Лекция 8

Принципы и конфигурация виртуальных локальных сетей VLAN

6B06201 - Радиотехника, электроника и телекоммуникации

А.А. Хохлов • Алматы, 2026

Цель лекции

- Сформировать знания о технологии виртуальных локальных сетей VLAN и её применении для логической сегментации корпоративной сетевой инфраструктуры.
- Изучить принципы разделения единой физической сети на независимые широковещательные домены, особенности идентификации VLAN и механизмы маркировки Ethernet-кадров в соответствии со стандартом IEEE 802.1Q.
- Рассмотреть назначение интерфейсов Access, Trunk и Hybrid, особенности передачи маркированных и немаркированных кадров, а также принципы назначения портов коммутаторов различным VLAN.
- Сформировать понимание практических подходов к проектированию и настройке VLAN для разделения пользовательских групп, повышения управляемости сети и ограничения распространения широковещательного трафика.

Результаты обучения

По завершении лекции обучающийся сможет:

- Объяснять назначение технологии VLAN и её роль в логической сегментации корпоративных Ethernet-сетей.
- Характеризовать механизм IEEE 802.1Q и различать режимы работы интерфейсов Access, Trunk и Hybrid.
- Описывать последовательность создания VLAN, назначения портов и проверки корректности передачи кадров между коммутаторами.

Зачем нужны виртуальные сети VLAN?

Единая сеть Ethernet

При большом числе узлов широковещательные кадры распространяются по всей общей сети.

Разделение на VLAN

Логические сегменты создают отдельные широковещательные домены на общих коммутаторах.

VLAN структурирует сеть, но не заменяет межсетевой экран и ACL.

Логическая сегментация одной физической сети

Пример: учебные лаборатории и административные службы



- Одна VLAN может охватывать разные коммутаторы.
- Кадры VLAN 20 не попадают в VLAN 10 при обычной L2-пересылке.

IEEE 802.1Q: тегирование Ethernet-кадров

802.1Q-тег занимает 4 байта и содержит TPID и TCI



- TPID: обычно 0x8100; TCI: PCP (3 бита), DEI (1 бит), VID (12 бит).
- Рабочие идентификаторы VLAN: 1–4094; значения 0 и 4095 специальные.

Тегированные и нетегированные кадры

Untagged

Кадр не содержит 802.1Q-тег. При поступлении на порт его VLAN определяет PVID.

Tagged

Кадр содержит VID; магистраль может переносить трафик нескольких VLAN.

PVID = VLAN для классификации входящего нетегированного кадра.

Как назначается принадлежность к VLAN

По порту

Наиболее распространённый способ: физический интерфейс привязан к сегменту.

По MAC-адресу

Используется таблица соответствия MAC → VLAN. Не является надёжной аутентификацией.

По политике

Назначение с учётом IP-подсети, протокола или механизма доступа, если поддерживается.

Режимы портов Access, Trunk и Hybrid

Access

Обычно одна VLAN. Для подключения компьютера; передача клиенту без тега.

Trunk

Несколько разрешённых VLAN по одному каналу между коммутаторами.

Hybrid

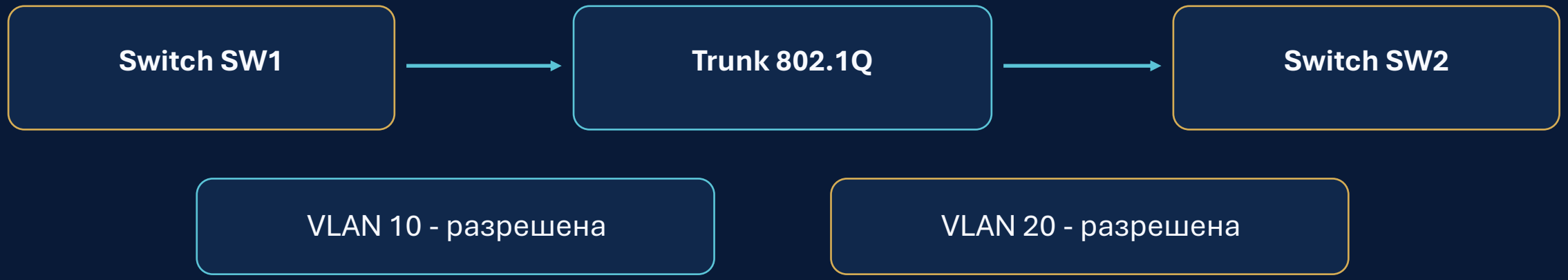
Несколько VLAN; отдельно задаётся формат Tagged / Untagged для каждого сегмента.

Access-порт: конечное устройство



- Клиент обычно отправляет нетегированные Ethernet-кадры.
- Входящие кадры связываются с PVID (в примере VLAN 10).
- Сигнал для устройства передаётся без VLAN-тега.

Trunk: две VLAN через одну магистраль



- Проверяют список allow-pass VLAN и согласованность PVID.
- В типовом VRP кадр VLAN, равной PVID trunk, передаётся без тега.

Hybrid: гибкая обработка VLAN

Входной трафик

PVID определяет VLAN для нетегированного кадра.

Исходящий трафик

Для каждой VLAN задают Tagged или Untagged.

Пример: PVID 10 • VLAN 10: Untagged • VLAN 20: Tagged

Передача кадра VLAN 10 между двумя коммутаторами

01	**ПК А → SW1**	Untagged на access-порт VLAN 10
02	**SW1 → SW2**	По trunk с нужной обработкой 802.1Q
03	**SW2 → ПК Б**	Untagged через access VLAN 10

Для обмена между VLAN 10 и VLAN 20 нужна маршрутизация L3.

Команды Huawei VRP: создание VLAN и порты

Создать VLAN	`vlan batch 10 20 100`
Access VLAN 10	`port link-type access` `port default vlan 10`
Trunk VLAN 10, 20	`port link-type trunk` `port trunk allow-pass vlan 10 20`
Проверить	`display vlan  |  display port vlan`

После проверки сохранить текущую конфигурацию: save

Типичные ошибки конфигурации VLAN

01 Нужная VLAN не разрешена на trunk

02 PVID не совпадает на концах соединения

03 Неверная настройка Tagged / Untagged в hybrid

04 Ошибки VLAN ID, IP-шлюза и правил L3-доступа

05 Отсутствие резервной копии и проверки изменений

Проверяйте: display vlan, display port vlan, display current-configuration

Итоги и контрольные вопросы

- VLAN создаёт отдельные широковещательные домены на общей инфраструктуре.
- Тег IEEE 802.1Q переносит идентификатор VLAN между устройствами.
- Access, trunk и hybrid различаются правилами обработки кадров.
- PVID определяет VLAN входящего нетегированного кадра.
- Между разными VLAN необходим L3-маршрутизатор и политика доступа.

Вопрос: чем отличаются режимы trunk и hybrid?