Настройка VLAN’ов и маршрутизации между ними

Петухов Андрей
petand@lvk.cs.msu.su
Антоненко Виталий
anvial@lvk.cs.msu.su
комната 247

Логика возникновения (1 из 5)

- Дано: абонентские машины, технология Ethernet, коммутаторы, 85-90 годы 20 века
- Порешаем две задачи:
  - попробуем построить глобальную сеть
  - попробуем построить хотя бы корпоративную сеть
- Пусть порядок глобальной сети – 10^6 абонентских машин:
  - Каждый коммутатор должен иметь таблицу на 10^6 mac-адресов, или $(6+1)*10^6$ байт = примерно 7Мб
  - Поиск в такой таблице будет занимать по грубой оценке 3 500 000 операций сравнения, если таблица не отсортирована, или будут накладки на поддержку отсортированной таблицы
  - Так как сеть плоская, то одинаковые требования предъявляются как к абонентским коммутаторам, так и к магистральным
  - IBM AT в 1984 году: 6МГц, 512Кб – 1Мб ОЗУ

Логика возникновения (2 из 5)

- А что будет в корпоративном секторе?
  - рассмотрим организацию с сетью на 10 000 абонентов
- Для разрешения адресов используется ARP
- Прикинем масштаб вещательного трафика:
  - пусть каждый абонент в среднем посылает один ARP-запрос каждую минуту и получает на него ARP-ответ
  - длина запроса и ответа примерно 30 байт
  - суммарный служебный трафик за минуту составит $60*10^4$ или 10^4 байт в секунду, то есть примерно 0.1Мбит/сек будет тратиться на служебный трафик
  - кроме того, каждый хост должен будет в секунду обработать 10^4 вещательных кадров (огромная нагрузка на конечные устройства!!!)

Логика возникновения (3 из 5)

- Проблема масштабируемости технологии
  - из-за плоской организации адресации
  - из-за метода разрешения адресов сетевого уровня
- Решения обеих проблем хорошо известны
  - иерархическая адресация
    - см. телефонные сети
  - разделение большого вещательного домена на N маленьких
- Заметим, что задача передачи данных в сетях с небольшим числом абонентов уже решена
- Новый уровень – сетевой – решение задачи передачи данных в больших сетях (см. масштабирование)
  - метод сведения задачи к решенной – надо разбить большую сеть на кучу маленьких, в которых мы уже все умеем

Логика возникновения (4 из 5)

Иерархическая адресация

- Иерархическая адресация позволит сократить время поиска и снизить использование памяти
  - см. телефонные сети
- Иерархию на mac-адресах реализовать невозможно (их распределение не контролируется, они вшиты в сетевую карту)
- Надо ввести логическую адресацию
- Логическая адресация должна содержать как минимум три уровня:
  - ID организации для маршрутизации в глобальной сети
  - ID подразделения для маршрутизации внутри организации
  - ID абонента в подразделении
- Кол-во абонентов в подразделении можно выбирать из соображений объема вещательного трафика

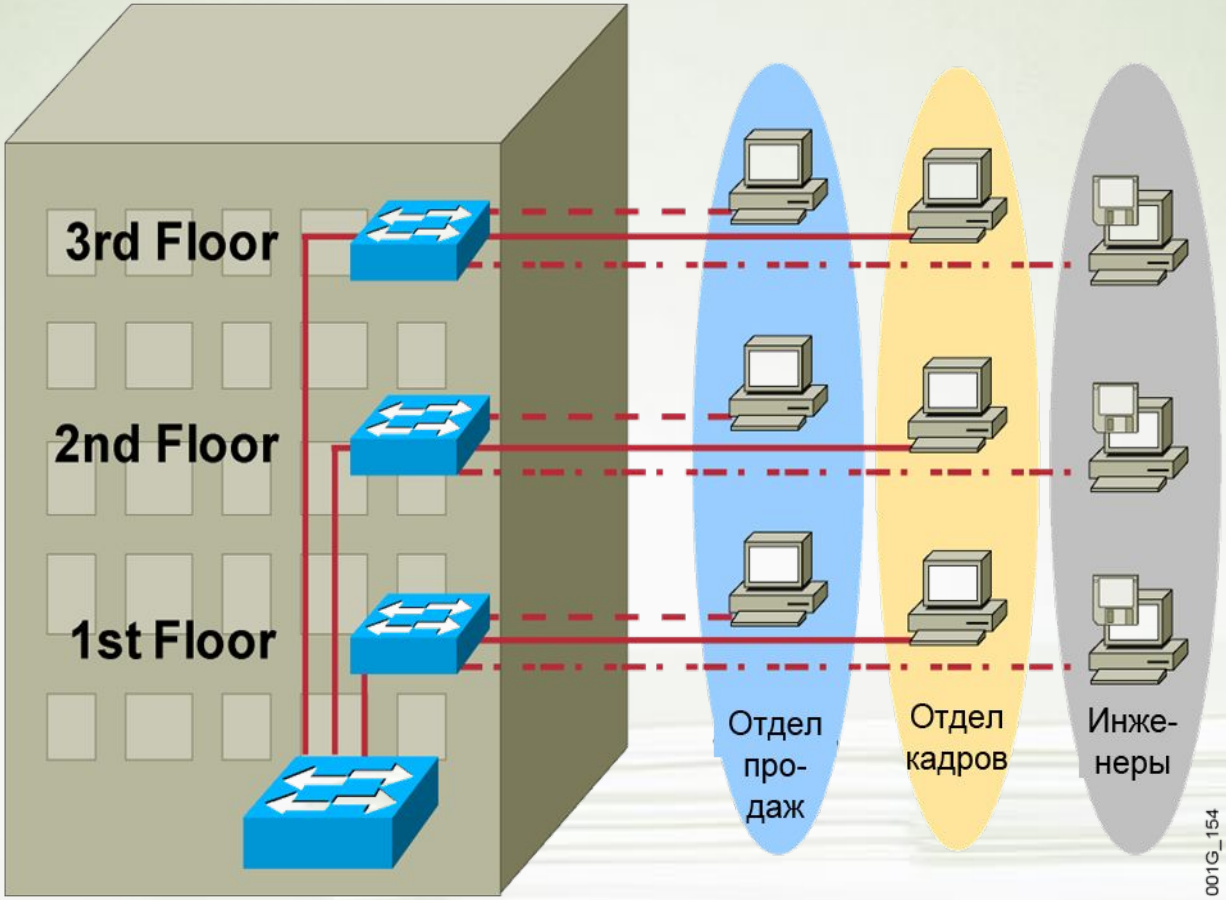
Логика возникновения (5 из 5)

- Протокол IP – протокол с иерархической адресацией
- IP адрес состоит из ID сети, опционально ID подсети, и ID хоста в (под)сети
  - для каждой (под)сети определен вещательный адрес, который отображается протоколом ARP на вещательный mac-адрес
- Раз IP – логическая адресация, нужна организация по раздаче адресов, IANA
  - IANA раздает ID сетей организациям; организация сама решает, как разбить сеть на подсети и как назначить ID хостам в подсетях
- Подсеть = вещательный домен
- Для пересылки данных между подсетями используются уже не MAC, а IP-адреса, а соответствующую логику реализуют маршрутизаторы
  - это потому, что ARP-запрос не выходит за пределы вещательного домена!
- Т.е. маршрутизаторы используются для сегментирования больших вещательных доменов на более маленькие так же, как коммутаторы использовались для сегментирования доменов коллизии

And more…

- Вещательный домен определяется на основе физических характеристик – близости расположения абонентов, подключенных к группе коммутаторов
- По концепции создания подсеть – это логическая группа, а сетевая адресация – абстракция над физической
- Но ведь подсеть должна отображаться на вещательный домен и наоборот
- Получается противоречие: логическая группа на самом деле никакая не логическая, а определяется исключительно близостью расположения хостов
- Чтобы решить эту проблему придумали понятие виртуального коммутатора
- Физический коммутатор может включать несколько виртуальных, каждый из которых будет обслуживать свой вещательный домен
- Один виртуальный вещательный домен может распространятся на несколько коммутаторов
- Виртуальный вещательный домен – это и есть VLAN

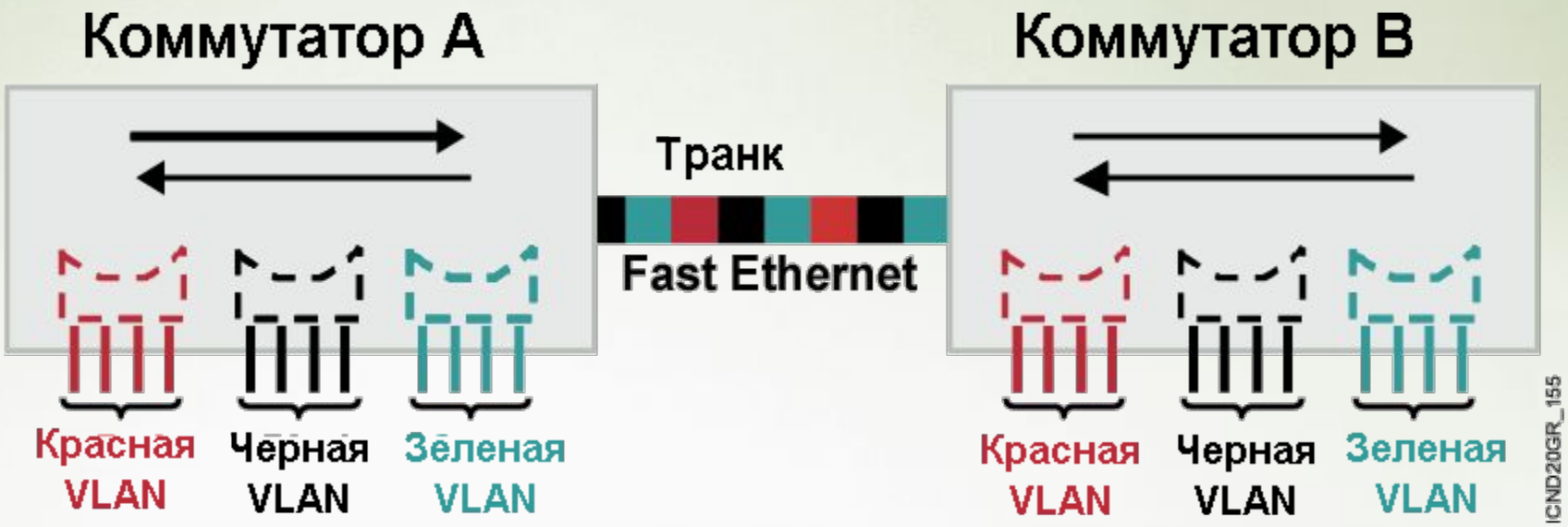
Пример VLAN



- **Разделение**
- **Гибкость**
- **Безопасность**

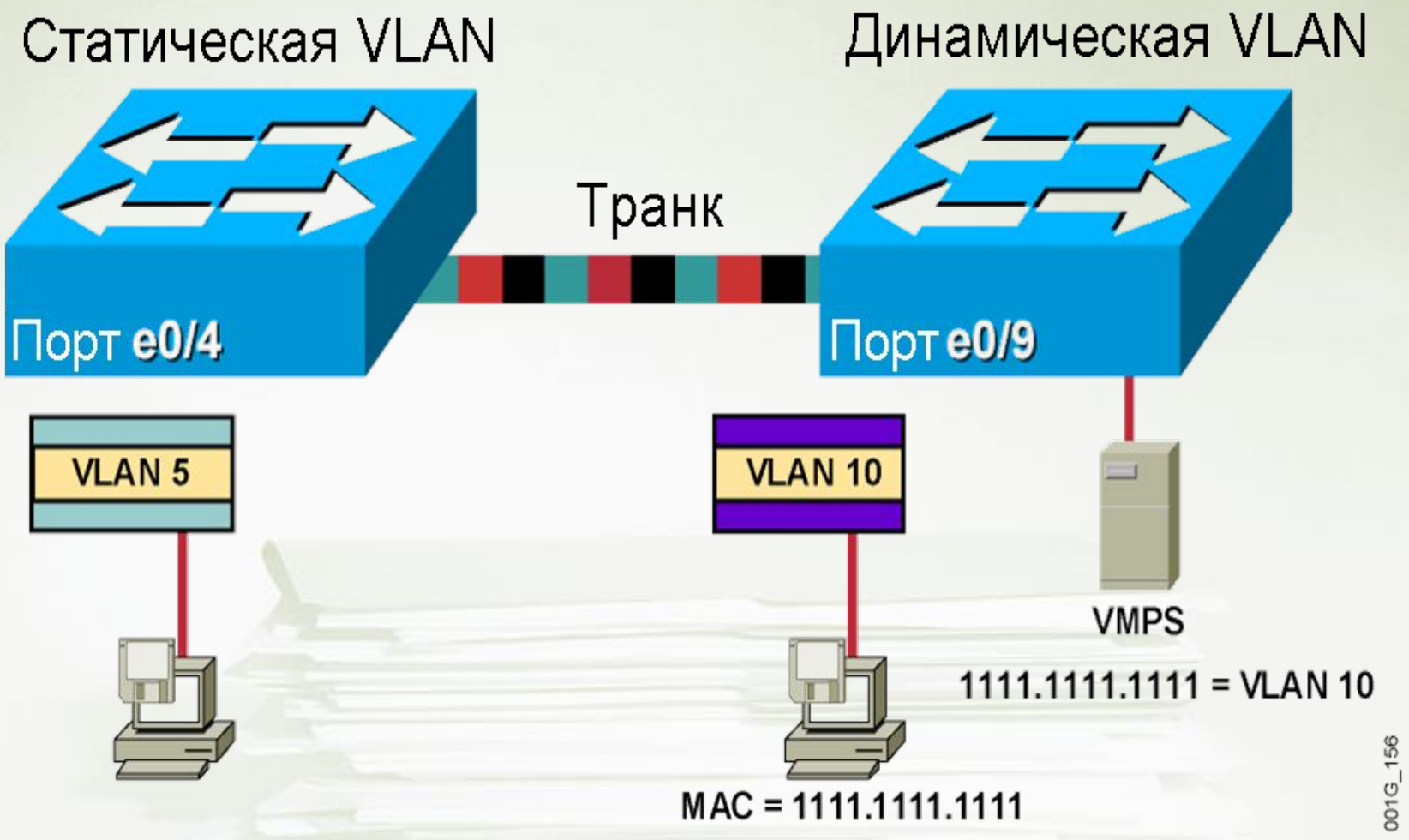
VLAN = Вещательный домен = Логическая сеть (Подсеть)

Функционирование VLAN

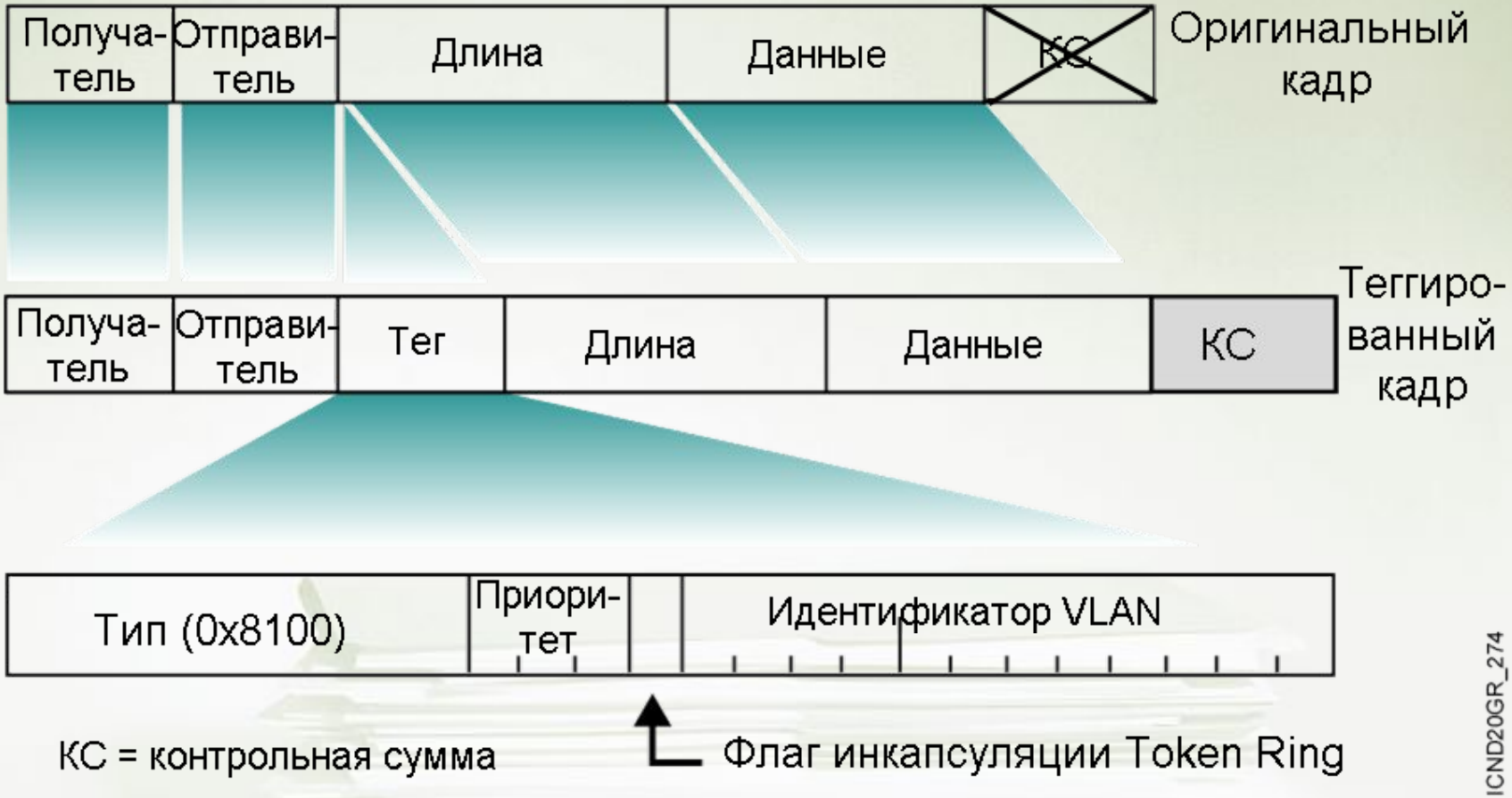


- Каждая логическая VLAN – как отдельный физический мост
- Для пересылки кадров, исходящих из разных VLAN используются транки
- Транки используют специальную инкапсуляцию для того, чтобы различать кадры, принадлежащие разным VLANам

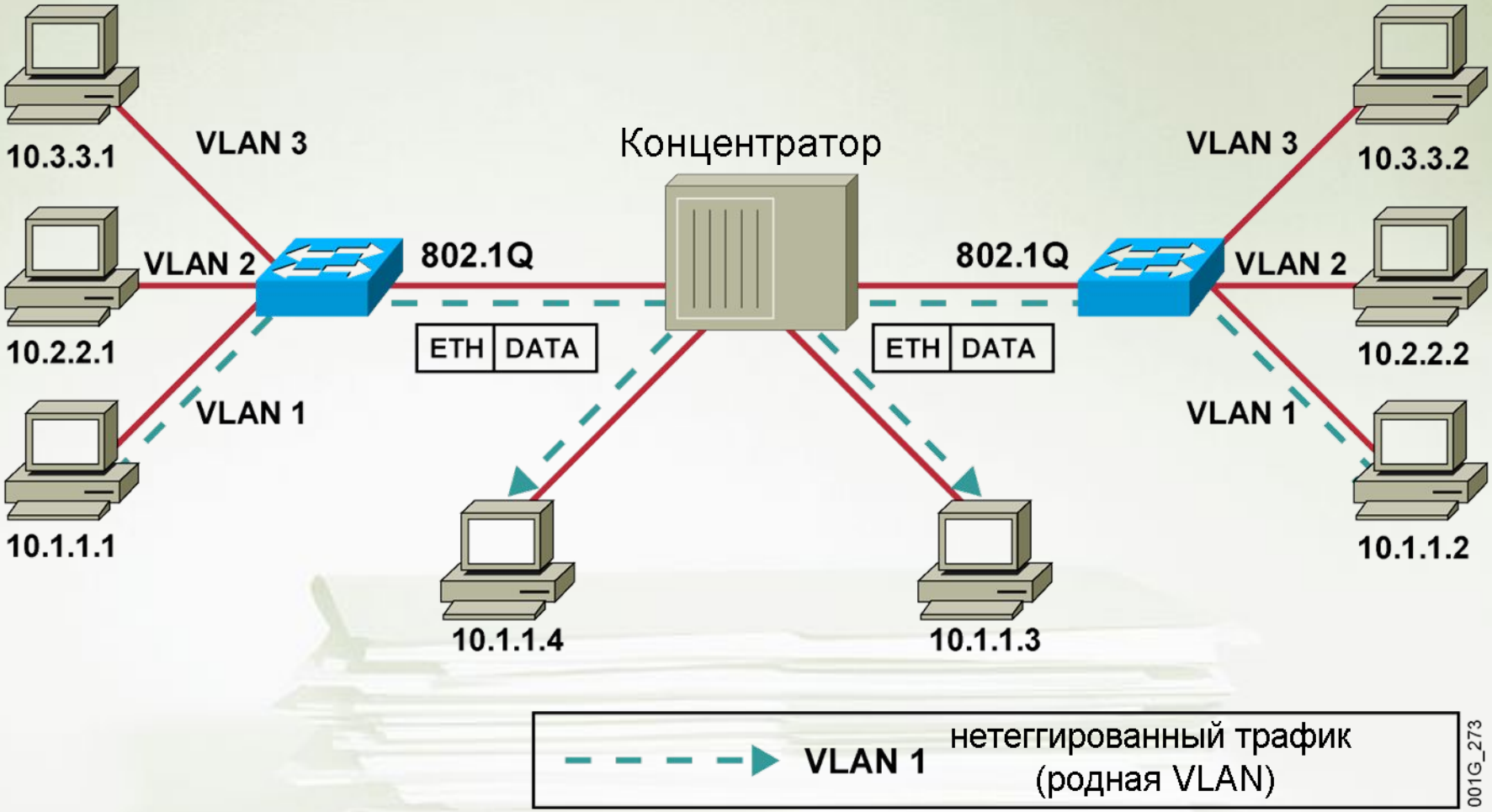
Членство в VLAN



Кадр 802.1Q


Получа-тель
Отправи-тель
Длина
Данные
КС
Оригинальный кадр
Получа-тель
Отправи-тель
Тег
Длина
Данные
КС
Теггиро-ванный кадр
Тип (0x8100)
Приори-тет
Идентификатор VLAN
КС = контрольная сумма
Флаг инкапсуляции Token Ring
ICND20GR_274

Родные VLANы



Добавление VLAN

Catalyst 2950 Series

```
Switch# configure terminal
Switch(config)# vlan 2
Switch(config-vlan)# name VLAN2
```

- VLAN 1 есть по умолчанию
- По умолчанию VLAN 1 используется для управления и может иметь IP адрес
- CDP и прочие служебные протоколы используют VLAN 1

Добавление портов в VLAN

Catalyst 2950 Series

```
wg_sw_2950(config-if)# switchport access [vlan vlan# |
                                dynamic]
```

```
wg-sw_2950# configure terminal
wg_sw_2950(config)# interface fastethernet 0/2
wg_sw_2950(config-if)# switchport access vlan 2

wg_sw_2950# show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -----------------------
1    default                          active    Fa0/1, Fa0/3, Fa0/4
  .    .    .    .    .
2    vlan2                            active    Fa0/2
```

Настройка транка 802.1Q

```
SwitchX(config-if)
#switchport mode {access |  dynamic {auto | desirable} | trunk}
```

- Позволяет перевести порт в режим транка и обратно

```
SwitchX(config-if)
#switchport mode trunk
```

- Переводит порт в режим транка

Проверка настроек транка

```
SwitchX# show interfaces interface [switchport | trunk]
```

```
SwitchX# show interfaces fa0/11 switchport
Name: Fa0/11
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
```

. . .

```
SwitchX# show interfaces fa0/11 trunk

Port        Mode         Encapsulation  Status       Native vlan
Fa0/11      desirable    802.1q         trunking     1

Port      Vlans allowed on trunk
Fa0/11      1-4094

Port        Vlans allowed and active in management domain
Fa0/11      1-13
```

Просмотр членства портов в VLANах

```
wg_sw_2950# show vlan
brief
```

```
wg_sw_2950# show vlan brief
VLAN Name                             Status    Ports
---- -------------------------------- ---------
-------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
2    vlan2                            active
3    vlan3                            active
4    vlan4                            active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup

VLAN Name                             Status    Ports
---- -------------------------------- ---------
-------------------------------
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

```
wg_sw_2950# show interfaces interface
switchport
```

Обеспечение безопасности портов

Коммутаторы серии Catalyst 2950

```
SwitchX(config-if)#switchport port-security [  mac-address
mac-address | mac-address sticky [mac-address] | maximum value |
violation {restrict | shutdown}]
```

```
SwitchX(config)#interface fa0/5
SwitchX(config-if)#switchport mode access
SwitchX(config-if)#switchport port-security
SwitchX(config-if)#switchport port-security maximum 1
SwitchX(config-if)#switchport port-security mac-address 00d0.58ad.cb1f
SwitchX(config-if)#switchport port-security violation shutdown
SwitchX(config-if)#switchport port-security aging time 10
```

Проверка настроек безопасности портов (1 из 2)

```
SwitchX#show port-security [interface interface-id] [address] [ |
{begin | exclude | include} expression]
```

```
SwitchX#show port-security interface fastethernet 0/5
Port Security                : Enabled
Port Status                  : Secure-up
Violation Mode               : Shutdown
Aging Time                   : 20 mins
Aging Type                   : Absolute
SecureStatic Address Aging   : Disabled
Maximum MAC Addresses        : 1
Total MAC Addresses          : 1
Configured MAC Addresses     : 0
Sticky MAC Addresses         : 0
Last Source Address          : 0000.0000.0000
Security Violation Count     : 0
```

Проверка настроек безопасности портов (2 из 2)

```
SwitchX#sh port-security address
          Secure Mac Address Table
-----------------------------------------------------------------------
Vlan    Mac Address       Type                  Ports   Remaining Age
                                                            (mins)
----    -----------       ----                  -----   -------------
 1      0008.dddd.eeee    SecureConfigured      Fa0/5        -
-----------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
```

```
SwitchX#sh port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                (Count)       (Count)          (Count)
-----------------------------------------------------------------------
      Fa0/5        1             1                0          Shutdown
-----------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
```

Функции маршрутизаторов

```
RouterX# show ip route
D 192.168.1.0/24 [90/25789217] via 10.1.1.1
R 192.168.2.0/24 [120/4] via 10.1.1.2
O 192.168.3.0/24 [110/229840] via 10.1.1.3
```

1

2

1. По адресу назначения определять, через какой интерфейс переслать пакет дальше
2. Передавать соседним маршрутизаторам сведения о тех сетях, в которые он умеет пересылать пакеты

Таблицы маршрутизации

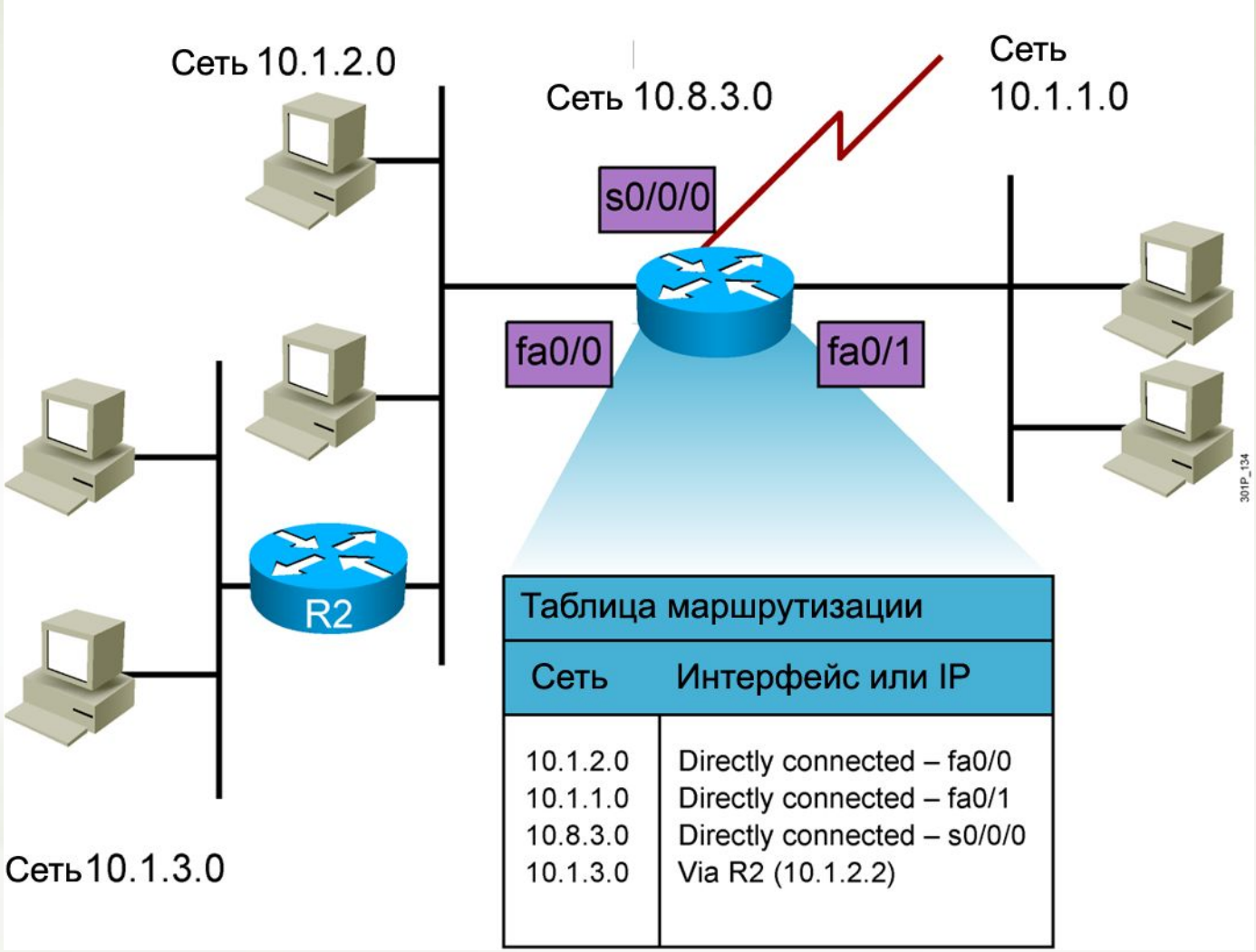
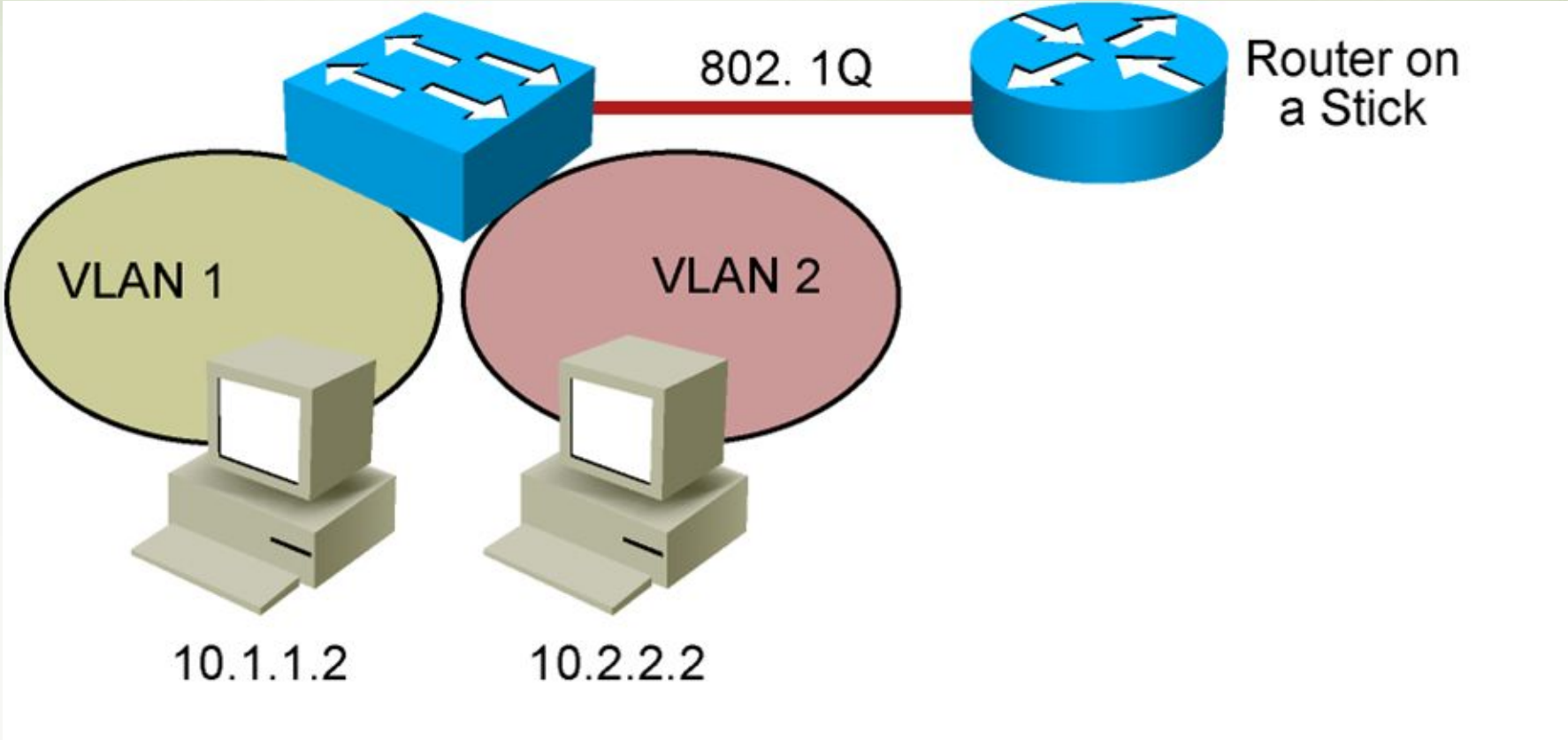


Таблица маршрутизации	
Сеть	Интерфейс или IP
10.1.2.0	Directly connected – fa0/0
10.1.1.0	Directly connected – fa0/1
10.8.3.0	Directly connected – s0/0/0
10.1.3.0	Via R2 (10.1.2.2)

Записи в таблице маршрутизации

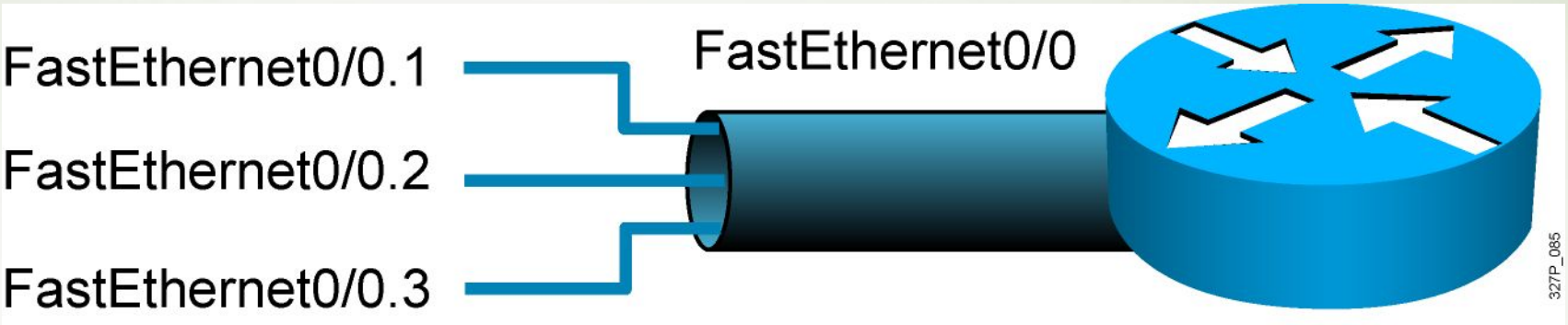
- Подключенные сети: сети, адреса из которых настроены на интерфейсах маршрутизатора
- Статические маршруты – маршруты, заданные администратором
- Динамические маршруты – маршруты, вычисленные устройством в результате обмена маршрутной информацией по одному из протоколов маршрутизации
- Маршрут по умолчанию: статический или динамический маршрут, по которому будут пересылаться пакеты, если путь к адресу назначения не задан в таблице явно

Маршрутизация между VLAN’ами



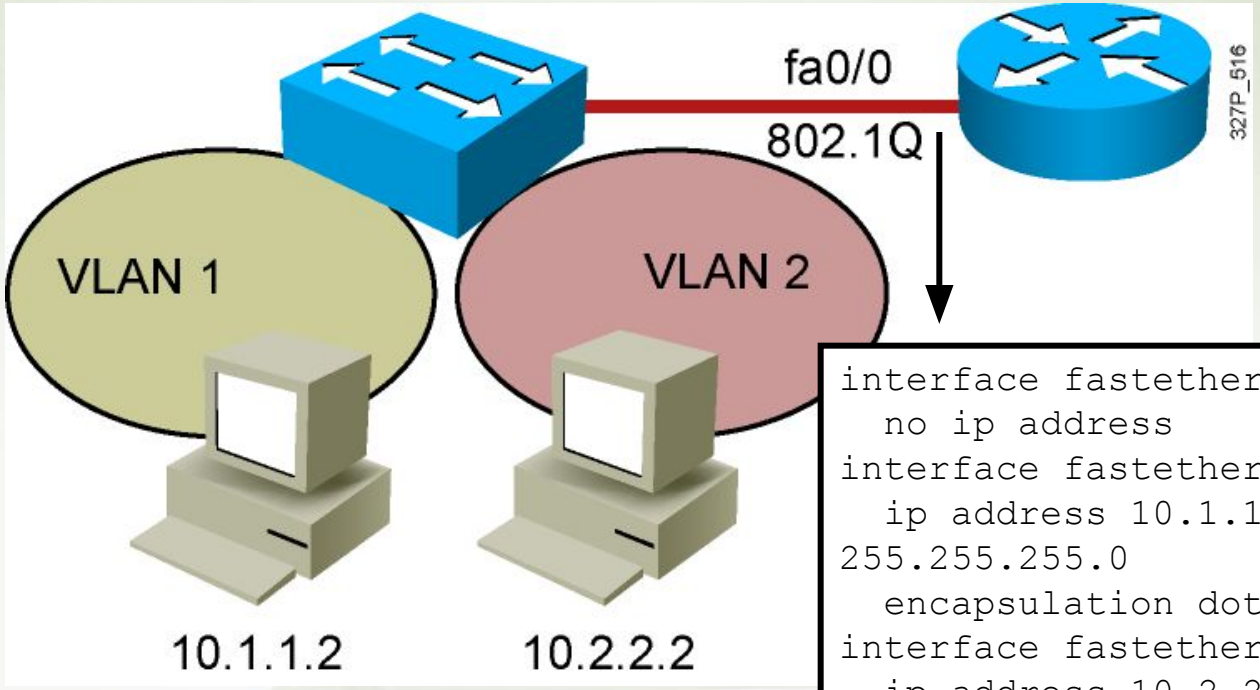
- Для пересылки данных между вещательными доменами необходим маршрутизатор

Создание логических подинтерфейсов на основе одного физического



- Для каждого вещательного домена, подключенного к маршрутизатору через транк, нужно создать свой логический подинтерфейс

Реализация «router-on-a-stick»




```
interface fastethernet 0/0
  no ip address
interface fastethernet 0/0.1
  ip address 10.1.1.1
255.255.255.0
  encapsulation dot1q 1
interface fastethernet 0/0.2
  ip address 10.2.2.1
255.255.255.0
  encapsulation dot1q 2
```

Проблема: нет связи между хостами

- Проверить физическое подключение
- Проверить настройки безопасности портов
- Проверить, изучает ли коммутатор MAC адреса хостов
- Проверить, не пересчитывается ли STP
- Если хосты в одной VLAN, они должны иметь IP адреса в одной подсети
- Если хосты в разных VLAN, необходимо проверить маршрутизацию и транки

Вопросы?