Настройка VLAN’ов и маршрутизации между ними

Антоненко Виталий
anvial@lvk.cs.msu.su

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

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

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

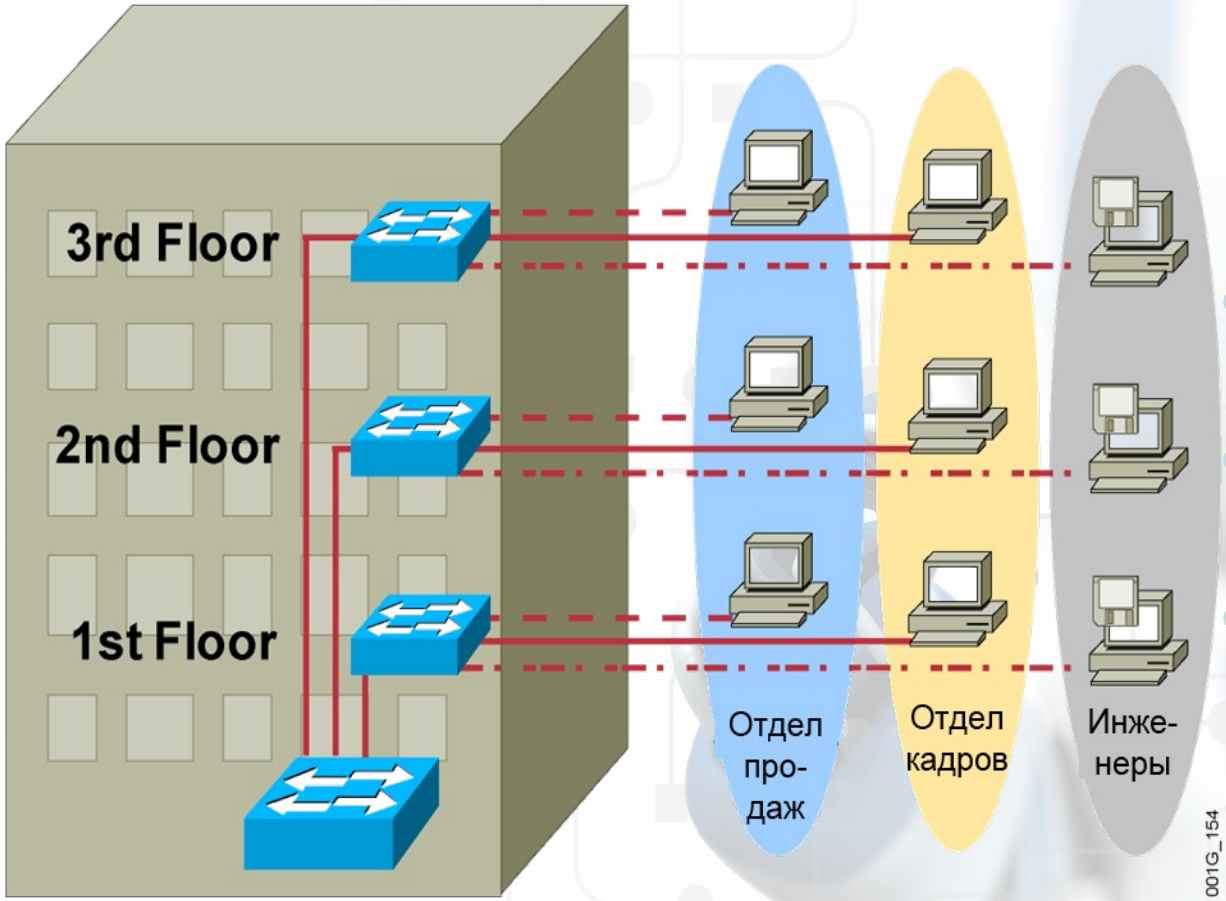
Логика возникновения (5 из 5)

- 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

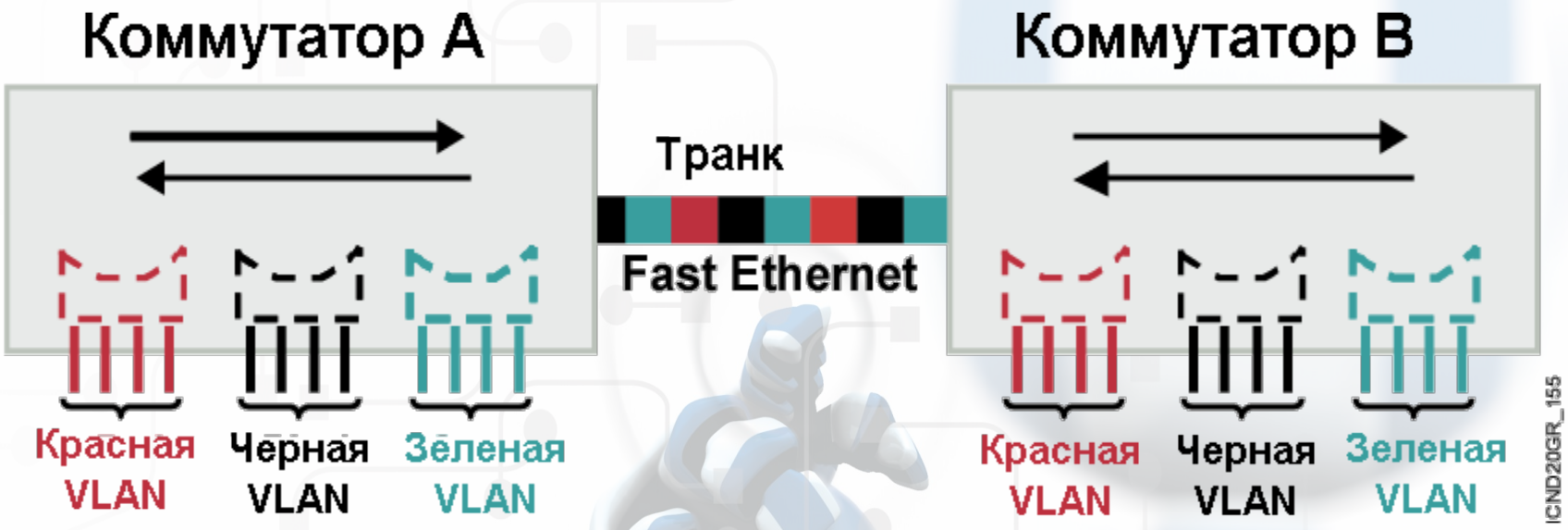
Пример VLAN



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

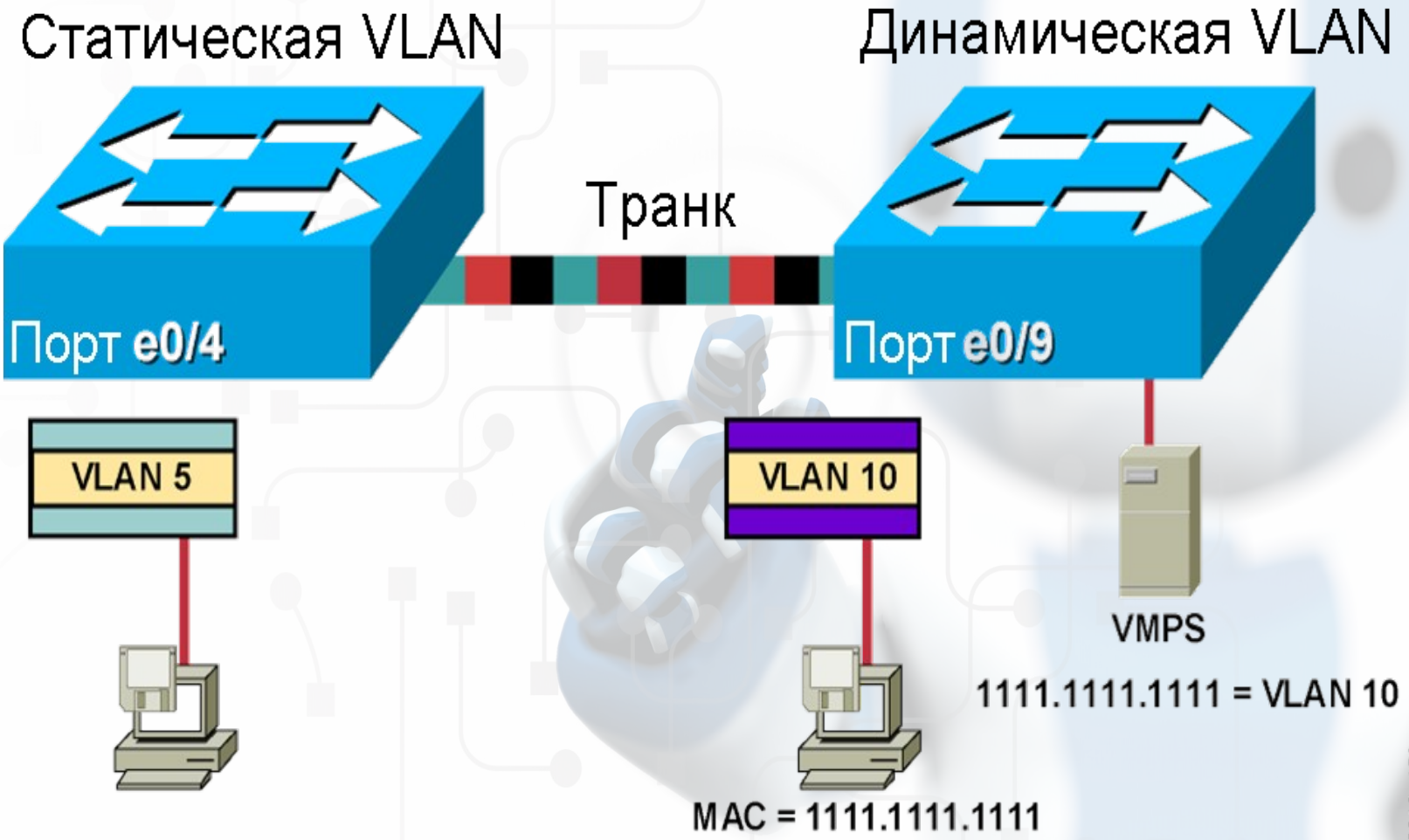
VLAN = Вещательный домен = Логическая сеть (Подсеть)

Функционирование VLAN

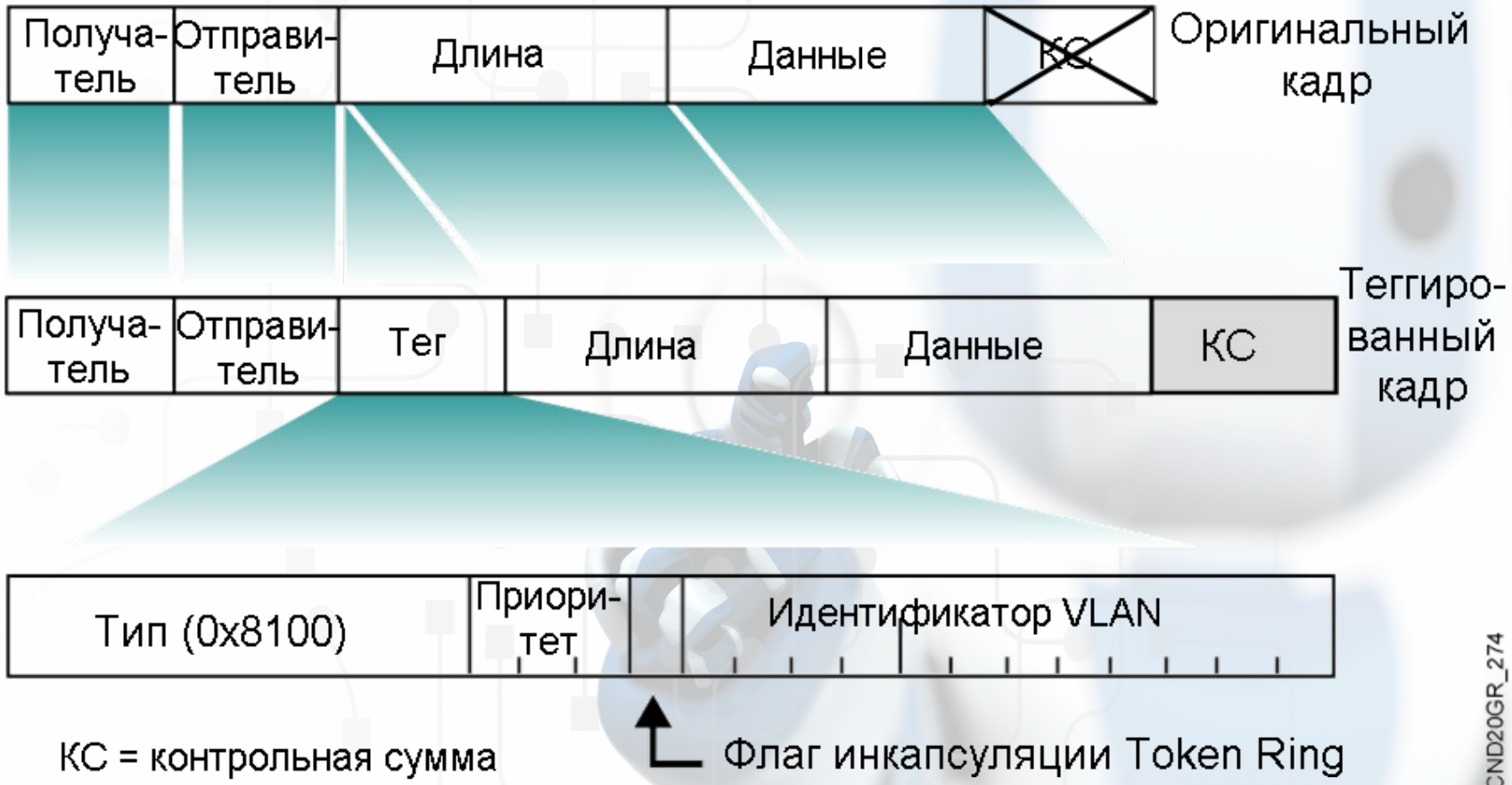


- Каждая логическая VLAN – как отдельный физический мост
- Для пересылки кадров, исходящих из разных VLAN используются транки
- Транки используют специальную инкапсуляцию для того, чтобы различать кадры, принадлежащие разным VLANам

Членство в VLAN

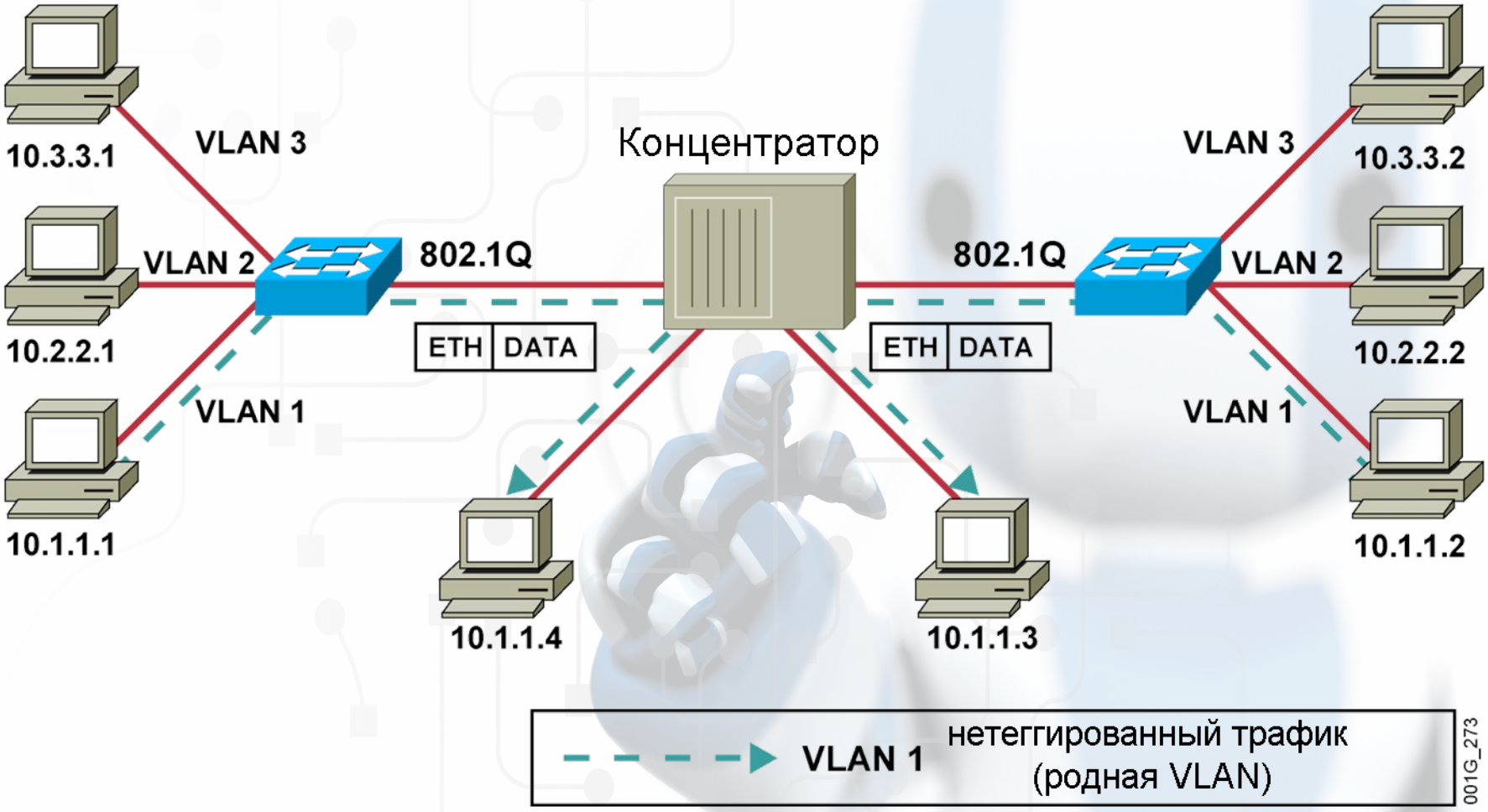


Кадр 802.1Q

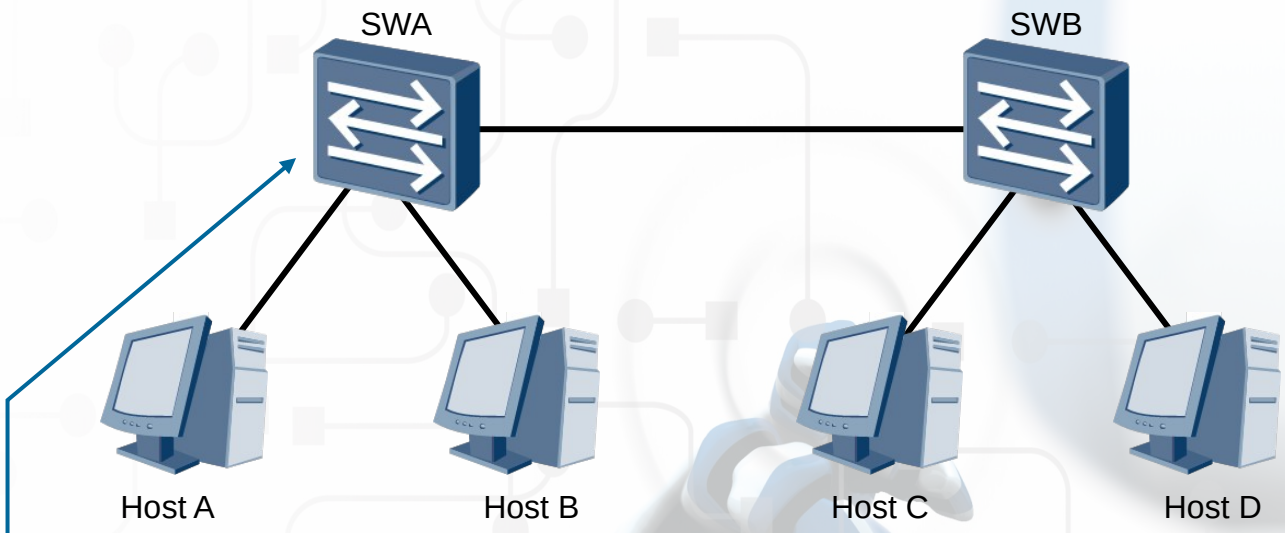


ICND20GR_274

Родные VLANы



Создание VLAN



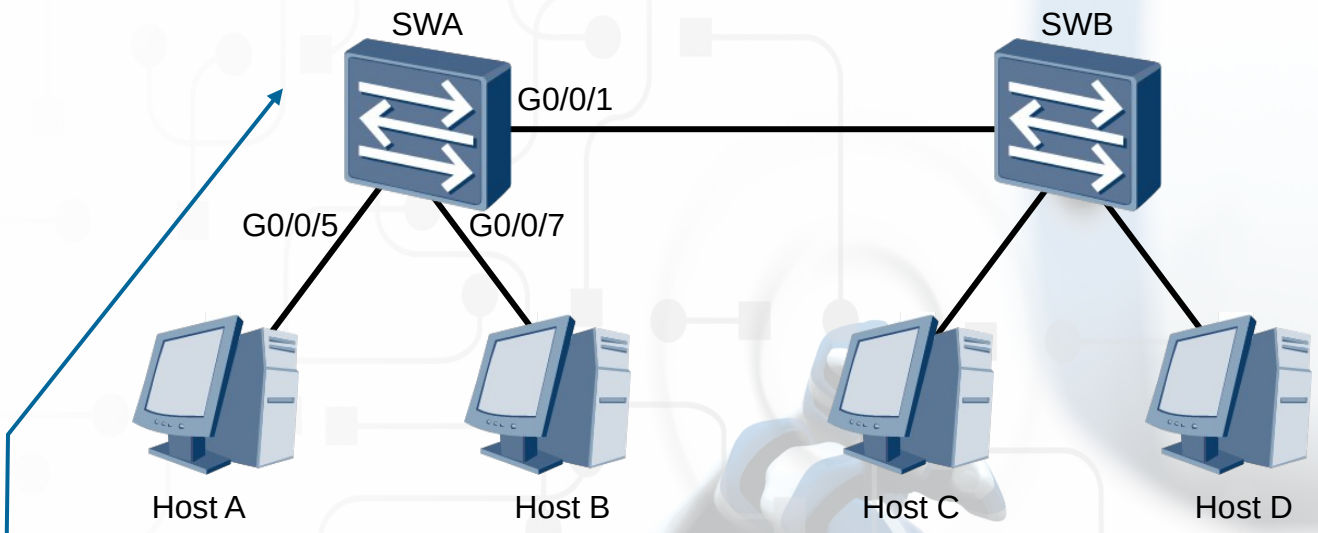

```
[SWA]vlan 10
[SWA-vlan10]quit
[SWA]vlan batch 2 to 3
Info: This operation may take a few seconds. Please wait for a
moment...done.
```

- VLAN 1 есть по умолчанию

Вывод информации о VLAN

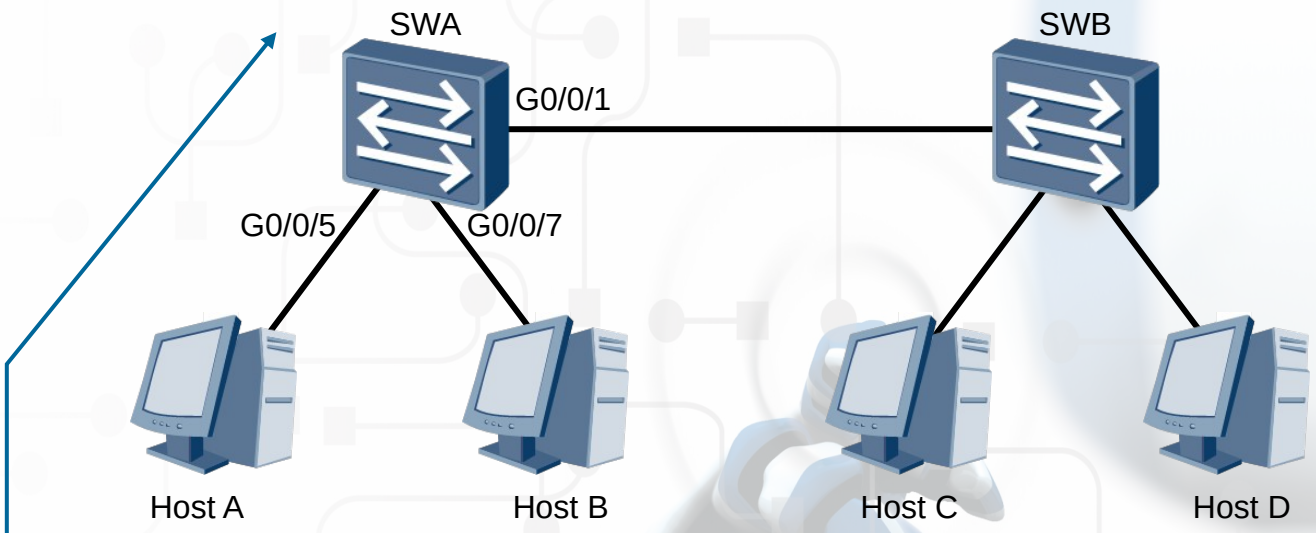
```
[SWA]display vlan
The total number of vlans is : 4
--------------------------------------------------------------
U:Up; D:Down; TG:Tagged; UT:Untagged; MP:Vlan-mapping;
ST:Vlan-stacking; #: ProtocolTransparent-vlan; *:Management-
vlan;
--------------------------------------------------------------
VID  Type    Ports
--------------------------------------------------------------
1    common  UT:GE0/0/1(U) ……
2    common
3    common
10   common
……
```

Настройка типа порта




```
[SWA]interface GigabitEthernet 0/0/1
[SWA-GigabitEthernet0/0/1]port link-type trunk
[SWA-GigabitEthernet0/0/1]quit
[SWA]interface GigabitEthernet 0/0/5
[SWA-GigabitEthernet0/0/5]port link-type access
```

Добавление порта в VLAN

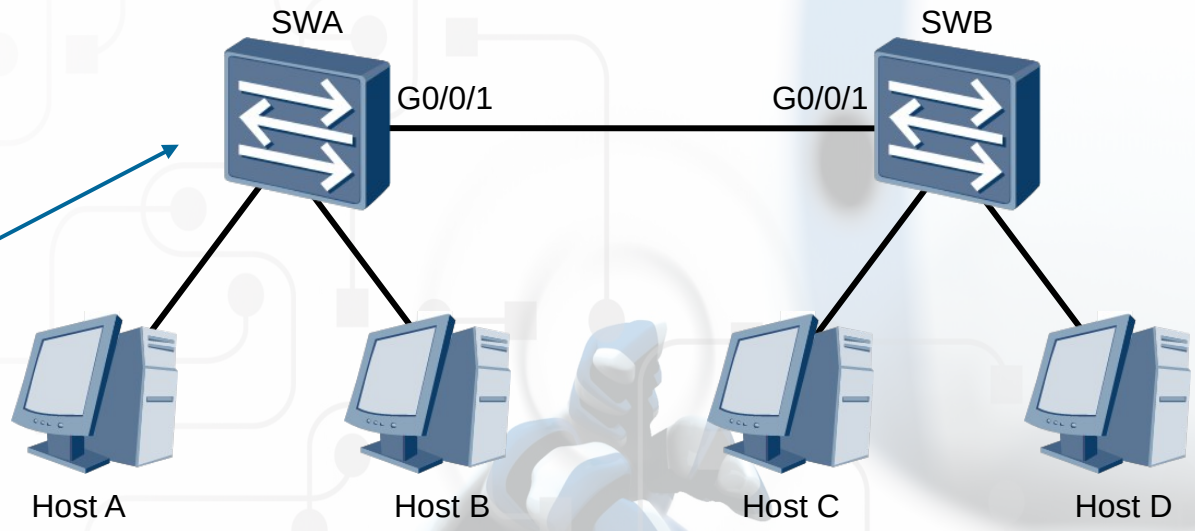



```
[SWA]vlan 2
[SWA-vlan2]port GigabitEthernet 0/0/7
[SWA-vlan2]quit
[SWA]interface GigabitEthernet 0/0/5
[SWA-GigabitEthernet0/0/5]port link-type access
[SWA-GigabitEthernet0/0/5]port default vlan 3
```

Просмотр членства портов в VLANax

```
[SWA]display vlan
The total number of vlans is : 4
--------------------------------------------------------------
U:Up; D:Down; TG:Tagged; UT:Untagged; MP:Vlan-mapping;
ST:Vlan-stacking; #: ProtocolTransparent-vlan; *:Management-
vlan;
--------------------------------------------------------------
VID  Type    Ports
--------------------------------------------------------------
1    common  UT:GE0/0/1(U) ……
2    common  UT:GE0/0/7(D)
3    common  UT:GE0/0/5(U)
10   common
……
```

Настройка транкового порта




```
[SWA-GigabitEthernet0/0/1]port link-type trunk
[SWA-GigabitEthernet0/0/1]port trunk pvid vlan 10
[SWA-GigabitEthernet0/0/1]port trunk allow-pass vlan 2 3
```

Контроль настройки транкового порта

```
[SWA]display vlan
The total number of vlans is : 4
--------------------------------------------------------------
U:Up; D:Down; TG:Tagged; UT:Untagged; MP:Vlan-mapping;
ST:Vlan-stacking; #: ProtocolTransparent-vlan; *:Management-
vlan;
--------------------------------------------------------------
VID  Type    Ports
--------------------------------------------------------------
1    common  UT:GE0/0/1(U) ……
2    common  UT:GE0/0/7(D) TG:GE0/0/1(U)
3    common  UT:GE0/0/5(U) TG:GE0/0/1(U)
10   common
……
```

Функции маршрутизаторов

```
[Huawei]display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 2        Routes : 2

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        127.0.0.0/8      Direct  0    0           D   127.0.0.1       InLoopBack0
        127.0.0.1/32     Direct  0    0           D   127.0.0.1       InLoopBack0
```

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

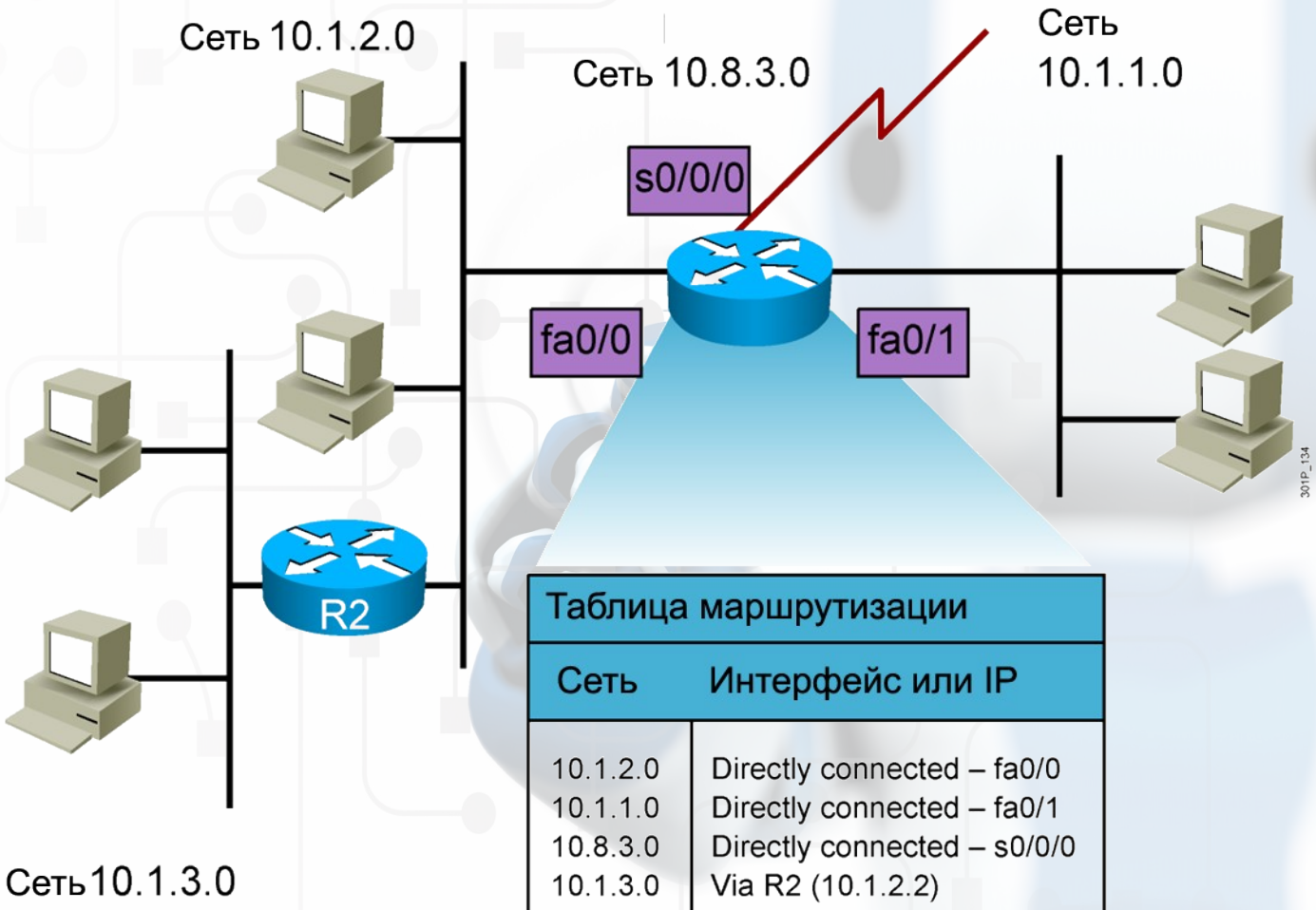
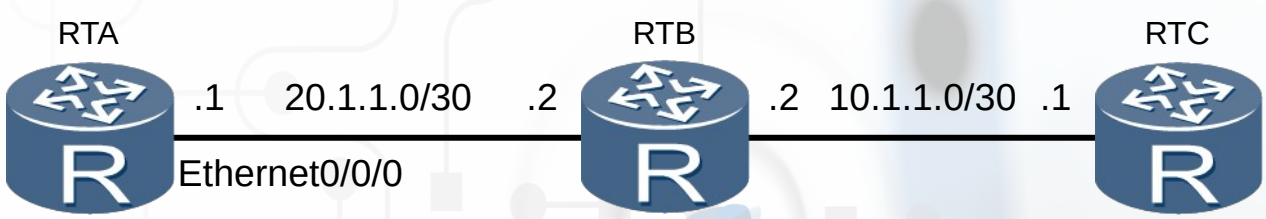


Таблица маршрутизации	
Сеть	**Интерфейс или IP**
10.1.2.0	Directly connected – fa0/0
10.1.1.0	Directly connected – fa0/1
10.8.3.0	Directly connected – s0/0/0
10.1.3.0	Via R2 (10.1.2.2)

Записи в таблице маршрутизации

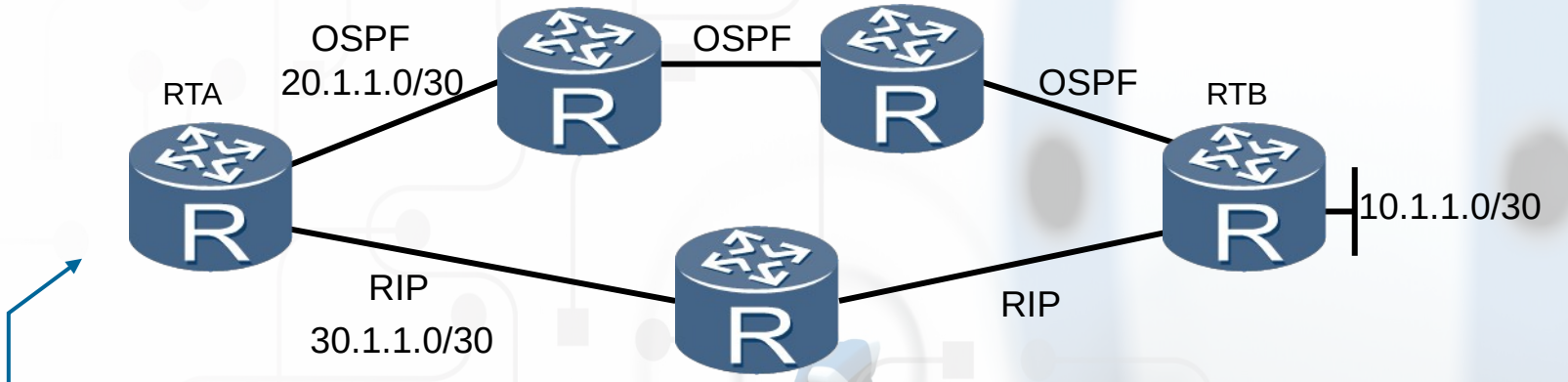
- Подключенные сети: сети, адреса из которых настроены на интерфейсах маршрутизатора
- Статические маршруты – маршруты, заданные администратором
- Динамические маршруты – маршруты, вычисленные устройством в результате обмена маршрутной информацией по одному из протоколов маршрутизации
- Маршрут по умолчанию: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

Выбор маршрута - самое длинное совпадение




```
[RTA]display ip routing-table
Destination/Mask   Proto   Pre  Cost      Flags NextHop         Interface
10.1.1.0/24        Static  60   0           RD  20.1.1.2        Ethernet0/0/0
10.1.1.0/30        Static  60   0           RD  20.1.1.2        Ethernet0/0/0
```

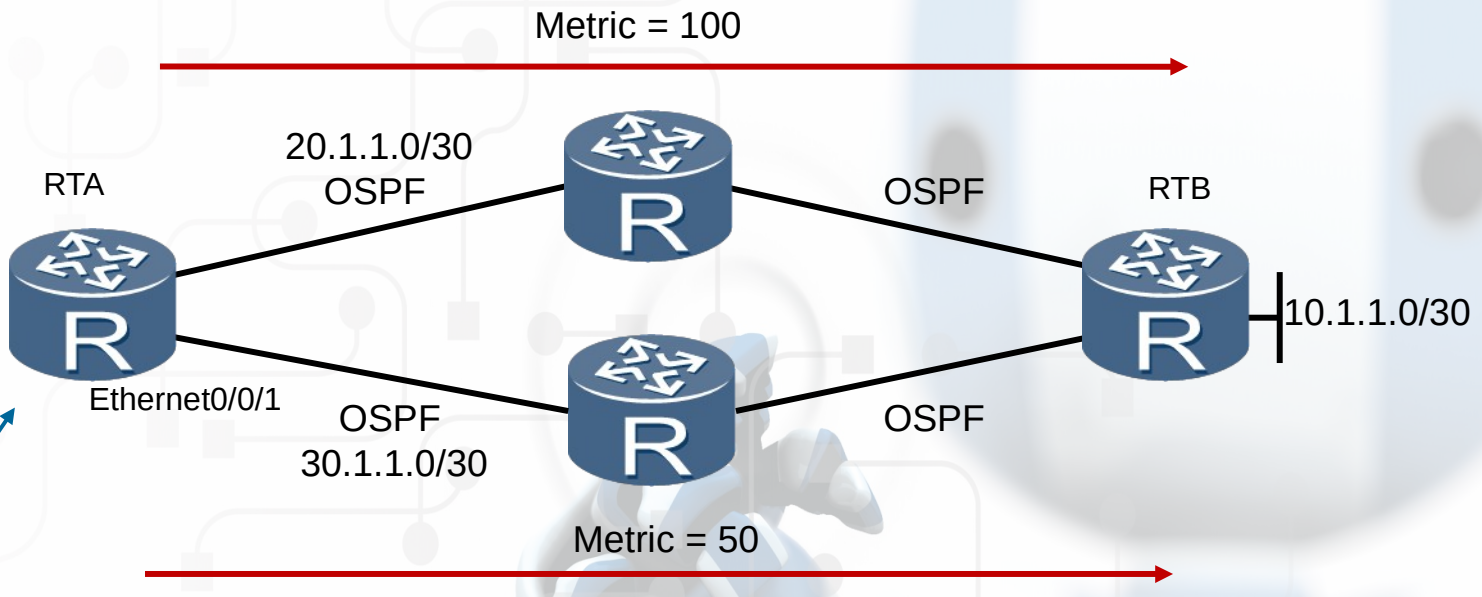
Выбор маршрута - предпочтение




```
[RTA]display ip routing-table
Destination/Mask   Proto   Pre  Cost      Flags NextHop         Interface
10.1.1.0/30        OSPF    10   60        RD    20.1.1.2        Ethernet0/0/0
......
```

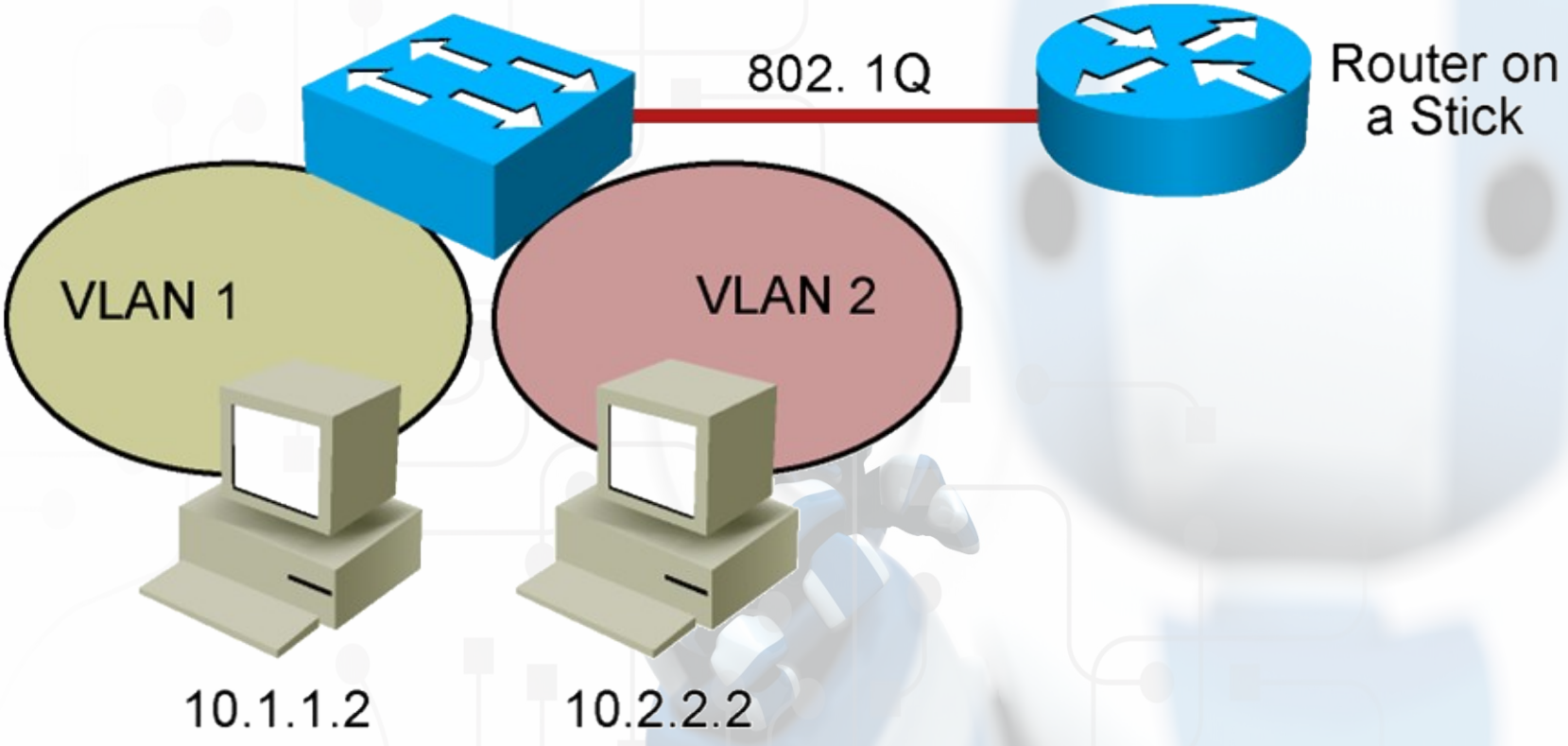
Route	Direct	OSPF	Static	RIP
Preference	0	10	60	100

Выбор маршрута - метрика



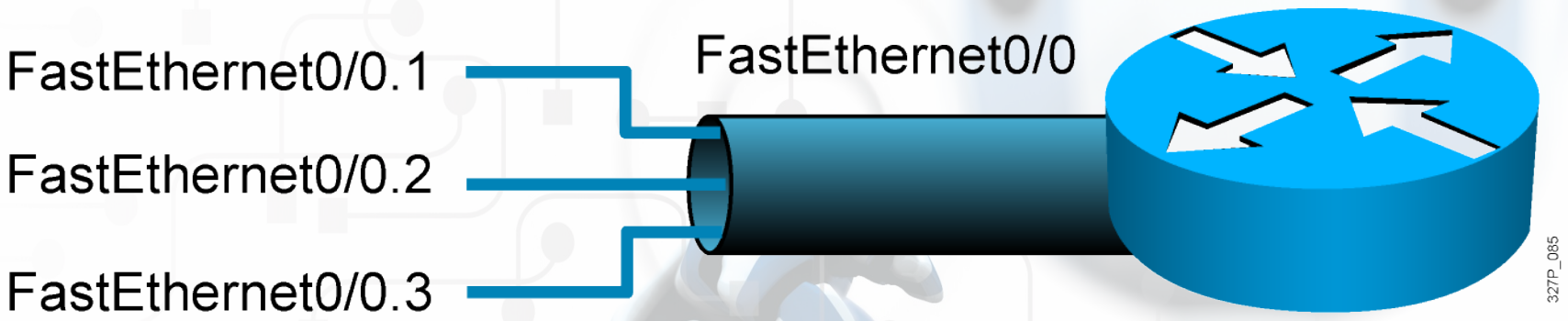

```
[RTA]display ip routing-table
Destination/Mask  Proto   Pre  Cost      Flags NextHop         Interface
10.1.1.0/30       OSPF    10   50        RD    30.1.1.2        Ethernet0/0/1
```

Маршрутизация между VLAN’ами



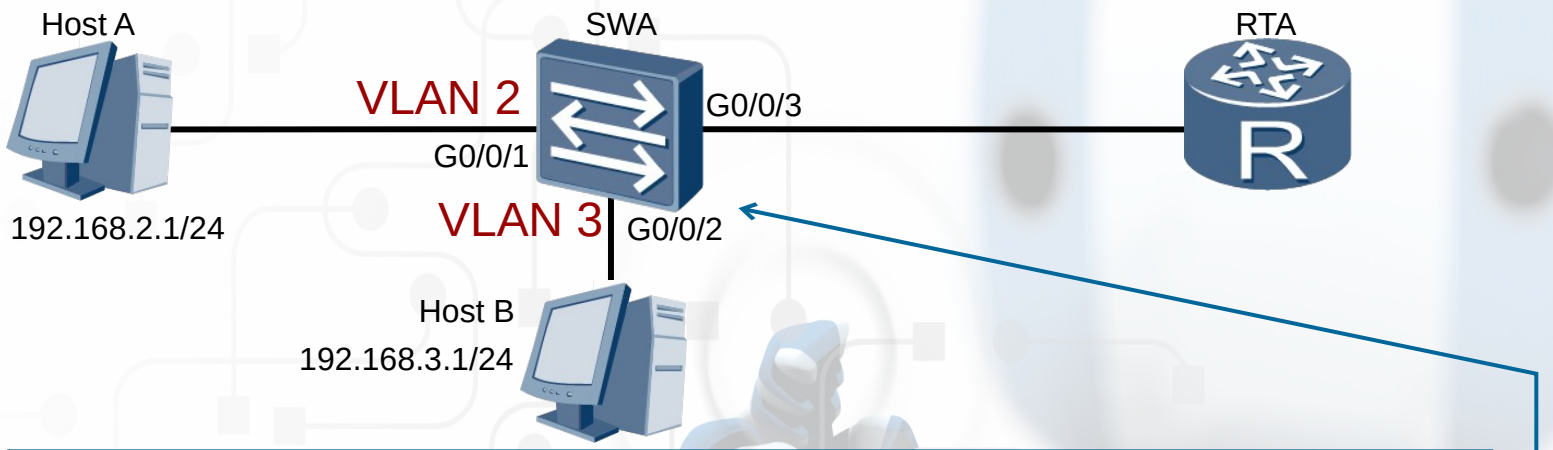
- Для пересылки данных между вещательными доменами необходим маршрутизатор

Создание логических подинтерфейсов на основе одного физического



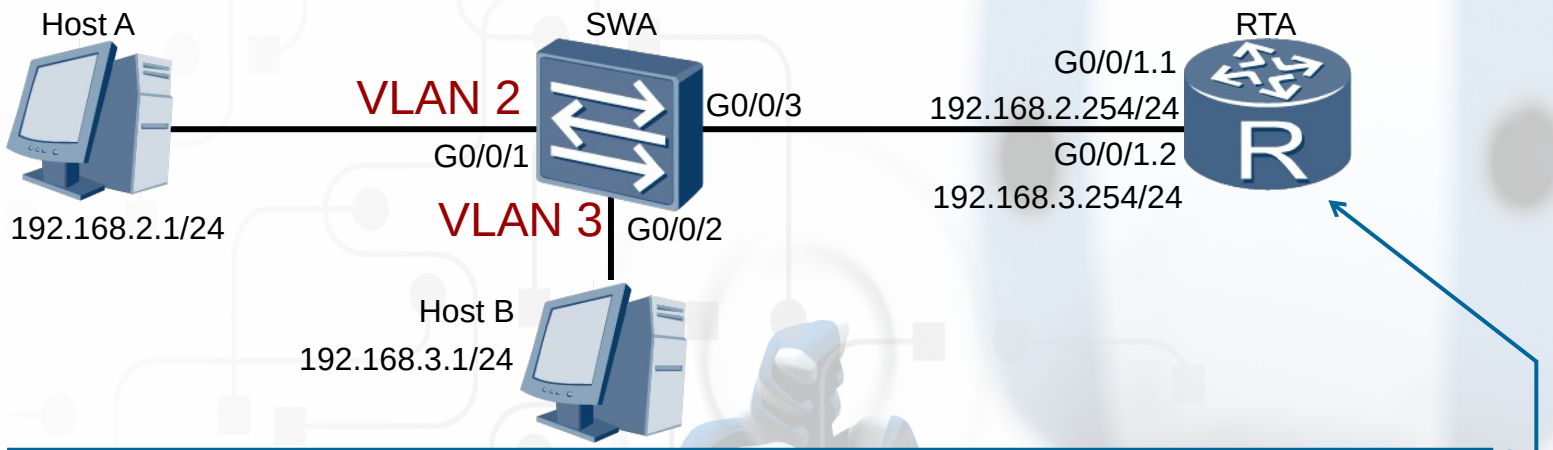
- Для каждого вещательного домена, подключенного к маршрутизатору через транк, нужно создать свой логический подинтерфейс

Реализация «router-on-a-stick»




```
[SWA]vlan batch 2 3
[SWA-GigabitEthernet0/0/1]port link-type access
[SWA-GigabitEthernet0/0/1]port default vlan 2
[SWA-GigabitEthernet0/0/2]port link-type access
[SWA-GigabitEthernet0/0/2]port default vlan 3
[SWA-GigabitEthernet0/0/3]port link-type trunk
[SWA-GigabitEthernet0/0/3]port trunk allow-pass vlan all
```

Реализация «router-on-a-stick»




```
[RTA]interface GigabitEthernet0/0/1.1
[RTA-GigabitEthernet0/0/1.1]dot1q termination vid 2
[RTA-GigabitEthernet0/0/1.1]ip address 192.168.2.254 24
[RTA-GigabitEthernet0/0/1.1]arp broadcast enable
[RTA]interface GigabitEthernet0/0/1.2
[RTA-GigabitEthernet0/0/1.2]dot1q termination vid 3
[RTA-GigabitEthernet0/0/1.2]ip address 192.168.3.254 24
[RTA-GigabitEthernet0/0/1.2]arp broadcast enable
```

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?