**Лабораторная работа №4**

**Виртуальные локальные сети (VLAN)**

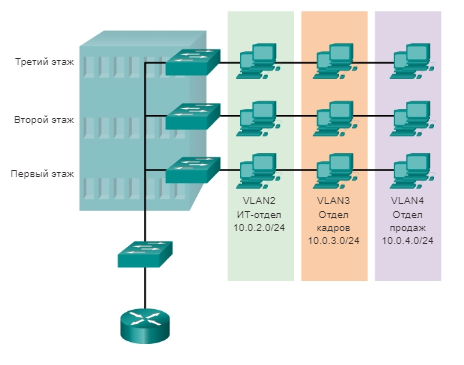
1. **Виртуальные сети (VLAN)**

В коммутируемых объединённых сетях сети VLAN обеспечивают гибкость сегментации и организации. 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.

Сети VLAN позволяют администратору производить сегментацию по функциям, проектным группам или областям применения, вне зависимости от физического расположения пользователя или устройства. Устройства в пределах сети VLAN работают таким образом, будто находятся в собственной независимой сети, даже если делят одну общую инфраструктуру с другими VLAN. Любой порт коммутатора может принадлежать сети VLAN. Одноадресные, широковещательные и многоадресные пакеты пересылаются и рассылаются только к конечным станциям в пределах той сети VLAN, которая является источником этих пакетов. Каждая сеть VLAN считается отдельной логической сетью, и пакеты, адресованные станциям, не принадлежащим данной сети VLAN, должны пересылаться через устройство, поддерживающее маршрутизацию.

Сеть VLAN создаёт логический широковещательный домен, который может охватывать несколько физических сегментов LAN. Разделяя крупные широковещательные домены на более мелкие сети, VLAN повышают производительность сети. 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.

Сети VLAN позволяют реализовывать политику обеспечения доступа и безопасности, учитывая интересы различных групп пользователей. Каждый порт коммутатора может быть назначен только одной сети VLAN (за исключением порта, подключённого к IP-телефону или к другому коммутатору).



*Рис. 1. Виртуальная сеть представляет собой группу устройств или пользователей, не ограниченную физическим сегментом сети*

Сети VLAN облегчают процесс проектирования сети, обеспечивающей помощь в выполнении целей организации. К основным преимуществам использования VLAN относятся:

* **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. При введении в эксплуатацию нового коммутатора на назначенных портах реализуются все правила и процедуры, уже применённые в этой конкретной VLAN. Также ИТ-специалистам легче определять функцию сети VLAN, назначая ей соответствующее имя.
* **Упрощённое 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. Пример такой прикладной задачи — платформа разработки приложений для электронного обучения преподавателей.

Каждая VLAN в коммутируемой сети относится к какой-либо IP-сети; таким образом, в проекте VLAN нужно учитывать реализацию иерархической системы сетевой адресации. Иерархическая адресация подразумевает упорядоченное назначение номеров IP-сети сегментам или сетям VLAN с учетом работы сети в целом.

В современных сетях используется множество различных типов сетей VLAN. Некоторые типы VLAN определяются классами трафика. Другие типы VLAN обусловлены функциями, которые они выполняют.

**Виртуальная локальная сеть для данных**

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 VLAN по умолчанию**

Все порты коммутатора становятся частью VLAN по умолчанию после первоначальной загрузки коммутатора. Порты коммутатора, находящиеся в сети VLAN по умолчанию, являются частью одного широковещательного домена. Благодаря этому любое устройство, подключённое к любому порту коммутатора, может обмениваться данными с другими устройствами на других портах коммутатора. Сетью VLAN по умолчанию для коммутаторов Cisco установлена VLAN 1.

Команда **show vlan brief** показывает активные VLAN и порты на котором настроен данный VLAN

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.

**Native VLAN**

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.

Сети native VLAN определены в спецификации IEEE 802.1Q для обеспечения обратной совместимости с нетегированным трафиком, характерным для устаревших сценариев локальных сетей. Сеть native VLAN служит общим идентификатором на противоположных концах транкового канала.

Рекомендуется настроить native VLAN как неиспользуемую VLAN, отличающуюся от сети VLAN 1 и других VLAN. Фактически принято выделять фиксированную VLAN для выполнения роли сети native VLAN для всех транковых портов в коммутируемом домене.

**Управляющая VLAN**

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.

Несмотря на то, что теоретически коммутатор может обладать более чем одной управляющей VLAN, использование нескольких сетей данного типа увеличивает подверженность сетевым атакам.

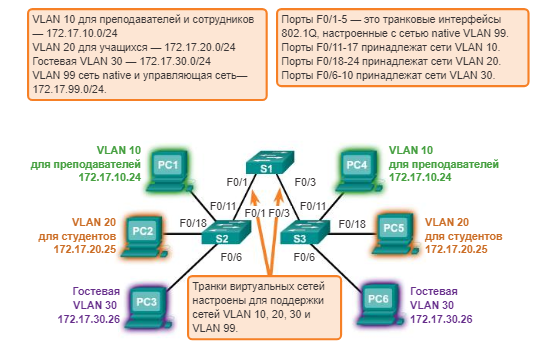
1. **Виртуальные локальные сети в среде с множеством коммутаторов**

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.

Использование сетей VLAN без транковых каналов существенно снижает полезные возможности VLAN. Транки виртуальных сетей обеспечивают распространение всего трафика VLAN между коммутаторами так, чтобы устройства, находящиеся в одной сети VLAN, но подключённые к разным коммутаторам, могли обмениваться данными без вмешательства маршрутизатора.

Транк виртуальных сетей не принадлежит какой-либо определённой сети VLAN, а, скорее, является «кабельным каналом» передачи многих VLAN между коммутаторами и маршрутизаторами. 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.

На рисунке каналы между коммутаторами S1 и S2, а также между S1 и S3 настроены для передачи трафика, отправляемого по всей сети от VLAN 10, 20, 30 и 99. Данная сеть не сможет работать без транковых каналов VLAN.



Коммутаторы серии Catalyst 2960 являются устройствами 2-го уровня. Для пересылки пакетов они используют данные заголовка кадра Ethernet. Они не содержат таблиц маршрутизации. 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. Заголовок 802.1Q содержит тег размером 4 байта, который добавляется в оригинальный заголовок кадра Ethernet и идентифицирует VLAN, к которой относится кадр.

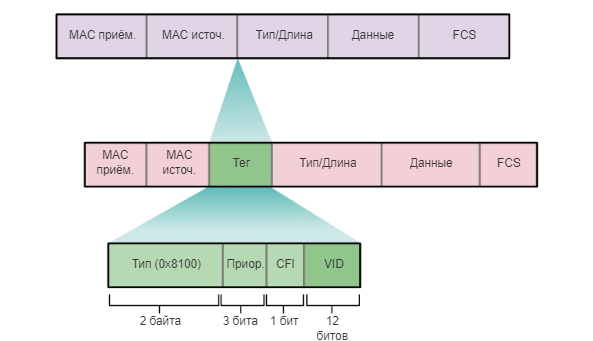
Когда коммутатор получает кадр через порт, настроенный в режиме доступа и назначенный сети VLAN, коммутатор добавляет в заголовок кадра метку VLAN, заново вычисляет FCS и отправляет тегированный кадр из транкового порта.

**Подробнее о поле тега VLAN**

Поле тега VLAN состоит из поля типа, поля приоритета, поля идентификатора канонического формата и поля идентификатора VLAN.

* **Тип** — это 2-байтовое значение, которое называется значением идентификатора протокола тегирования (TPID). Значение для Ethernet имеет вид шестнадцатеричного числа 0x8100.
* **Приоритет пользователя** — это 3-битовое значение, которое поддерживает реализацию уровня или сервиса.
* **Идентификатор канонического формата (CFI)** — это 1-битовый идентификатор, который обеспечивает передачу кадров Token Ring по каналам Ethernet.
* **VLAN-идентификатор (VID)** — это 12-битный идентификационный номер VLAN, который поддерживает до 4096 идентификаторов VLAN.

После того как коммутатор добавит поля типа и управляющей информации тега, он пересчитывает значения FCS и добавляет в кадр новое значение FCS.



**Тегированные кадры в сети native VLAN**

Некоторые устройства, поддерживающие транковую связь, добавляют метку в трафик сети native 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. Следовательно, при настройке порта коммутатора в коммутаторе Cisco настраивайте устройства таким образом, чтобы они не отправляли тегированные кадры по сети native VLAN. К устройствам от других производителей, которые поддерживают тегированные кадры в сети native VLAN, относятся IP-телефоны, серверы, маршрутизаторы и коммутаторы не от Cisco.

**Нетегированные кадры в сети native VLAN**

Когда транковый порт коммутатора Cisco получает нетегированные кадры (которые редко встречаются в хорошо спроектированной сети), он пересылает эти кадры в сеть native VLAN. Если с сетью native VLAN не связаны никакие устройства (что бывает довольно часто), а также нет других транковых портов (что также часто случается), 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. Например, если сеть VLAN 99 настроена в качестве native VLAN, то значение PVID равно 99, а весь нетегированный трафик пересылается в сеть VLAN 99. Если сеть native VLAN не была перенастроена, то значение PVID присваивается равным 1.

**Назначение виртуальной локальной сети**

Различные коммутаторы Cisco Catalyst поддерживают разное количество сетей VLAN. Количество поддерживаемых сетей VLAN достаточно велико для удовлетворения потребностей большинства организаций. Например, коммутаторы Catalyst 2960 и 3560 способны поддерживать более 4 тысяч сетей VLAN. Виртуальные локальные сети стандартного диапазона на этих коммутаторах имеют идентификатор от 1 до 1 005, а сети VLAN расширенного диапазона — от 1 006 до 4 094.

**Виртуальные локальные сети стандартного диапазона**

* Используются в малых и средних сетях предприятий и организаций.
* Определяются идентификатором VLAN от 1 до 1005.
* Идентификаторы от 1002 до 1005 зарезервированы для сетей VLAN 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 под именем vlan.dat. Файл vlan.dat расположен во флеш-памяти коммутатора.
* Протокол VTP (транковый протокол VLAN), помогающий управлять конфигурациями VLAN между коммутаторами, может распознавать и хранить только сети VLAN стандартного диапазона.

**Сети VLAN расширенного диапазона**

* Позволяют операторам связи расширять свою инфраструктуру для большого числа клиентов. Некоторым крупным международным корпорациям нужны идентификаторы VLAN расширенного диапазона.
* Определяются идентификатором VLAN от 1006 до 4094.
* Конфигурации сетей не записываются в файл vlan.dat.
* Поддерживают меньше функций VLAN, чем сети VLAN стандартного диапазона.
* По умолчанию сохраняются в файл текущей конфигурации.
* Протокол VTP не распознаёт сети VLAN расширенного диапазона.

**Примечание**. 4096 — это максимальное количество VLAN, доступных на коммутаторах Catalyst, поскольку в поле идентификатора VLAN заголовка IEEE 802.1Q насчитывается 12 бит.

# Статические виртуальные сети

**Статическая виртуальная сеть (Static** VLAN) представляет собой совокупность портов коммутатора, статически объединенных в виртуальную сеть. Эти порты поддерживают назначенную конфигурацию до тех пор, пока она не будет изменена администратором. Хотя для внесения изменений статические виртуальные сети требуют вмешательства администратора, к их достоинствам можно отнести высокий уровень безопасности, легкость конфигурирования и возможность непосредственного наблюдения за работой сети Статические виртуальные сети эффективно работают в ситуациях, когда необходимо контролировать переезды пользователей и вносить соответствующие изменения в конфигурацию.

# Динамические виртуальные сети

**Динамические виртуальные сети (dynamic VLAN)** представляют собой логическое объединение портов коммутатора, которые могут автоматически определять свое расположение в виртуальной сети. Функционирование динамической виртуальной сети основывается на МАС-адресах, на логической адресации или на типе протокола пакетов данных. При первоначальном подключении станции к неиспользуемому порту коммутатора соответствующий коммутатор проверяет МАС-адрес в базе данных управления виртуальной сетью и динамически устанавливает соответствующую конфигурацию на данном порте. Основными достоинствами такого подхода является уменьшение объема работ в монтажном шкафу при добавлении нового пользователя или при переезде уже существующего и централизованное извещение всех пользователей при добавлении в сеть неопознанного пользователя. Основная работа в этом случае заключается в установке базы данных в программное обеспечение управления виртуальной сетью и в поддержания базы данных, содержащей точную информацию обо всех пользователях сети.

Команды для создания виртуальных локальных сетей на коммутаторе Cisco

|  |  |
| --- | --- |
| Войдите в режим глобальной конфигурации | S1**# conf t** |
| Создайте сеть VLAN с допустимым номером идентификатора | S1**(config)# vlan** *vlan-id* |
| Укажите уникально имя для идентификации VLAN | S1**(config)# name** *vlan-name* |

Следующий шаг после создания сети VLAN — назначение портов сетям VLAN. Порт доступа может одновременно принадлежать только одной VLAN.

Назначение портов сетям VLAN

|  |  |
| --- | --- |
| Войдите в режим глобальной конфигурации | S1**# conf t** |
| Войдите в режим конфигурации интерфейса | S1**(config)# interface** *interface-id*  либо S1**(config)# int** *interface-id* |
| Переведите порт в режиме доступа | S1**(config-if)# switchport mode access** |
| Назначьте порт сети VLAN | S1**(config-if)# switchport access vlan** *vlan-id* |
| Удалить назначение сети VLAN из порта | S1**(config-if)# no switchport access vlan** *vlan-id* |
| Удаление сети VLAN | S1**(config)# no vlan** *vlan-id* |

**Внимание!** Перед удалением сети VLAN обязательно переназначьте все порты, которые ей принадлежат, в другие сети VLAN. После удаления VLAN все порты, которые не были перемещены в активную сеть VLAN, не смогут обмениваться данными с другими узлами, пока не будут назначены активной VLAN.

Команда**show vlan name** *vlan-name*генерирует выходные данные, которые нелегко интерпретировать. Рекомендуется использовать команду**show vlan brief**. Команда**show vlan summary** отображает список всех настроенных сетей VLAN.

Транк виртуальной сети — это канал OSI 2-го уровня между двумя коммутаторами, который передаёт трафик во все сети VLAN (если список допустимых сетей VLAN не ограничен вручную или динамически). Для того чтобы активировать транковые каналы, настройте порты на любом конце физического канала с помощью параллельных наборов команд.

Чтобы настроить порт коммутатора на одном конце транкового канала, используйте команду**switchport mode trunk**. С помощью этой команды интерфейс переходит в постоянный транковый режим.

Настройка транковых каналов

|  |  |
| --- | --- |
| Настройте канал в качестве транкового | S1**(config-if)# switchport mode trunk** |
| Укажите сеть Native VLAN для транков 802.1Q без меток. Сброс транка | S1**(config-if)# (no) switchport trunk native vlan** *vlan-id* |
| Укажите список сетей VLAN, которым разрешен доступ в транковый канал. Сброс транка | S1**(config-if)# (no) switchport trunk allowed vlan** *vlan-list* |

**Задание**

## Задание 1. Получатели широковещательной рассылки

Откройте файл " 3.1.1.5 Packet Tracer - Who Hears the Broadcast Instructions.pka" и выполните указанные задания

## Задание 2. Исследование методов реализации сети VLAN

Откройте файл "3.1.2.7 Packet Tracer - Investigating a VLAN Implementation Instructions.pka " и выполните указанные задания.

## Задание 3. Конфигурация сетей VLAN

Откройте файл "3.2.1.7 Packet Tracer - Configuring VLANs Instructions.pka" и выполните указанные задания.

## Задание 4. Отработка комплексных практических навыков

Откройте файл "3.4.1.2 Skills Integration Challenge.pka" и выполните указанные задания.

**Задание 5. Создание сети**

Разработать сеть с VLAN и динамической маршрутизаций, перед разработкой сети утвердить схему сети у преподавателя