправильно назначен VLAN, просто повторно введите команду конфигурации интерфейса **switchport access vlan vlan-id** с правильным идентификатором VLAN.

Чтобы изменить членство порта на VLAN 1 по умолчанию, используйте команду **no switchport access vlan** в режиме настройки интерфейса.

Задача	Команда
Войдите в режим глобальной настройки.	Switch# configure terminal
Войдите в режим конфигурации интерфейса.	Switch(config)# interface interface-id
Переведите порт в режим доступа.	Switch(config-if)# switchport mode access
Назначьте порт сети VLAN.	Switch(config-if)# switchport access vlan vlan-id
Вернитесь в привилегированный режим.	Switch(config-if)# end

Перед удалением сети VLAN необходимо сначала переназначить все ее порты другой сети VLAN. Все порты, которые не будут перемещены в активную VLAN, не смогут взаимодействовать с другими станциями после удаления VLAN.

11. Опишите, как происходит обработка и пересылка тегированных и нетегированных кадров в сети native VLAN. В каком типе памяти хранится информация о созданных VLAN?

Управляющий трафик, отправляемый в сети native VLAN, тегировать не следует. Если транковый порт 802.1Q получает тегированный кадр с таким же идентификатором VLAN, как у сети native VLAN, то он отбрасывает кадр.

Когда транковый порт коммутатора Cisco получает нетегированные кадры, он пересылает эти кадры в сеть native VLAN. Если с сетью native VLAN не связаны никакие устройства, а также нет других транковых портов, то кадр отбрасывается.

Сетью native VLAN по умолчанию является сеть VLAN 1. При настройке транкового порта 802.1Q порту идентификатора VLAN по умолчанию (PVID) присваивают значение идентификатора сети native VLAN. Весь нетегированный трафик, поступающий в порт 802.1Q или из него, пересылается в соответствии со значением PVID.

12. Как можно удалить конкретную VLAN из файла vlan.dat? Как можно удалить файл vlan.dat целиком и в каком случае это может быть необходимо?

Конфигурации хранятся в файле базы данных VLAN под именем vlan.dat. Файл vlan.dat расположен во флеш-памяти коммутатора.

Удалите VLAN с помощью команды **no vlan vlan-id**. Перед удалением сети VLAN необходимо сначала переназначить все ее порты другой сети VLAN.

Удалите все VLAN с помощью команды **delete flash:vlan.dat** или команды **delete vlan.dat**. Перезагрузите коммутатор после удаления всех VLAN.

Прак №3

Вопросы:

1. Что такое маршрутизация между VLAN? Какие бывают методы маршрутизации между VLAN?

VLAN используются для сегментации коммутируемых сетей уровня 2 по разным причинам. Независимо от причины, хосты в одной VLAN не могут взаимодействовать с хостами в другой VLAN, если нет маршрутизатора или коммутатора уровня 3 для предоставления услуг маршрутизации.

Маршрутизация между сетями VLAN — это процесс переадресации сетевого трафика из одной сети VLAN в другую с помощью маршрутизатора.

Существуют три варианта маршрутизации между VLAN.

- **Старый метод маршрутизации между VLAN** - это устаревшее решение. Плохо масштабируется.
- **Router-on-a-Stick** - это приемлемое решение для сети малых и средних размеров.

- **Коммутатор уровня 3 с использованием коммутируемых виртуальных интерфейсов (SVI)** — это наиболее масштабируемое решение для средних и крупных организаций.

2. Опишите устаревший метод маршрутизации между сетями VLAN. В чем заключается преимущество маршрутизации между VLAN с помощью коммутатора уровня 3?

Первое решение маршрутизации между VLAN основывалось на использовании маршрутизатора с несколькими интерфейсами Ethernet. Каждый интерфейс маршрутизатора был подключен к порту коммутатора в разных VLAN. Интерфейсы маршрутизатора служат шлюзами по умолчанию для локальных узлов в подсети VLAN.

Преимущества использования коммутаторов уровня 3 для маршрутизации между VLAN:

- Это более быстрая маршрутизация, чем конфигурация router-on-stick, поскольку и коммутация, и маршрутизация выполняются аппаратно;
- для маршрутизации не требуются внешние каналы от коммутатора к маршрутизатору.
- Они не ограничиваются одним каналом, поскольку EtherChannels уровня 2 можно использовать в качестве магистральных каналов между коммутаторами для увеличения пропускной способности.
- Задержка намного короче, поскольку для маршрутизации в другую сеть данным не нужно покидать коммутатор.
- Они чаще развертываются в локальной сети кампуса, чем маршрутизаторы.

3. Дайте характеристику методу маршрутизации Router-on-a-Stick. В чем заключается недостаток устаревшего метода маршрутизации между сетями VLAN?

Метод маршрутизации между VLAN «router-on-a-stick» преодолевает ограничение устаревшего метода маршрутизации между VLAN. Для маршрутизации трафика между несколькими сетями VLAN в сети требуется только один физический интерфейс Ethernet.

Устаревший метод маршрутизации между VLAN, использующий физические интерфейсы, имеет большие ограничения. Он не является достаточно масштабируемым, поскольку маршрутизаторы имеют ограниченное количество физических интерфейсов. По мере возрастания количества VLAN в сети, требующих по одному физическому интерфейсу на каждую VLAN, количество свободных интерфейсов маршрутизатора быстро уменьшается.

4. Опишите алгоритм настройки маршрутизации между сетями VLAN методом Router-on-a-Stick. В чем заключается недостаток метода маршрутизации Router-on-a-Stick?

Шаг 1. Сети VLAN и конфигурации магистральных каналов.

```

vlan [id]                создание сете VLAN
name []
interface vlan [id]      интерфейс управления
ip add [ip]
no shut
ip default-gateway [ip]
interface fa[0/6]        порты доступа
switchport mode access
switchport access vlan [id]
no shut
interface fa[0/1]        транковые порты
switchport mode trunk

```

```
no shut
```

Шаг 2. Конфигурация подинтерфейса.

Подинтерфейс создается с помощью команды режима глобальной конфигурации **interface** *interface_id subinterface_id*. Затем каждый подинтерфейс настраивается с помощью следующих двух команд:

- **encapsulation dot1q** *vlan_id [native]* - This command configures the subinterface to respond to 802.1Q encapsulated traffic from the specified *vlan-id*. The **native** ключевого слова добавляется только для установки собственной VLAN отличной от VLAN 1.
- **ip address** *ip-address subnet-mask* - Эта команда настраивает IPv4-адрес подинтерфейса. Этот адрес обычно служит шлюзом по умолчанию для данной VLAN.

После создания всех подинтерфейсов включите физический интерфейс с помощью команды конфигурации **no shutdown** интерфейса. Если отключить физический интерфейс, то все подчиненные интерфейсы также отключаются.

Шаг 3. Проверка подключения между PC.

```
ipconfig, ping . . .
```

Шаг 4. Проверка маршрутизации.

Помимо использования **ping** между устройствами, следующие **show** команды могут использоваться для проверки и устранения неполадок конфигурации маршрутизатора на палке.

- **show ip route**
- **show ip interface brief**
- **show interfaces**
- **show interfaces trunk**

Маршрутизация между VLAN с использованием метода router-on-a-stick не масштабируется при работе более 50 сетей VLAN.

5. Опишите алгоритм настройки маршрутизации между VLAN с помощью коммутатора уровня 3. Дайте определение понятию "подинтерфейс".

Выполните следующие шаги для настройки S1 с созданием VLAN и магистральных каналов:

Шаг 1. Создайте сети VLAN.

```
vlan [id]  
name []
```

Шаг 2. Создание SVI интерфейсов VLAN.

```
interface vlan [id]  
description Default Gateway SVI for [ip]  
ip add [ip]  
no shut
```

Шаг 3. Настройка портов доступа

```
interface GigabitEthernet[1/0/18]  
description Access port to [PC1]  
switchport mode access  
switchport access vlan [id]
```

Шаг 4. Активация IP-маршрутизации.

```
ip routing
```

Передача трафика между VLAN может осуществляться с помощью маршрутизатора. Для того чтобы маршрутизатор мог передавать трафик из одного VLAN в другой (из одной сети в другую), необходимо чтобы в каждой сети у него был интерфейс. Для того чтобы не выделять под сеть каждого VLAN отдельный физический интерфейс, создаются логические **подинтерфейсы** на физическом интерфейсе для каждого VLAN.

Создание виртуального интерфейса (подинтерфейса или сабинтерфейса (sub-interface)):

```
interface fa0/0.2
description Management
```

Сначала указываем обычным образом физический интерфейс, к которому подключена нужная сеть, а после точки ставим некий уникальный идентификатор этого виртуального интерфейса. Для удобства, обычно номер сабинтерфейса делают аналогичным влану, который он терминирует.

6. Опишите алгоритм настройки маршрутизации на коммутаторе уровня 3. В чем заключается недостаток использования многоуровневых коммутаторов для маршрутизации между VLAN?

Шаг 1. Настройте маршрутизируемый порт.

```
interface GigabitEthernet[1/0/1]
description routed Port Link to [R1]
no switchport
ip address [ip]
no shut
```

Шаг 2. Включите маршрутизацию.

```
ip routing
```

Шаг 3. Настройте маршрутизацию.

```
router ospf 10
network 192.168.10.0 0.0.0.255 area 0
network 192.168.20.0 0.0.0.255 area 0
network 10.10.10.0 0.0.0.3 area 0
^z
```

Шаг 4. Проверка маршрутизации.

```
show ip route | begin Gateway
```

Шаг 5. Проверьте подключение.

```
ping . . .
```

7. Какие неполадки могут возникнуть при настройке маршрутизации между VLAN и как их исправить? В каком режиме должен находиться порт коммутатора при подключении его к маршрутизатору для маршрутизации между VLAN методом Router-on-a-Stick?

Неполадки при настройке маршрутизации между VLAN и способы их исправления:

- **Отсутствующие сети VLAN**

VLAN может отсутствовать, если она не была создана, случайно удалена или не разрешена на магистральном канале.

Если сеть VLAN случайно удаляется, все порты, назначенные этой сети, становятся неактивными. Они остаются связанными с этой сетью VLAN (и, следовательно, неактивными), пока не будут назначены новой сети VLAN. Используйте команду **show interface interface-id switchport** для проверки

членства в VLAN. Повторное создание отсутствующей VLAN автоматически переназначает хосты в нее. После этого необходимо выйти из режима конфигурации VLAN.

- **Проблемы магистрального порта коммутатора**

В устаревшем решении маршрутизации между VLAN это может быть вызвано, когда порт доступа маршрутизатора не назначен правильной VLAN. Однако при решении ROS наиболее распространенной причиной является неправильная настройка магистрального порта.

Решение: **show interface trunk, show running-config interface fa[0/5]**. Скорее всего необходимо снова включить порт: **interface fa[0/5], no shut, do show interface trunk**.

- **Неполадки в работе порта коммутатора**

В настройках коммутатора могут присутствовать проблемы, поэтому рекомендуется использовать специальные команды для проверки конфигурации и определения неполадок.

Решение: **ping, show interface fa[0/6] switchport, show running-config interface fa[0/6]**. Скорее всего необходимо назначить порт во VLAN: **interface fa[0/6], switchport access vlan [id]**.

- **Неполадки в настройках маршрутизатора**

Проблемы конфигурации маршрутизатора ROS обычно связаны с неправильными конфигурациями подинтерфейса. Например, был настроен неверный IP-адрес или неправильный идентификатор VLAN был присвоен подинтерфейсу.

Чтобы исправить эту проблему, настройте подчиненный интерфейс [G0/0.10] на правильную сеть VLAN с помощью команды режима глобальной конфигурации подинтерфейса **encapsulation dot1q [id]**.

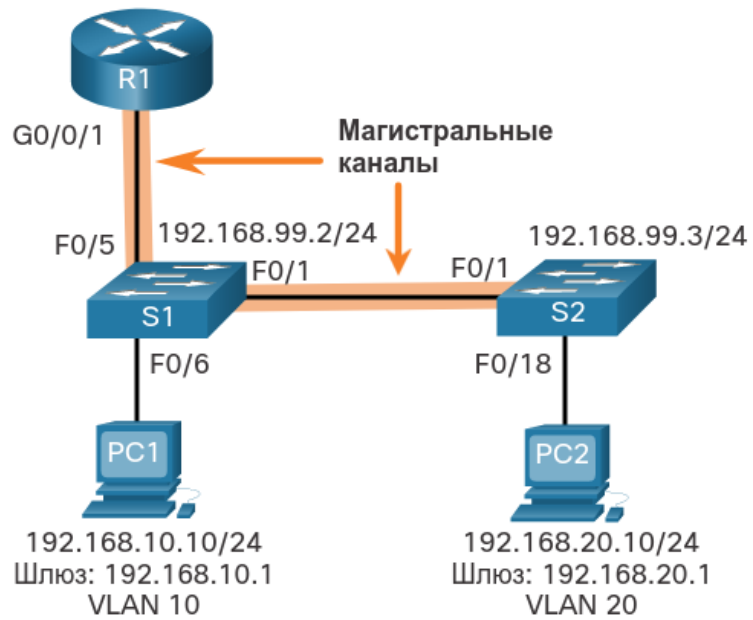
8. Какими возможностями обладает коммутатор уровня 3 по сравнению с коммутатором уровня 2? Между какими устройствами необходимо настроить магистральный канал при использовании метода Router-on-a-Stick?

Корпоративные локальные локальные сети используют коммутаторы уровня 3 для обеспечения маршрутизации между VLAN. Коммутаторы уровня 3 используют аппаратную коммутацию для достижения более высоких скоростей обработки пакетов, чем маршрутизаторы. Коммутаторы уровня 3 также обычно используются в корпоративных сетях стойка уровня распределения.

Возможности коммутатора уровня 3 включают в себя возможность выполнения следующих действий:

- Маршрутизация от одной VLAN к другой с использованием нескольких коммутируемых виртуальных интерфейсов (SVI).
- Преобразовать порт коммутатора уровня 2 в интерфейс уровня 3 (т.е. маршрутизируемый порт). Маршрутизируемый порт — простой интерфейс 3-го уровня, аналогичный физическому интерфейсу на маршрутизаторе Cisco IOS.

При использовании метода Router-on-a-Stick между маршрутизаторами и коммутаторами необходимо настроить магистральный канал.



Прак №4

Вопросы:

Прак №5

Вопросы:

Прак №6

Вопросы:

Прак №7

Вопросы:

Прак №8

Вопросы:

Прак №9

Вопросы:

Прак №10

Вопросы:

Прак №11

Вопросы:

Прак №12

Вопросы:

Афсё

блин блэт