

VLAN

01 мая 2023 года

Часто в средних и крупных сетях передачи данных требуется деление сети на отдельные сегменты. Однако в современных реалиях такое деление может потребоваться и в совсем небольших сетях на пару десятков пользователей. Приведу примеры сегментирования сети:

- по типу оборудования. Например разделить серверы и компьютеры пользователей;
- по структурным единицам компании. Например отделить отдел продаж от бухгалтерии.
- для небольших сетей может быть примером выделение в отдельную сеть гостевого Wi-Fi (бары, кафе, рестораны).

Деление сети можно выполнить подключением для каждого сегмента отдельного коммутатора. А в случае с Wi-Fi – подключением дополнительной точки доступа. Однако, очевидно, что этот путь весьма дорог и лишён гибкости в настройке сети. Поэтому широкое распространение получила технология разбиения сети на виртуальные подсети – Virtual Local Area Network (VLAN).

Технология достаточно проста, но для её применения всё же необходимо разобраться как она работает. Если в IP пакете есть VLAN – значит такой пакет называют тегированным. Если нету – то нетегированным. Есть оборудование, которое не понимает тегированный трафик (старые «неуправляемые» коммутаторы). Тем не менее стандарт 802.11Q предусматривает такое оборудование. В этом случае информация о VLAN игнорируется, его пропускает, просто оно не в состоянии распознать дополнительную информацию о VLAN в пакете, как то повлиять на неё или действовать в соответствии с установленными стандартом 802.11Q правилами. Также следует отметить, что помечать пакеты может как само оконечное устройство, так и коммутирующее оборудование (коммутаторы и маршрутизаторы). Как правило обычные компьютеры не тегировать свой трафик. Такой трафик можно тегировать на уровне коммутатора. Примером устройств, способных тегировать свой трафик являются IP телефоны. В этом случае порт на коммутаторе должен понимать, что принимает уже тегированный трафик.

Есть смешанная технология. Например, когда IP телефон подключен к порту коммутатора, а компьютер подключен ко второму порту IP телефона. Телефон и компьютер должны быть в разных VLAN-ах. В этом случае коммутатор должен принимать оба типа трафика. Такой порт называется гибридным.

Из выше изложенного, казалось бы, простая технология вызывает некоторые трудности в настройке. Потому что каждый производитель, в целом соблюдая стандарт, обозначает те или иные сущности по разному. Встречаются у производителей коммутирующего оборудования - tagged VLAN и untagged VLAN.

И некоторые «специалисты» начинают употреблять термины «тегированный VLAN» и «нетегированный VLAN». Но это не верно. Не бывает «нетегированных» VLANов. Если пакет помечен тегом, то значит ему назначен какой-то VLAN и такой трафик называют тегированным. Если не помечен, то никакого тега нет, и соответственно трафик - нетегированный и никакому VLANу принадлежать не может.

Tagged VLAN и untagged VLAN – это лишь свойства порта коммутирующего оборудования. В случае tagged VLAN – трафик на этом порту пометится тегом с соответствующим VLANом. Untagged VLAN – это свойство порта (как правило транкового) пропускать тегированный трафик заданного VLANа (но не помечать дополнительно его).

На оконечном оборудовании, которое способно помечать свой трафик VLANом – никогда не найти понятия tagged/untagged. Потому что это свойство исключительно коммутирующего оборудования.