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

**VLAN** (аббр. от англ. Virtual Local Area Network) — виртуальная локальная компьютерная сеть. Представляет собой группу хостов с общим набором требований, которые взаимодействуют так, как если бы они были подключены к широковещательному домену независимо от их физического местонахождения.

Сети VLAN позволяют администратору производить сегментацию сети по функциям, проектным группам или областям применения, независимо от физического расположения пользователя или устройства. Каждая VLAN считается отдельной логической сетью. Устройства в пределах VLAN работают таким образом, будто находятся в собственной независимой сети, даже если делят одну общую инфраструктуру с другими VLAN. Любой коммутационный порт может принадлежать сети VLAN.

В коммутируемой сети может быть несколько подсетей IP без использования нескольких сетей VLAN. Однако устройства будут находиться в одном и том же домене широковещательной рассылки уровня 2. Это означает, что все широковещательные рассылки уровня 2, например ARP-запрос, будут приниматься всеми устройствами в коммутируемой сети, даже теми, которые не предназначены для приема данной рассылки.

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

| **Преимущество** | **Описание** |
| --- | --- |
| Меньший размер широковещательных доменов | * Разделение сети на VLAN уменьшает количество устройств в домене широковещательной рассылки. * На рисунке есть шесть компьютеров в сети, но только три широковещательных домена (например, Faculty, Student и Guest). |
| Повышение безопасности | * Только пользователи одной и той же сети VLAN могут общаться вместе. * На рисунке, сетевой трафик факультета на VLAN 10 полностью отделен и защищен от пользователей в других VLAN. Улучшена эффективность ИТ-инфраструктуры |
| Повышение эффективности ИТ-инфраструктуры | * VLAN упрощают управление сетью, поскольку пользователи с аналогичными требованиями к сети используют одну и ту же сеть VLAN. * VLAN можно назначить соответствующее имя, чтобы упростить идентификацию. * На рисунке VLAN 10 названа «Faculty», VLAN 20 «Student», и VLAN 30 «Guest». |
| Снижение затрат | VLAN сокращают потребность в дорогостоящем обновлении сети и используют существующую пропускную способность и восходящие каналы более эффективно, что приводит к сокращению затрат. |
| Повышение производительности | Меньшие широковещательные домены уменьшают ненужный трафик в сети, а также повышения производительности. |
| Упрощенная форма управления проектами и приложениями | * VLAN объединяют пользователей и сетевые устройства для поддержки бизнес или географических требований. * Наличие отдельных функций позволяет управлять проектом или работать с специализированным приложением; примером такого приложения является платформа развития электронного обучения для преподавателей. |

VLAN по умолчанию на коммутаторе Cisco — VLAN 1. Таким образом, все порты коммутатора находятся на VLAN 1, если они явно не настроены на другую VLAN. По умолчанию весь управляющий трафик уровня 2 связан с VLAN 1.

Важные факты, которые следует помнить о VLAN 1, включают следующее:

* По умолчанию все порты назначены сети VLAN 1.
* Сетью VLAN с нетегированным трафиком по умолчанию является сеть VLAN 1.
* Сетью управления VLAN по умолчанию является сеть VLAN 1.
* VLAN 1 нельзя переименовывать или удалять.

Например, в выходных данных команды **show vlan brief** все порты в настоящее время назначены во VLAN 1 по умолчанию. Ни одна сеть не назначена в качестве VLAN с нетегированным трафиком, и ни одна другая сеть VLAN не является активной. Таким образом, сетью VLAN с нетегированным трафиком будет управляющая сеть VLAN. Это считается угрозой безопасности.

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

VLAN данных — это VLAN, настроенные для разделения пользовательского трафика. Они называются пользовательскими VLAN, поскольку они разделяют сеть на группы пользователей или устройств. Современная сеть будет иметь множество VLAN данных в зависимости от требований организации. Обратите внимание, что голосовой и сетевой трафик управления не должен быть разрешен в VLAN для передачи данных.

Пользовательский трафик из VLAN должен быть помечен идентификатором VLAN при его отправке на другой коммутатор. Транк порты используются между коммутаторами для поддержки передачи маркированного трафика. В частности, магистральный порт 802.1Q вставляет 4-байтовый тег в заголовок кадра Ethernet для идентификации VLAN, которой принадлежит кадр.

Коммутатору также может потребоваться отправить непомеченный трафик по магистральному каналу. Непомеченный трафик генерируется коммутатором и может также поступать с устаревших устройств. Транк порт 802.1Q размещает непомеченный трафик на собственной VLAN (Native VLAN). Собственная VLAN на коммутаторе Cisco — VLAN 1 (то есть VLAN по умолчанию).

Рекомендуется настроить собственную VLAN как неиспользуемую VLAN, отличную от VLAN 1 и других VLAN. Фактически, нет ничего необычного в том, чтобы выделять фиксированную VLAN для выполнения роли собственной VLAN для всех магистральных портов в коммутируемом домене.

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

Управляющая VLAN - это VLAN для передачи данных, специально настроенная для трафика управления сетью, включая SSH, Telnet, HTTPS, HHTP и SNMP. По умолчанию VLAN 1 настраивается как управляющая VLAN на коммутаторе уровня 2.

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

VLAN не были бы очень полезны без транков VLAN. VLAN транки позволяют передавать весь трафик VLAN между коммутаторами. Это позволяет устройствам, подключенным к различным коммутаторам, но в одной и той же VLAN, взаимодействовать без прохождения через маршрутизатор.

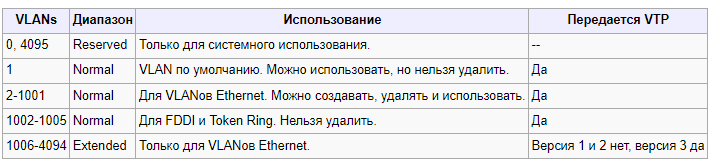
Магистраль сетей VLAN (транк) — это двухточечный канал связи, который обслуживает более одной сети VLAN. Транк VLAN расширяет сети VLAN по всей сети. Cisco поддерживает IEEE 802.1Q для координации магистралей на интерфейсах Fast Ethernet, Gigabit Ethernet и 10-Gigabit Ethernet.

Транк VLAN не принадлежит определенной VLAN. Вместо этого он является каналом для нескольких VLAN между коммутаторами и маршрутизаторами. Кроме того, магистраль может использоваться между сетевым устройством и сервером или другим устройством, оснащенным соответствующим сетевым адаптером 802.1Q. По умолчанию на коммутаторе Cisco Catalyst все VLAN поддерживаются на магистральном порту.

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

Стандартный заголовок фрейма Ethernet не содержит информации о VLAN, к которой принадлежит кадр. Поэтому при размещении кадров Ethernet в магистрали необходимо добавить информацию о VLAN, к которым они принадлежат. Этот процесс, называемый маркировка, выполняется с помощью заголовка IEEE 802.1Q, указанного в стандарте IEEE 802.1Q. Заголовок 802.1Q включает в себя 4-байтовый тег, вставленный в исходный заголовок фрейма Ethernet, определяющий VLAN, к которой принадлежит фрейм.

Когда коммутатор получает кадр на порте, настроенном в режиме доступа с назначенной сетью VLAN, он добавляет в заголовок кадра тег VLAN, заново вычисляет проверочную последовательность кадра (FCS) и отправляет этот тегированный кадр из магистрального порта.



Различные коммутаторы Cisco Catalyst поддерживают различные количества VLAN. Количество поддерживаемых VLAN достаточно велико, чтобы удовлетворить потребности большинства организаций. Коммутаторы Catalyst 2960 и 3560 способны поддерживать более 4000 сетей VLAN. VLAN нормального диапазона на этих коммутаторах нумеруются от 1 до 1 005, а VLAN расширенного диапазона — от 1 006 до 4 094. На рисунке показаны доступные сети VLAN на коммутаторе Catalyst 2960, работающем под управлением Cisco IOS версии 15.x.

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

**Сети VLAN стандартного диапазона**

Ниже приведены характеристики VLAN нормального диапазона:

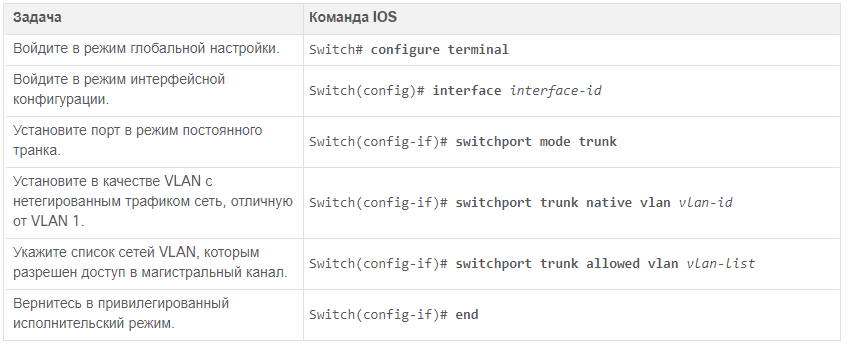
* Используются в малых и средних сетях предприятий и организаций.
* Сети VLAN обычного диапазона определяются идентификатором VLAN от 1 до 1005.
* (Идентификаторы от 1002 до 1005 резервируются для сетей VLAN типа Token Ring и FDDI.)
* Идентификаторы 1 и идентификаторы от 1002 до 1005 создаются автоматически и не могут быть удалены.
* Конфигурации хранятся в файле базы данных VLAN (vlan.dat), который находится во флеш-памяти.
* При настройке протокол магистрального соединения VLAN (VTP) помогает синхронизировать базу данных VLAN между коммутаторами.

**Сети VLAN расширенного диапазона**

Ниже приведены характеристики сетей VLAN расширенного диапазона:

* Они используются поставщиками услуг для обслуживания нескольких клиентов и глобальными предприятиями, достаточно крупными для того, чтобы нуждаться в идентификаторах VLAN расширенного диапазона.
* Определяются идентификатором VLAN от 1006 до 4094.
* По умолчанию они сохраняются в файле текущей конфигурации.
* Поддерживают меньше функций VLAN, чем сети VLAN стандартного диапазона.
* Требуется конфигурация прозрачного режима VTP для поддержки сетей VLAN расширенного диапазона.

**Примечание**: 4096 является верхней границей для числа VLAN, доступных на коммутаторах Catalyst, поскольку в поле идентификатора VLAN заголовка IEEE 802.1Q имеется 12 бит.



1. Опишите назначение протокола DTP. В каких случая стоит отключать протокол DTP и почему?

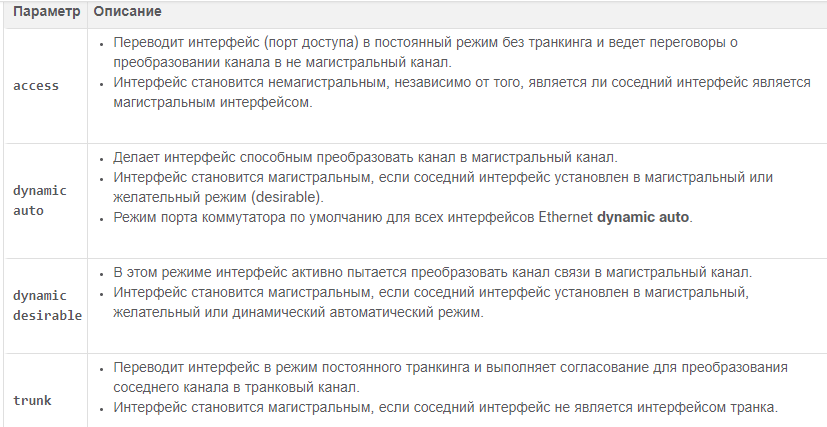
Некоторые коммутаторы Cisco имеют собственный протокол, который позволяет им автоматически согласовывать магистральные соединения с соседним устройством. Этот протокол называется протоколом динамического транкинга (DTP). DTP может ускорить процесс настройки для администратора сети. Магистральные интерфейсы Ethernet поддерживают различные режимы магистралей. Интерфейс может быть переведен в магистральный режим или режим без магистрали, либо настроен для согласования такого режима с соседним интерфейсом. Согласование магистрали управляется динамическим протоколом магистральных каналов (DTP), который действует по принципу подключения «точка-точка» между сетевыми устройствами.

Протокол DTP — это запатентованный протокол Cisco, который автоматически включён на коммутаторах Catalyst 2960 и Catalyst 3560. DTP управляет транковым согласованием только в случае, если порт соседнего коммутатора настроен в режиме транка, который поддерживает DTP. Коммутаторы других поставщиков не поддерживают DTP.

**Внимание**: Некоторые межсетевые устройства могут перенаправлять кадры DTP неправильно, что может привести к неправильным конфигурациям. Отключите протокол DTP на интерфейсах коммутатора Cisco, который подключен к устройствам, не поддерживающим DTP.

Конфигурация DTP по умолчанию для коммутаторов Cisco Catalyst 2960 и 3650 является динамической автоматической.

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





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

Существует несколько способов изменить членство во VLAN.

Если порт доступа коммутатора неправильно назначен VLAN, просто повторно введите команду конфигурации интерфейса **switchport access vlan** vlan-id с правильным идентификатором VLAN. Например, предположим, что Fa0/18 неправильно настроено на VLAN 1 по умолчанию вместо VLAN 20. Чтобы изменить порт на VLAN 20, просто введите **switchport access vlan 20**.

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

Команда **no vlan** vlan-id режима глобальной конфигурации используется для удаления VLAN из файла коммутатора vlan.dat.

**Внимание**: 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.

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

**Тегированные кадры в сети native VLAN**

Некоторые устройства, поддерживающие транкинг, добавляют тег VLAN в пакеты VLAN с нетегированным трафиком. Управляющий трафик, отправляемый в сети native VLAN, тегировать не следует. Если магистральный порт 802.1Q получает тегированный кадр с таким же идентификатором VLAN, как у сети VLAN с нетегированным трафиком, то он отбрасывает этот кадр. При настройке порта коммутатора Cisco настраивайте устройства таким образом, чтобы они не отправляли тегированные кадры по сети VLAN с нетегированным трафиком. Устройства других производителей, поддерживающие помеченные кадры в собственной VLAN, включают IP-телефоны, серверы, маршрутизаторы и коммутаторы, отличные от Cisco.

**Нетегированные кадры в сети native VLAN**

Когда магистральный порт коммутатора Cisco получает кадры без тегов (которые являются необычными для хорошо спроектированной сети), он пересылает эти кадры в собственную VLAN. Если нет устройств, связанных с собственной VLAN (что не является необычным) и нет других магистральных портов (что не является необычным), то кадр отбрасывается. Сетью VLAN с нетегированным трафиком по умолчанию является сеть VLAN 1. При настройке магистрального порта 802.1Q значение собственного идентификатора VLAN ID (PVID) назначается по умолчанию. Весь непомеченный трафик, поступающий в порт 802.1Q или исходящий из него, перенаправляется на основе значения PVID. Например, если VLAN 99 настроена как собственная VLAN, PVID равно 99 и весь непомеченный трафик перенаправляется в VLAN 99. Если встроенная VLAN не была перенастроена, для параметра PVID устанавливается значение VLAN 1.

При настройке сетей VLAN стандартного диапазона сведения о конфигурации хранятся во флеш-памяти коммутатора, в файле vlan.dat. Флэш-память является постоянной и не требует команды **copy running-config startup-config**. Однако, поскольку одновременно с созданием сетей VLAN на коммутаторах Cisco часто также настраиваются и другие параметры, рекомендуется сохранять изменения текущей конфигурации в файл загрузочной конфигурации.

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

Команда **no vlan** vlan-id режима глобальной конфигурации используется для удаления VLAN из файла коммутатора vlan.dat.

**Внимание**: 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.

Можно удалить весь файл vlan.dat с помощью команды **delete flash:vlan.dat** в привилегированном исполнительском режиме. Сокращенную версию команды (**delete vlan.dat**) можно использовать только в том случае, если файл vlan.dat находится в своем расположении по умолчанию. После выполнения этой команды и перезагрузки коммутатора ранее настроенные сети VLAN будут недоступны. Фактически, это позволяет восстановить на коммутаторе его заводские настройки VLAN.

**Примечание**: Чтобы восстановить заводское состояние коммутатора Catalyst, отключите от коммутатора все кабели, кроме консоли и кабеля питания. Затем введите привилегированную команду режима EXEC **erase startup-config**, за которой следует команда **delete vlan.dat**.