Networking
For everyone

VLANs and Ports

Сегодня в выпуске:

- VLANы
  - Стандартные
  - Расширенные
  - VLAN база данных
- Типы портов
  - Порт доступа
  - 802.1Q транк
  - Динамическое согласование типа порты

Virtual Local Area LAN

VLANы

- Есть несколько подходов к определению того, что такое VLAN
  - «стандартный» – как разделение границ широковещательного домена
  - «IETF edition»
  - Какой из них выбрать – решать Вам
- В целом, все VLANы можно разделить на несколько категорий
  - Стандартные
  - Расширенные
  - Внутренние
    - Platform depends

Коммутация с VLAN

- Эмуляция нескольких несвязанных сегментов Ethernet
  - VLAN – Virtual LAN, виртуальный широковещательный домен
  - Домены коллизий объединены в несколько широковещательных доменов
  - Обычно VLAN нумеруются от 1 до 4094
- На устройстве запускаются несколько таблиц коммутации
  - Любой кадр коммутируется только по одной из них
  - Максимально поддерживаемое число таблиц обычно меньше 4094*

Стандартные VLANы

- Относятся к диапазону от 1 до 1005
- VLAN 1
  - Стандарт для всех Cisco устройств
  - Нельзя удалить
  - Не может быть подавлена протоколом VTP
  - Не рекомендуется к использованию в боевых сетях
- VLAN 1002 – 1005
  - Token Ring/FDDI
  - Не используются в боевых сетях

Расширенные VLANы

- Относятся к диапазону 1006 – 4094
- Не передаются с помощью VTP
  - Если не брать в расчет VTPv3
- В большинстве случаев не все из них могут использоваться в сети
  - Часть является зарезервированными для внутренних нужд коммутатора
    - show vlan internal usage

Создание VLAN

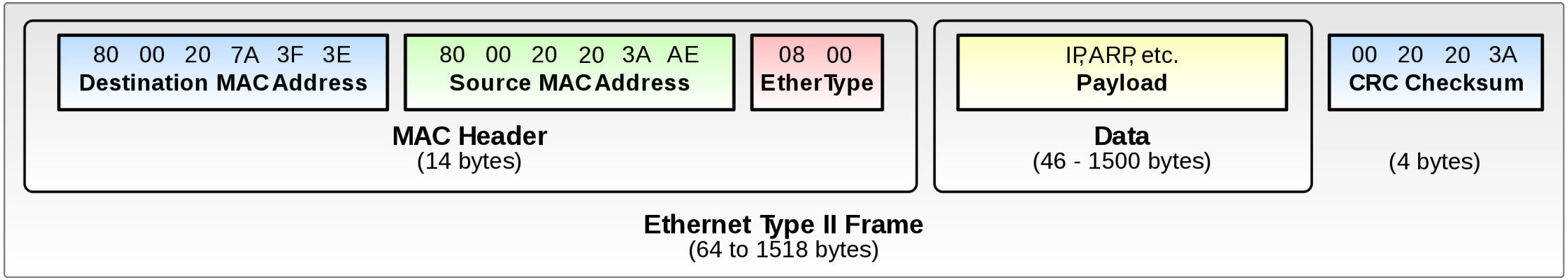
- Создание VLAN автоматически влечет за собой создание
  - STP дерева
  - Таблицы MAC
- Основные команды для проверки
  - show vlan [brief]
  - show spanning-tree vlan {VLAN_ID}

Ethernet порты

Типы Ethernet

- Ethernet v1
  - Довольно редкий вид
  - Из известного мне – применяется только в IS-IS
- Ethernet v2
  - Именно с ним Вы работаете ежедневно

Формат кадра DIX



Типы портов

- Порты 2-го уровня
  - Access
  - Trunk
  - Tunnel
  - и др.
- Порты 3-го уровня
  - SVI
  - no switchport

Порты 2-го уровня

- Access
  - Позволяют передавать трафик для одной VLAN
    - switchport mode access
- Trunk
  - Позволяют передавать трафик для одной или более VLAN
    - switchport mode trunk
- Tunnel
  - Прозрачная передача L2 трафика сквозь некое «облако»
    - switchport mode tunnel
- Динамические
  - DTP

Порты типа «access»

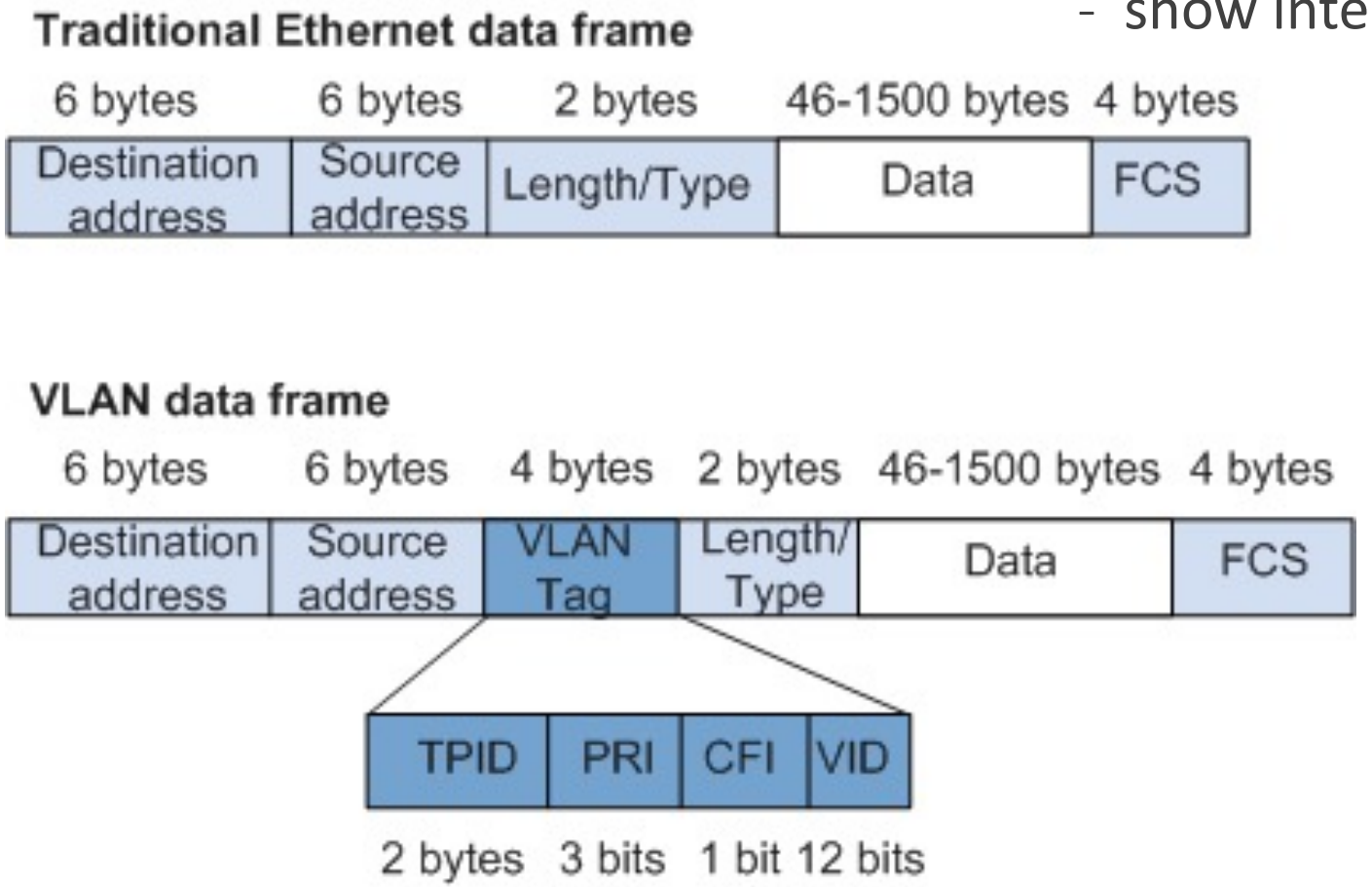
- Обычные абоненты ничего не знают про VLAN
  - В заголовке Ethernet нет указания на VLAN
- Как определить принадлежность кадра к VLAN?
  - По информации из содержимого кадра - небезопасно и немасштабируемо
  - Назначать один VLAN всем кадрам, приходящим на порту, легко и удобно
    - Проще всего - статически

Метки VLAN

- Есть несколько способов добавить в кадр информацию о VLAN:
- Cisco ISL: инкапсуляция в другой протокол
  - Проприетарный протокол
  - Номер VLAN указывается в заголовке ISL
  - Оверхед 30 байт (26 – заголовок, 4 – трейлер)
  - Врятли встретите в современном мире
- IEEE 802.1Q: добавление нового поля в кадр
  - Поддерживается всеми вендорами
  - Оверхед 4 байта

Стандарт 802.1 Q

- Для различия VLAN – отдельное поле в кадре
  - show interface trunk



- На портах доступа передаются кадры одного VLAN без метки
  - untagged – тот самый абонентский VLAN
  - tagged – не передаются
- На транках 802.1Q кадры могут передаваться с меткой и без:
  - untagged – не более одного VLAN, в терминологии Cisco – Native VLAN
    - switchport trunk native vlan {VLAN_ID}
      - Существуют атаки
  - tagged – все остальные VLAN
    - switchport trunk allowed vlan {VLAN_LIST}
      - Аккуратнее !!!

Dynamic Trunk Protocol

- Сеть предприятия работает хорошо, когда:
  - Абонентские порты работают в режиме access
  - Порты между однотипно настроенными коммутаторами - транки
- Коммутаторы Cisco поддерживают DTP (Dynamic Trunking Protocol)
  - Если сосед с DTP в том не обнаружен – порт переходит в access
  - Если сосед обнаружен в другом домене VTP – порт переходит в access
  - С соседом с DTP на порту автоматически включается транк (ISL или 802.1Q)
- По умолчанию DTP работает на всех портах
  - В старых версиях IOS – активно ищет соседей и пытается согласовать транк
  - В новых – активно ищет соседей, но не пытается согласовать транк

Рекомендации по транкам

- Вообще везде выключить поддержку DTP
  - На статических транках бесполезен
  - На абонентских портах – не нужен
- Рекомендации по портам:
  - Абонентские и незадействованные порты фиксировать в режиме access
  - До коммутаторов предприятия фиксировать статический транк 802.1Q
- Настройки на соседних транковых портах должны совпадать:
  - Одинаковые Native VLAN (и отсутствующие в базе)
  - Одинаковый набор Allowed VLAN

Голосовой VLAN

- Режим порта Catalyst для сквозного подключения IP-телефонов
  - Настройки для режима static access, кадры телефона помечаются Voice VLAN
  - Автонастройка IP-телефона Cisco с помощью CDP
  - "Это не транк, а Multi-VLAN порт" © Cisco

Межвиланная коммутация

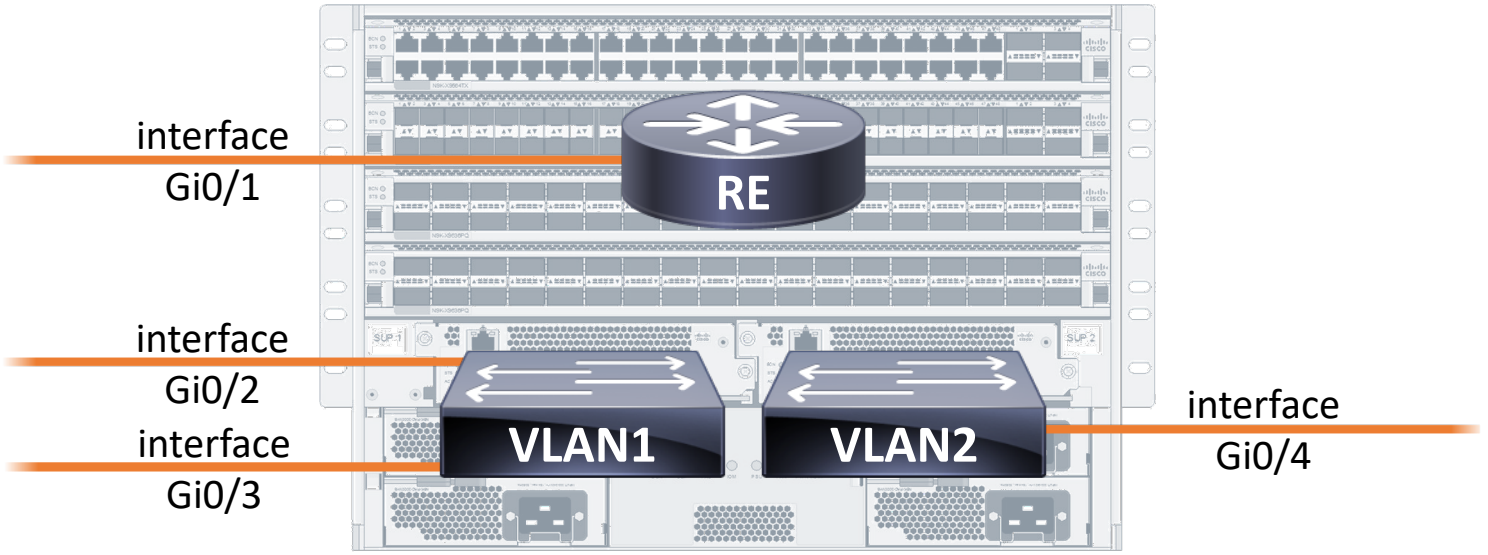
Транки на маршрутизаторах

- Настройки IP назначаются на интерфейсе
  - Каждому VLAN нужен отдельный интерфейс для соответствующих настроек маршрутизатора
  - Физический интерфейс один, но к нему создаются дочерние субинтерфейсы

Работа с субинтерфейсами

- Если родительский (физический) интерфейс выключен, субинтерфейсы работать не будут
  - Можно выключить отдельный субинтерфейс
- Все настройки, относящиеся к конкретному VLAN, выполняются на соответствующих субинтерфейсах

- SVI – Switch Virtual Interface
  - Виртуальный интерфейс RE, подключенный к VLAN как терминальный узел



Networking For everyone