VLAN — главный механизм для создания логической топологии сети, не зависящей от её физической топологии. VLAN'ы используются для сокращения широковещательного трафика в сети.

Гибкое разделение устройств на группы

Как правило, одному VLAN соответствует одна подсеть. Устройства, находящиеся в разных VLAN, будут находиться в разных подсетях. Но в то же время VLAN не привязан к местоположению устройств и поэтому устройства, находящиеся на расстоянии друг от друга, все равно могут быть в одном VLAN независимо от местоположения

Уменьшение количества широковещательного трафика в сети

Каждый VLAN — это отдельный широковещательный домен. Например, коммутатор — это устройство 2 уровня модели OSI. Все порты на коммутаторе с лишь одним VLAN находятся в одном широковещательном домене. Создание дополнительных VLAN на коммутаторе означает разбиение коммутатора на несколько широковещательных доменов. Если один и тот же VLAN настроен на разных коммутаторах, то порты разных коммутаторов будут образовывать один широковещательный домен.

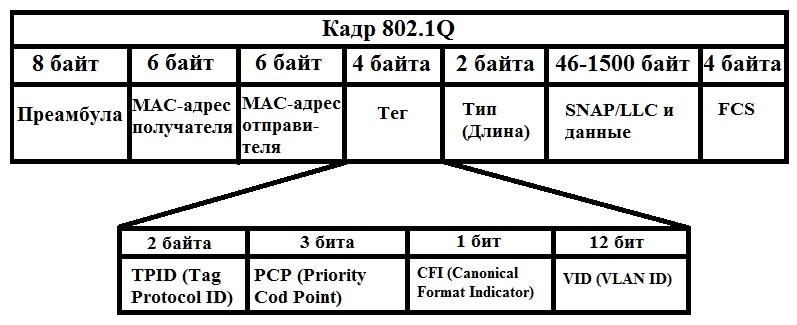
Увеличение безопасности и управляемости сети

Когда сеть разбита на VLAN, упрощается задача применения политик и правил безопасности. С VLAN политики можно применять к целым подсетям, а не к отдельному устройству. Кроме того, переход из одного VLAN в другой предполагает прохождение через устройство 3 уровня, на котором, как правило, применяются политики, разрешающие или запрещающие доступ из VLAN в VLAN.

Для начала взглянем на обычный «Ethernet-кадр», находящийся в своей привычной среде обитания:



А теперь взглянем на новый кадр 802.1q:



Что у нас в итоге получается – добавляется ещё один тег с нужной для нас информацией:

1. **TPID** – всегда будет состоять из 2 байт и обычно равен 0x8100. В переводе с английского «Tag Protocol ID» – обозначает «Идентификатор тегированного протокола».
2. **PCP** – в нем обычно записывается приоритет того или иного трафика. Чем приоритетнее трафик, тем больше шансов, что коммутатор обработает его первым. Полезная вещь в крупных сетях. Три буквы расшифровываются – как «Priority Code Point», а переводятся как – приоритет или значение приоритета
3. **CFI** – может иметь только два значения: 0 и 1, – так как данное поле имеет размер в 1 бит.
4. **VID** – определяет в каком VLAN находится выделенный кадр. Обычно состоит из 12 бит. Расшифровывается как VLAN ID.

* **Trunk port (магистральный порт)** – порт, который идет на другое сетевое устройство: коммутатор, маршрутизатор и т.д. Из этого порта обычно отправляются тегированные пакеты, то есть пакеты с этим самым тегом.
* **Access port (порт доступа)**– открытый или последний порт, из которого информация льется прямиком на компьютер пользователя. Сюда бессмысленно добавлять тег, забивая размер пакета.