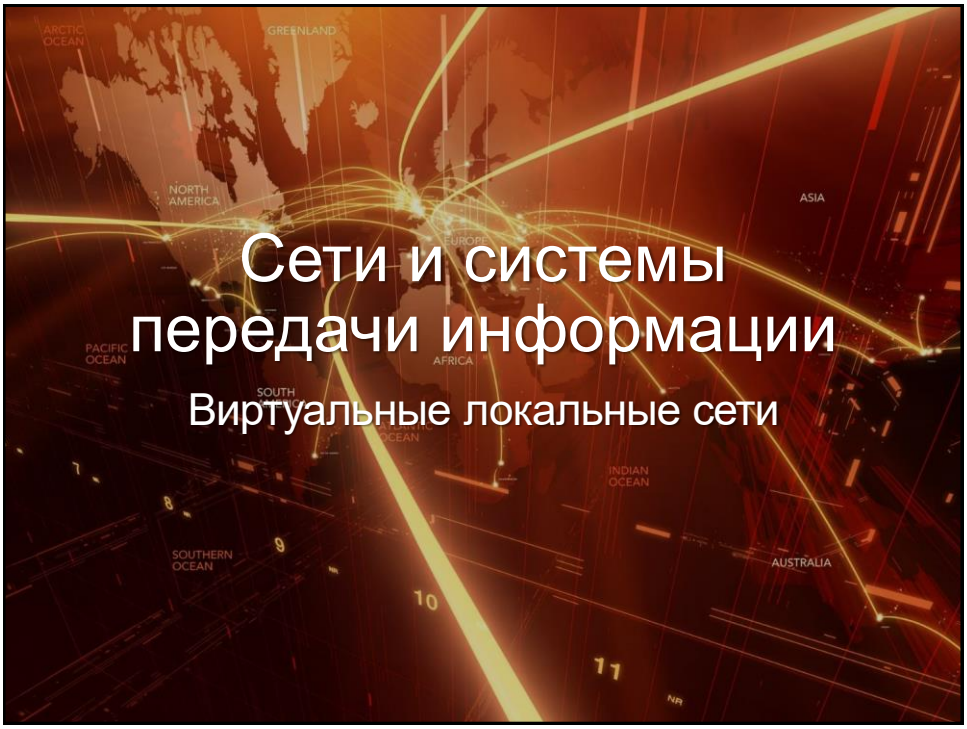


Сети и системы передачи информации

Виртуальные локальные сети

Понятие и назначение

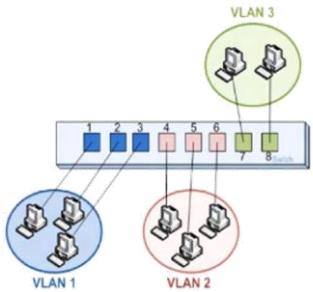
Виртуальной локальной сетью (англ. Virtual Local Area Network, VLAN) называется группа узлов сети, трафик которой, в том числе широковещательный, на канальном уровне полностью изолирован от трафика других узлов сети.

- Основное **назначение** технологии VLAN состоит в облегчении процесса создания изолированных сетей, которые затем обычно связываются между собой с помощью маршрутизаторов, при этом такое построение сети создает мощные барьеры на пути нежелательного трафика.
- **Достоинством** технологии VLAN является то, что она позволяет создавать полностью изолированные сегменты сети путем логического конфигурирования коммутаторов, не прибегая к изменению топологии.
- Для **связывания виртуальных сетей** в общую сеть требуется привлечение средств сетевого уровня, что может быть реализовано в отдельном маршрутизаторе или с помощью коммутатора третьего уровня.
- Технология VLAN долгое время не стандартизировалась, но положение изменилось после принятия в 1998 году **стандарта IEEE 802.1Q**, который определяет базовые правила построения виртуальных локальных сетей, не зависящие от протокола канального уровня коммутатора.

Создание VLAN на одном коммутаторе

При создании виртуальных сетей на основе одного коммутатора обычно используется механизм **группирования портов** коммутатора:

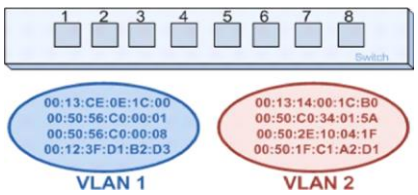
- каждый порт приписывается той или иной виртуальной сети;
- кадр, пришедший от порта, принадлежащего одной виртуальной сети, никогда не будет передан порту, не принадлежащему этой виртуальной сети;
- порт можно приписать нескольким виртуальным сетям, хотя на практике так делают редко – пропадает эффект полной изоляции сетей.



Создание VLAN на одном коммутаторе

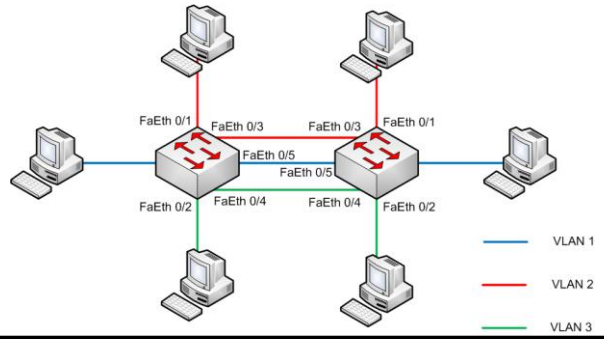
Второй способ образования виртуальных сетей основан на группировании MAC-адресов:

- каждый MAC-адрес, который изучен коммутатором, приписывается той или иной виртуальной сети;
- при существовании в сети множества узлов этот способ требует от администратора большого объема ручной работы;
- при построении виртуальных сетей на основе нескольких коммутаторов он оказывается более гибким, чем группирование портов.



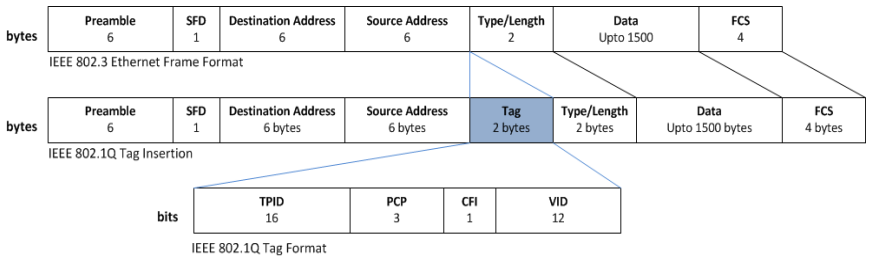
Создание VLAN на нескольких коммутаторах

- Если узлы какой-либо виртуальной сети подключены к разным коммутаторам, то для подключения каждой такой сети на коммутаторах должна быть **выделена специальная пара портов**.
- В ином случае, если коммутаторы будут связаны только одной парой портов, информация о принадлежности кадра той или иной виртуальной сети при передаче из коммутатора в коммутатор будет утеряна.
- Таким образом, коммутаторы с группированием портов требуют для своего соединения столько портов, сколько виртуальных сетей они поддерживают.



Создание VLAN по стандарту 802.1Q

- В стандарте 802.1Q используется дополнительное поля кадра для сохранения информации о принадлежности кадра той или иной виртуальной локальной сети при его перемещениях между коммутаторами.
- Нет необходимости помнить в каждом коммутаторе о принадлежности всех MAC-адресов составной сети виртуальным сетям.
- Дополнительное поле с пометкой о номере виртуальной сети используется только тогда, когда кадр передается от коммутатора к коммутатору, а при передаче кадра конечному узлу оно обычно удаляется.
- Модифицируется протокол взаимодействия между коммутаторами, а принципы работы конечных узлов остаются неизменным.



Структура тега по стандарту 802.1Q

Размер тега – 4 байта. Он состоит из полей:

- Tag Protocol Identifier (TPID) – Идентификатор протокола тегирования. Размер поля – 16 бит. Указывает, какой протокол используется для тегирования. Для 802.1Q используется значение 0x8100.
- Tag Control Information (TCI) – поле, инкапсулирующее в себе поля приоритета, канонического формата и идентификатора VLAN:
  - Priority – приоритет. Размер поля – 3 бита. Используется стандартом IEEE 802.1p для задания приоритета передаваемого трафика.
  - Canonical Format Indicator (CFI) – Индикатор канонического формата. Размер поля – 1 бит. Указывает на формат MAC-адреса. 0 – канонический (Кадр Ethernet), 1 – не канонический (Кадр Token Ring, FDDI).
  - VLAN Identifier (VID) – идентификатор VLAN. Размер поля – 12 бит. Указывает, какому VLAN принадлежит фрейм. Диапазон возможных значений VID от 0 до 4094.

Так как фрейм изменился, пересчитывается контрольная сумма всего кадра.

Создание VLAN по стандарту 802.1Q

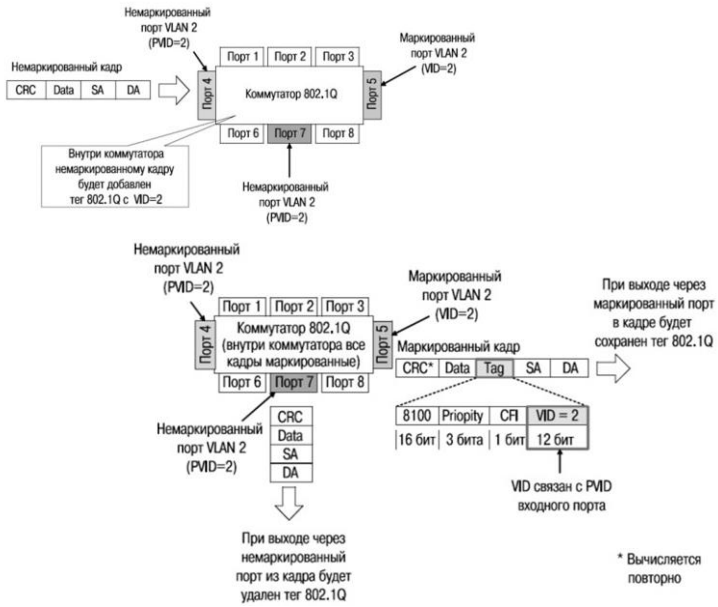
- Пользуясь значением VID в помеченных кадрах, коммутаторы сети выполняют групповую фильтрацию трафика, разбивая сеть на виртуальные сегменты, то есть на VLAN.
- Для поддержки этого режима каждый порт коммутатора приписывается к одной или нескольким виртуальным локальным сетям, то есть выполняется группировка портов.
- Для упрощения конфигурирования сети в стандарте 802.1Q вводятся понятия линии доступа и транка:
  - **Линия доступа** связывает порт коммутатора (называемый в этом случае портом доступа) с компьютером, принадлежащим некоторой виртуальной локальной сети.
  - **Транк** — это линия связи, которая соединяет между собой порты двух коммутаторов; в общем случае через транк передается трафик нескольких виртуальных сетей.
- Коммутаторы, поддерживающие технику VLAN, без специального конфигурирования по умолчанию работают как стандартные коммутаторы, обеспечивая соединения всех со всеми.

Алгоритм передачи кадра по стандарту 802.1Q

Правило входящих кадров

Правило исходящих кадров

Алгоритм передачи кадра по стандарту 802.1Q



Алгоритм передачи кадра по стандарту 802.1Q