VLAN – Virtual Local Area Network

VLAN (Virtual Local Area Network) – группа устройств, имеющих возможность взаимодействовать между собой напрямую на канальном уровне, хотя физически при этом они могут быть подключены к разным сетевым коммутаторам. И наоборот, устройства, находящиеся в разных VLAN'ах, невидимы друг для друга на канальном уровне, даже если они подключены к одному коммутатору, и связь между этими устройствами возможна только на сетевом и более высоких уровнях.

В современных сетях VLAN – главный механизм для создания логической топологии сети, не зависящей от её физической топологии. VLAN'ы используются для сокращения широковещательного трафика в сети. Имеют большое значение с точки зрения безопасности, в частности как средство борьбы с ARP-spoofing'ом.

Зачем нужен VLAN?

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.

Тегирование трафика VLAN

Компьютер при отправке трафика в сеть даже не догадывается,в каком VLAN’е он размещён. Об этом думает коммутатор. Коммутатор знает, что компьютер, который подключен к определённому порту,находится в соответствующем VLAN’е. Трафик, приходящий на порт определённого VLAN’а, ничем особенным не отличается от трафика другого VLAN’а. Другими словами, никакой информации о принадлежности трафика определённому VLAN’у в нём нет.

Однако, если через порт может прийти трафик разных VLAN’ов, коммутатор должен его как-то различать. Для этого каждый кадр (frame) трафика должен быть помечен каким-то особым образом. Пометка должна говорить о том, какому VLAN’у трафик принадлежит.

Наиболее распространённый сейчас способ ставить такую пометку описан в открытом стандарте IEEE 802.1Q. Существуют проприетарные протоколы, решающие похожие задачи, например, протокол ISL от Cisco Systems, но их популярность значительно ниже (и снижается).

Коммутатор и VLAN’ы

VLAN’ы могут быть настроены на коммутаторах, маршрутизаторах, других сетевых устройствах и на хостах. Однако, для объяснения

VLAN лучше всего подойдет коммутатор.

Коммутатор – устройство 2го уровня и изначально все порты коммутатора находятся, как правило, в VLAN 1 и, следовательно, в одном широковещательном сегменте.

Это значит, что если одно из устройств, которое подключено к порту коммутатора, отправит широковещательный фрейм, то коммутатор перенаправит этот фрейм на все остальные порты, к которым подключены устройства, и они получат этот фрейм.