

Тема 2.2. Обеспечение информационной безопасности на сетевом уровне

Лекция 4. Технология виртуализации уровня управления
телекоммуникационного оборудования

Дисциплина: Анализ информационных
потребностей подразделений информационно-
аналитического мониторинга

Доцент: Кирьянов Александр
Владимирович
email:kiryanov_a@mirea.ru

Учебные вопросы:

1. Назначение и основные возможности технологии виртуализации в коммуникационном оборудовании.
2. Порядок настройки технологии виртуализации.
3. Настройка VRF в коммуникационном оборудовании.

Возможности виртуализации в СКП:

- не изменяя физической связности, создавать различные логические топологии;
- в каждой виртуальной сети реализация независимых политик адресации, коммутации, маршрутизации;
- увеличение количества логических маршрутизаторов, а соответственно и расширение возможности для построения сложных топологий;
- создание для определенных приложений выделенную логическую топологию;
- использовании виртуальной сети вместе с виртуальными машинами - законченное полноценно виртуальное пространство;

Для виртуальных сетей необходимы виртуальные каналы связи и виртуальные маршрутизаторы.

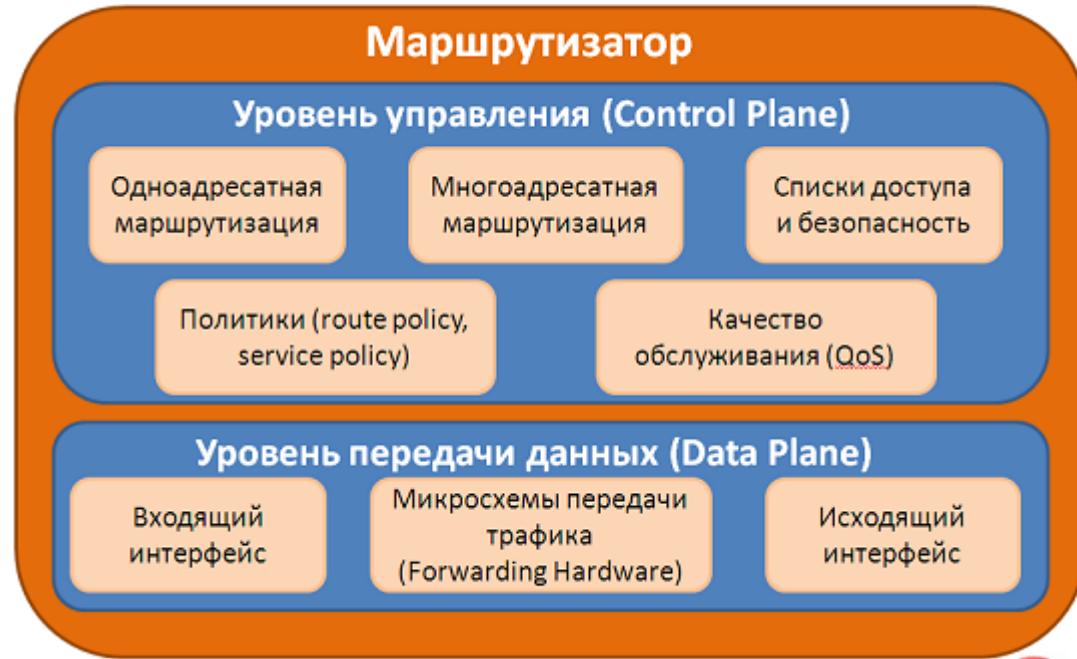
Виртуализация канального уровня— организуется на основе VLAN.

Виртуализация маршрутизаторов на основе VRF (Virtual Routing and Forwarding).

Cisco активно позиционируют его как инструмент MPLS VPN, однако возможности его гораздо шире и не менее известны.

Технология VRF (Virtual Routing and Forwarding) - механизм создания виртуальных маршрутизаторов на базе одного физического устройства. Достигается полная независимость таблиц адресации, коммутации, маршрутизации, настроек разных виртуальных устройств.

Логическое устройство маршрутизатора



Маршрутизатор делят на два уровня (plane): уровень передачи данных (data plane); уровень управления (control plane).

Уровень управления – это фактически “мозг” маршрутизатора, так как он отвечает за построение одноадресной (unicast) и многоадресной (multicast) таблиц маршрутизации, применение различных политик (маршрутных, сервисных и т.д.) и механизмов безопасности.

Все протоколы маршрутизации, резервирования шлюза, построения беспетлевой топологии на канальном уровне (STP и его модификации) функционируют на уровне управления.

Также уровню управления принадлежат логические интерфейсы маршрутизатора (настройку интерфейса в IOS (IP-адрес, инкапсуляция, VLAN, подинтерфейсы)).

Уровень передачи данных отвечает непосредственно за прием/передачу трафика, никакие решения о том, куда и как передавать трафик в общем случае здесь не принимаются, предоставляя эту функцию уровню управления.

В отдельных случаях на уровне передачи данных могут приниматься такие решения.

Применение механизма CEF (Cisco Express Forwarding).

Работа CEF заключается в том, что информация **таблиц маршрутизации и списков доступа** записывается в специальную микросхему, которая относится к микросхемам передачи трафика (**Forwarding Hardware**), тем самым значительно ускоряя процесс передачи трафика в сети.

Таким образом, таблица CEF относится к уровню передачи данных, однако для каждого виртуального маршрутизатора таблица CEF - своя.

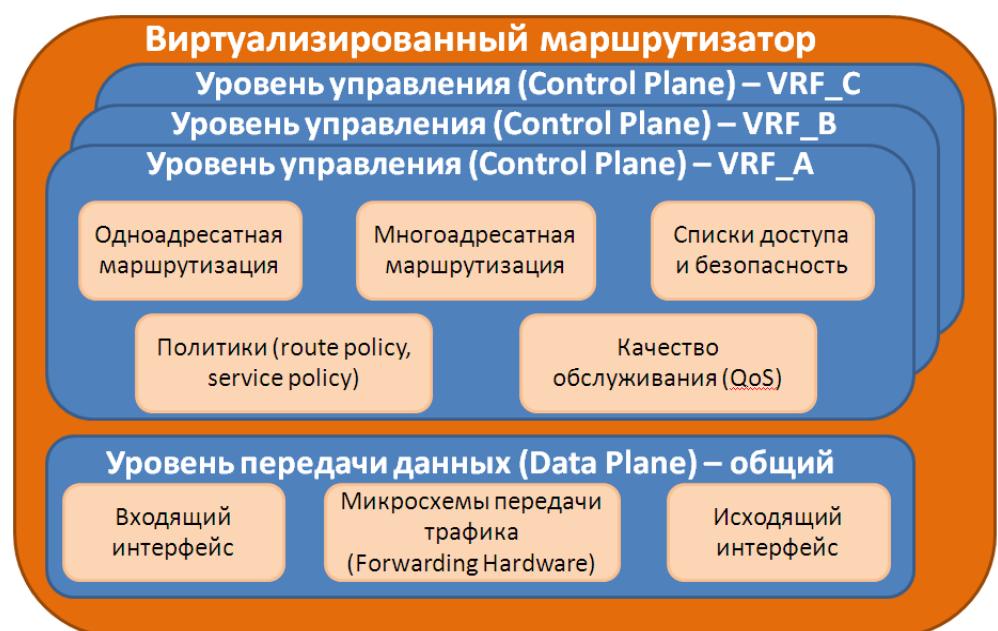
Просмотреть таблицу CEF: «**show ip cef vrf name**», где name – это название виртуального маршрутизатора.

С точки зрения логики работы виртуальный маршрутизатор не ничем не отличается от физического маршрутизатора.

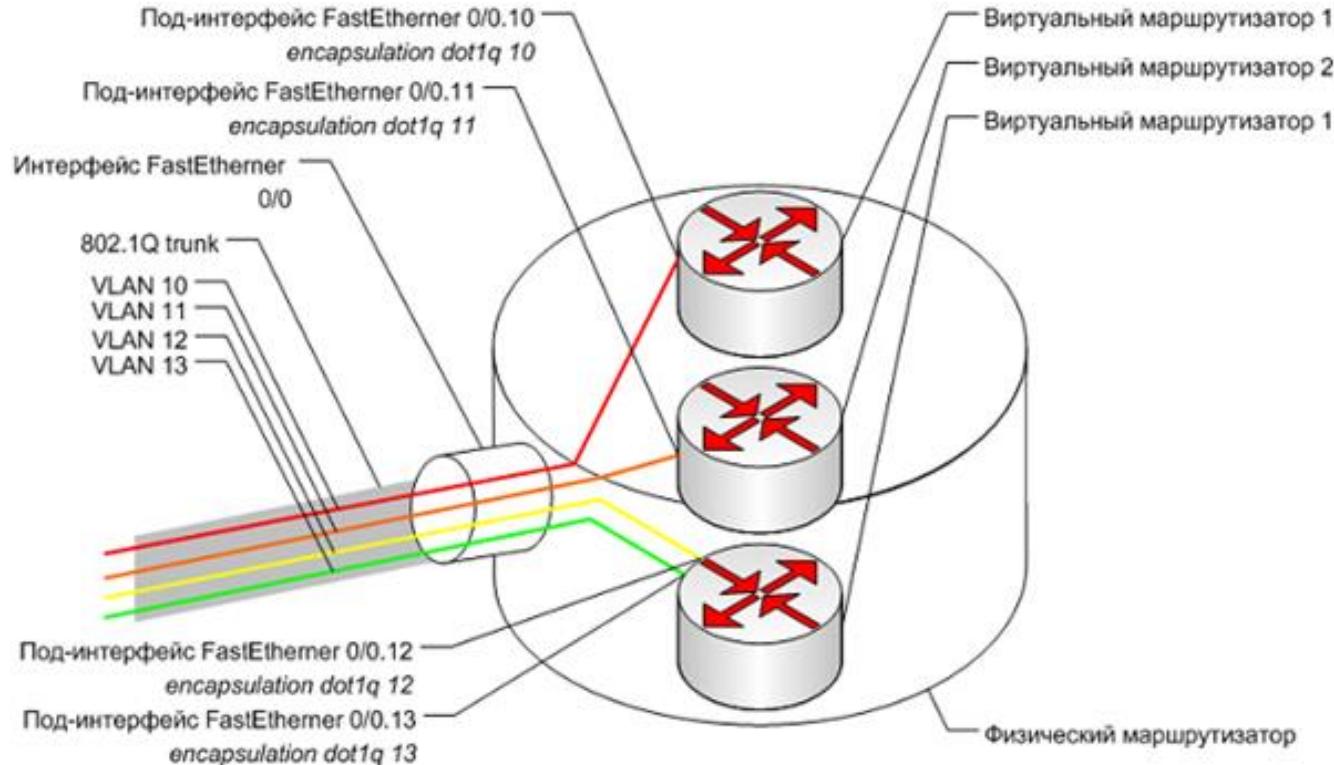
Поэтому виртуализированный представить следующим образом:

Виртуальный маршрутизатор - это независимая копия уровня управления.

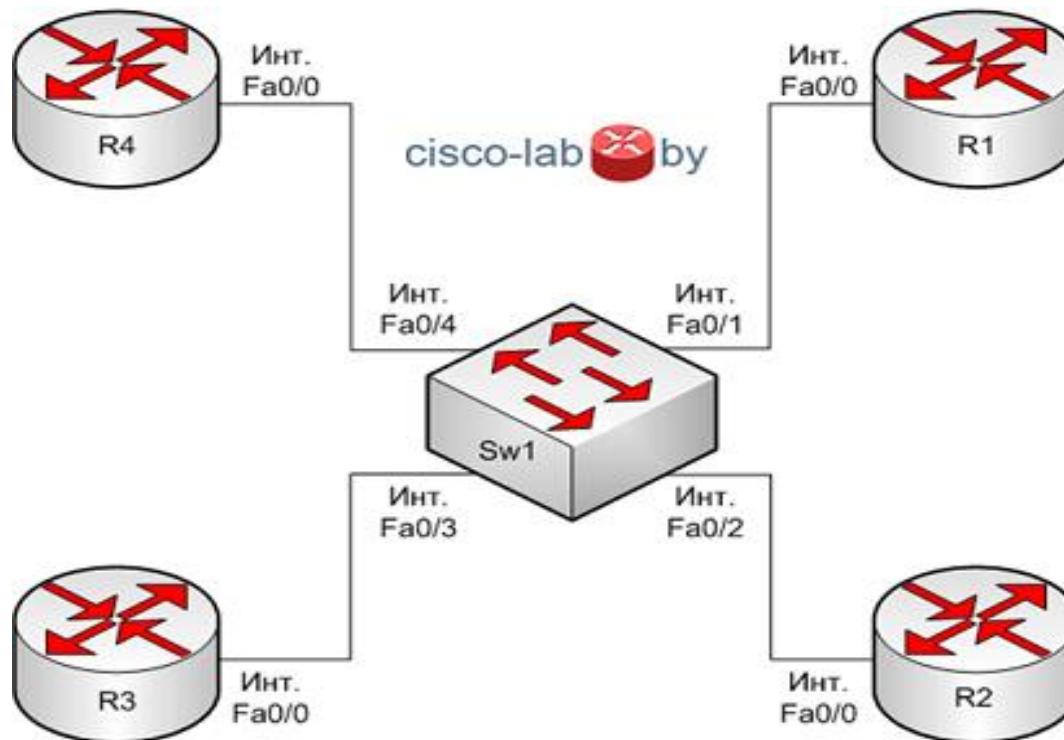
физический маршрутизатор можно



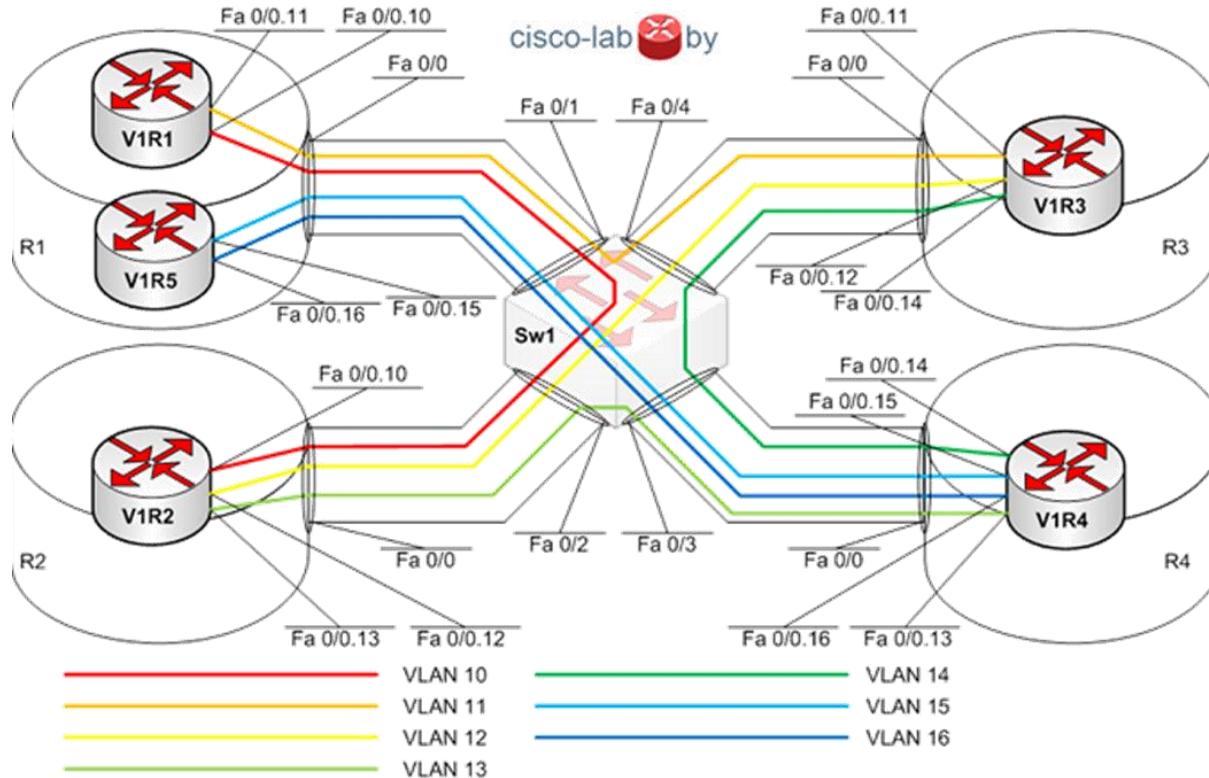
Связь виртуальных и физических интерфейсов маршрутизаторов



Различия физических и виртуальных топологий



Различия физических и виртуальных топологий



Выводы по первому вопросу:

В ходе отработки первого вопроса получены знания о следующих особенностях реализации технологии VRF:

- назначение и основные возможности технологии виртуализации vrf;
- виртуализация адресного пространства;
- виртуализация таблиц маршрутизации;

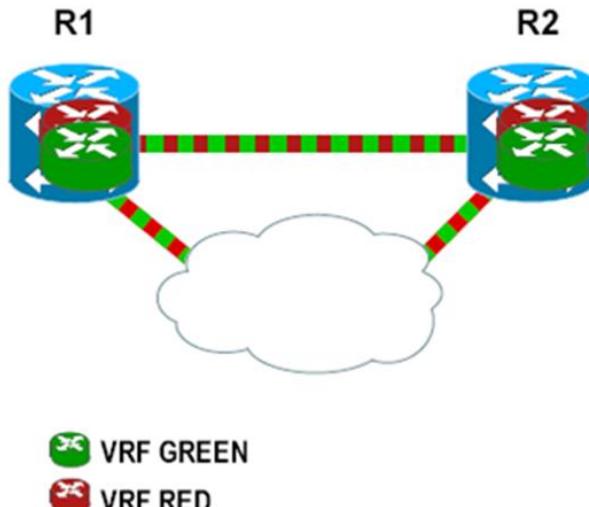
Технология виртуализации широко применяется в коммуникационном оборудовании и современных технологиях(MPLS) в ТСКП, RSNET.

Технология VRF-lite

Каждый маршрутизатор разбит на контексты
Для связи контекстов используются:

Транки dot1Q;

Логические каналы (FR/ATM PVC, SVC)



```
!
ip vrf VRF_GREEN
rd 65000:1
!
ip vrf VRF_RED
rd 65001:1

interface FastEthernet0/0.12
encapsulation dot1Q 12
ip vrf forwarding VRF_GREEN
ip address 10.1.3.1 255.255.255.0
!
interface FastEthernet0/0.112
encapsulation dot1Q 112
ip vrf forwarding VRF_RED
ip address 100.1.3.1 255.255.255.0
!
interface Serial12/0
no ip address
encapsulation frame-relay
serial restart-delay 0
frame-relay intf-type dte
!
interface Serial12/0.12 point-to-point
ip vrf forwarding VRF_GREEN
ip address 10.1.7.1 255.255.255.0
frame-relay interface-dlci 12
!
interface Serial12/0.12 point-to-point
ip vrf forwarding VRF_RED
ip address 100.1.7.1 255.255.255.0
frame-relay interface-dlci 112
!
```

Технология VRF-lite

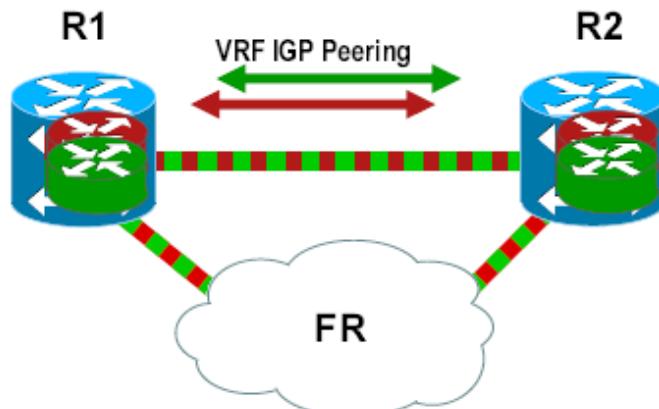
Соседние маршрутизаторы связаны протоколом маршрутизации

Каждый контекст имеет свой процесс маршрутизации

OSPF – отдельный процесс;

EIGRP, RIP – выделенная address family;

Каждый контекст связан с аналогичным контекстом соседа

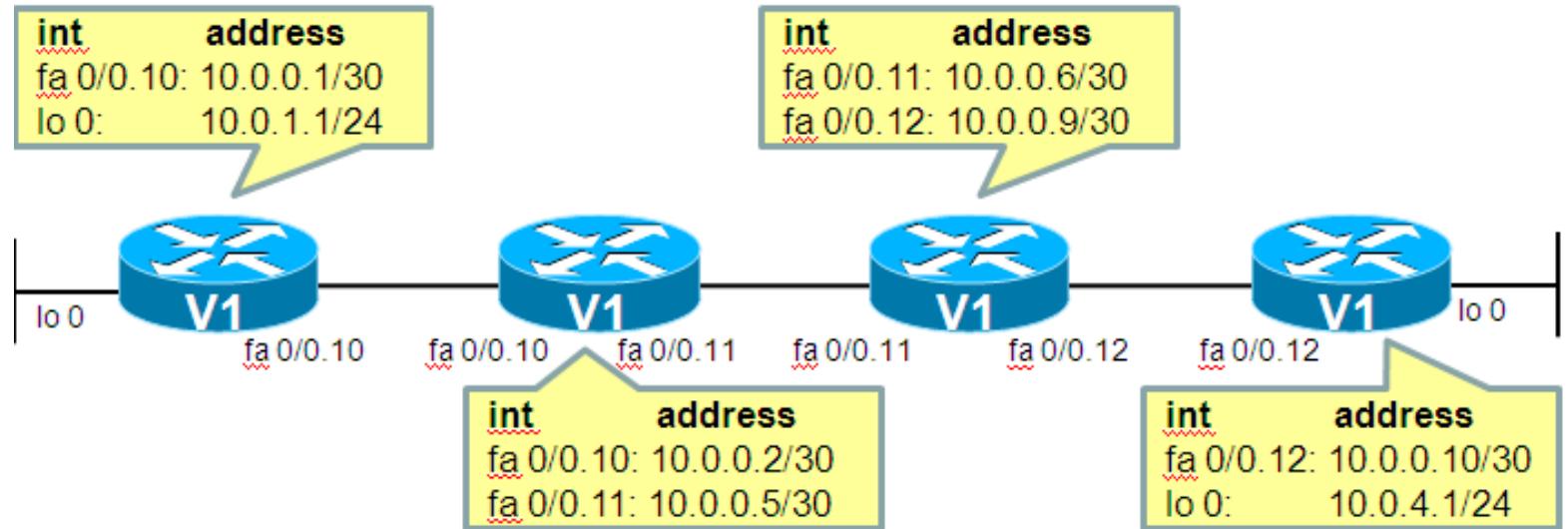


```
!
router ospf 10 vrf VRF_GREEN
log-adjacency-changes
network 10.1.3.0 0.0.0.255 area 0
network 10.1.7.0 0.0.0.255 area 0
!
router eigrp 10
auto-summary
!
address-family ipv4 vrf VRF_RED
network 100.1.3.0 0.0.0.255
network 100.1.7.0 0.0.0.255
no auto-summary
autonomous-system 1
exit-address-family
!
```

Виртуальный маршрутизатор, созданный при помощи VRF, обладает своей собственной таблицей маршрутизации, а также интерфейсами. Рассмотрим процесс создания и функционирования виртуальной сети на примере. Физическая топология сети:



Требуемая логическая топология



Создание виртуального маршрутизатора осуществляется командой: **ip vrf <name>**.

Описание (description) не обязательно.

Виртуальному маршрутизатору необходимо присвоить интерфейсы командой: **ip vrf forwarding <name>**.

Отметим, что привязывать интерфейс к виртуальному маршрутизатору необходимо **до того**, как настраивается IP-адрес.

В противном случае адрес удалиться, о чём будет свидетельствовать характерное сообщение в консоли.

В этом случае настройку адреса на интерфейсе необходимо повторить.

Пример настройки маршрутизатора R1. R2 настраивается аналогично:

```
R1#conf t
R1(config)#ip vrf V1
R1(config-vrf)#descr Virtual Router 1
R1(config-vrf)#ip vrf V3
R1(config-vrf)#descr Virtual Router 3
R1(config-vrf)#int fa 0/0.10
R1(config-subif)#enc dot 10
R1(config-subif)#ip vrf forwarding V1
R1(config-subif)#ip address 10.0.0.1
255.255.255.252
R1(config-subif)#int fa 0/0.11
R1(config-subif)#enc dot 11
R1(config-subif)#ip vrf forwarding V3
R1(config-subif)#ip address 10.0.0.6
255.255.255.252
R1(config-subif)#int fa 0/0.12
R1(config-subif)#enc dot 12
R1(config-subif)#ip vrf forwarding V3
R1(config-subif)#ip address 10.0.0.9
255.255.255.252
R1(config-subif)#int fa 0/0
R1(config-if)#no shut
R1(config-if)#int lo 0
R1(config-if)#ip vrf forwarding V1
R1(config-if)#ip address 10.0.1.1 255.255.255.0
```

Просмотр таблиц маршрутизации:

```
R1#show ip vrf
Name                               Default RD      Interfaces
V1                                <not set>     Fa0/0.10
                                     Lo0
V3                                <not set>     Fa0/0.11
                                     Fa0/0.12
```

```
R1#show ip route vrf V1
```

Routing Table: V1

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF ex

i - IS-IS, su - IS-IS summary, L1 - IS-Route Table: V3

ia - IS-IS inter area, * - candidate default, o - ODR, P - periodic downloaded static

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

ia - IS-IS inter area, * - candidate default, U - per-user static route

o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C 10.0.0.0/8 is variably subnetted, 2 subnets

C 10.0.0.0/30 is directly connected, FastEthernet0/0.12

C 10.0.1.0/24 is directly connected, Lo0

Gateway of last resort is not set

10.0.0.0/30 is subnetted, 2 subnets

C 10.0.0.8 is directly connected, FastEthernet0/0.12

C 10.0.0.4 is directly connected, FastEthernet0/0.11

Настройка маршрутизации: статические маршруты

```
R1(config)#ip route vrf V1 10.0.4.0 255.255.255.0 10.0.0.2  
R1(config)#ip route vrf V1 10.0.0.4 255.255.255.252 10.0.0.2  
R1(config)#ip route vrf V1 10.0.0.8 255.255.255.252 10.0.0.2  
R1(config)#ip route vrf V3 10.0.1.0 255.255.255.0 10.0.0.5  
R1(config)#ip route vrf V3 10.0.0.0 255.255.255.252 10.0.0.5  
R1(config)#ip route vrf V3 10.0.4.0 255.255.255.0 10.0.0.10
```

Настройка динамической маршрутизации: OSPF

```
LeftSPRouter(config)# router ospf 2 vrf Client1vrf  
LeftSPRouter(config-router)# network 10.10.10.0 0.0.0.255 area 0  
LeftSPRouter(config-router)# network 1.1.1.0 0.0.0.3 area 0
```

Просмотр работоспособности виртуальных сетей

```
R1#ping vrf V1 10.0.4.1 so lo 0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.4.1, timeout is 2 seconds:
Packet sent with a source address of 10.0.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms
R1#traceroute vrf V1 10.0.4.1
Type escape sequence to abort.
Tracing the route to 10.0.4.1

 1 10.0.0.2 0 msec 0 msec 4 msec
 2 10.0.0.6 0 msec 0 msec 4 msec
 3 10.0.0.10 4 msec 0 msec *
```

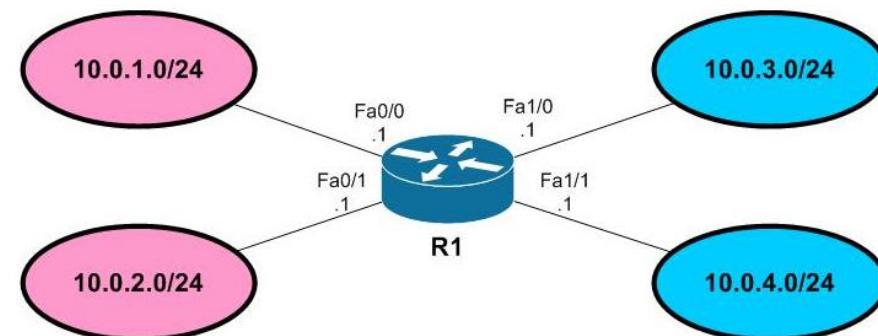
VRF Lite

Технология Virtual Routing and Forwarding (VRF) нашла широкое применение в сетях MPLS. В таких сетях метки MPLS применяются для разграничения трафика различных пользователей, а VRF поддерживает таблицу маршрутизации для каждого из них. Для обмена маршрутной информацией в таких сетях применяется MP-BGP.

Но существует возможность использовать технологию VRF без MPLS — VRF Lite.

VRF Lite

Предположим, к маршрутизатору R1 подключены четыре сети. Необходимо разграничить взаимодействие между сетями так, чтобы первая имела связь со второй, третья с четвертой, но между первой и третьей, первой и четвертой, второй и третьей, второй и четвертой связи не было. Одним из возможных решений будет применение списков доступа (ACL). Второй путь — разделить сети с помощью VRF. Ниже приведена конфигурация, позволяющая это сделать.



Configure VRF Lite

!включаем маршрутизацию

ip routing

!включаем Cisco Express Forwarding, необходимый для работы VRF

ip cef

!объявляем VRF с именем ONE

ip vrf ONE

!указываем route-distinguisher

rd 65000:1

!объявляем VRF с именем TWO и указываем route- distinguisher

ip vrf TWO

rd 65000:2

Configure VRF Lite

interface FastEthernet 0/0

!указываем, что интерфейс
относится к тому или иному VRF

!это необходимо сделать до
указания IP адреса

!так как команда ip vrf forwarding
удаляет адрес с интерфейса

```
ip vrf forwarding ONE
ip address 10.0.1.1 255.255.255.0
no shutdown
```

```
interface FastEthernet 0/1
ip vrf forwarding ONE
ip address 10.0.2.1 255.255.255.0
no shutdown
```

```
interface FastEthernet 1/0
ip vrf forwarding TWO
ip address 10.0.3.1 255.255.255.0
no shutdown
```

```
interface FastEthernet 1/1
ip vrf forwarding TWO
ip address 10.0.4.1 255.255.255.0
no shutdown
```

Configure VRF Lite

Route-distinguisher (RD) — уникальное число, храняющееся рядом с каждым маршрутом в таблице маршрутизации для различения, к какому VRF какой маршрут принадлежит.

RD может быть записан в одном из двух форматов: :<число> или <IP адрес>:<число>, где <число> — десятичное число.

При использовании VRF Lite RD не так важно, как в полноценных сетях MPLS+VRF, потому единственное требование, чтобы его значение было уникальным в рамках одного маршрутизатора.

Настройка динамической маршрутизации: OSPF

```
router ospf 1 vrf ONE
```

```
network 10.0.1.0 0.0.0.255 area 0
```

```
network 10.0.2.0 0.0.0.255 area 0
```

Monitoring VRF Lite

R1#show ip interface brief

Interface IP-Address OK? Method Status Protocol

FastEthernet0/0 10.0.1.1 YES manual up up

FastEthernet0/1 10.0.2.1 YES manual up up

FastEthernet1/0 10.0.3.1 YES manual up up

FastEthernet1/1 10.0.4.1 YES manual up up

R1#show ip vrf

Name	Default RD	Interfaces
------	------------	------------

ONE 65000:1 Fa0/0

Fa0/1

TWO 65000:2 Fa1/0

Fa1/1

Проверка работоспособности VRF

```
R1#ping vrf TWO 10.0.3.1
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.0.3.1, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

```
R1#ping vrf TWO 10.0.4.1
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.0.4.1, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

**Для того, чтобы посмотреть arp таблицу отдельного VRF
используйте команду**

`show ip arp vrf NAME`

где NAME — имя VRF.

Кроме того, чтобы установить telnet подключение из определенного VRF необходимо выполнить следующую команду:

`telnet HOST /vrf NAME`

где HOST — узел, к которому устанавливается подключение, NAME --- имя VRF.

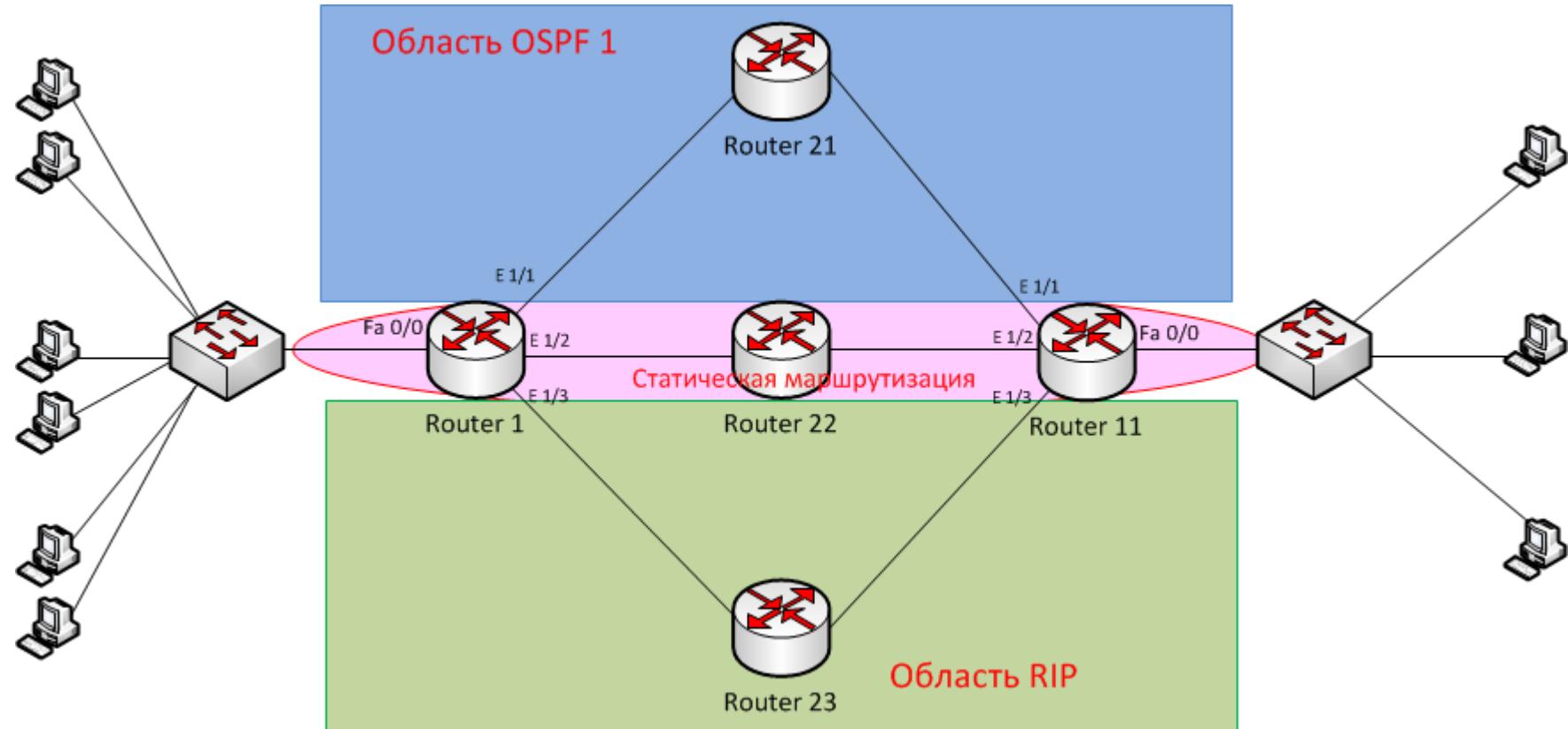
Выводы по второму вопросу:

В ходе отработки первого вопроса занятия следует акцентировать внимание обучаемых на следующих аспектах вопроса:

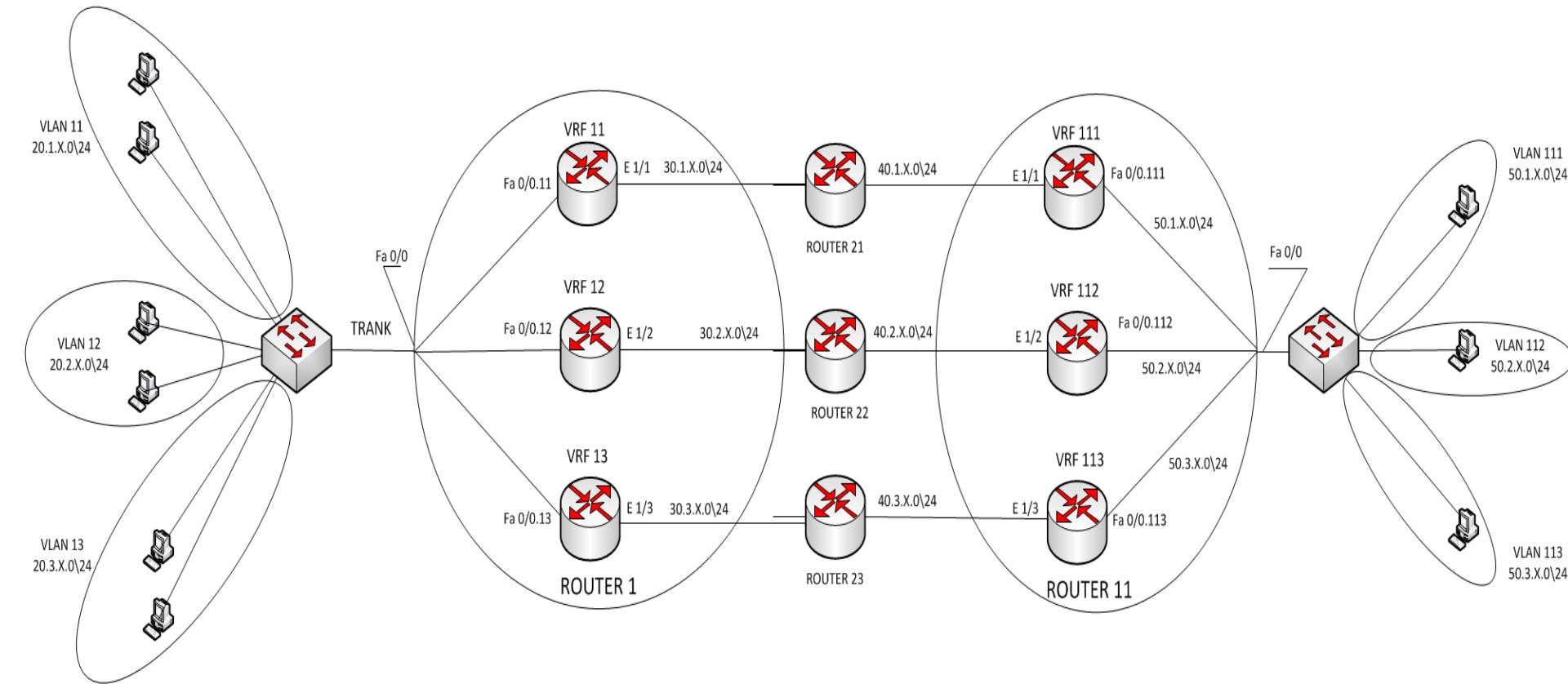
- порядок настройки vrf;
- включение vrf на интерфейсе;
- настройка виртуализации таблиц маршрутизации vrf;

Технология виртуализации широко применяется в коммуникационном оборудовании и современных технологиях(MPLS) в ТСКП в частности.

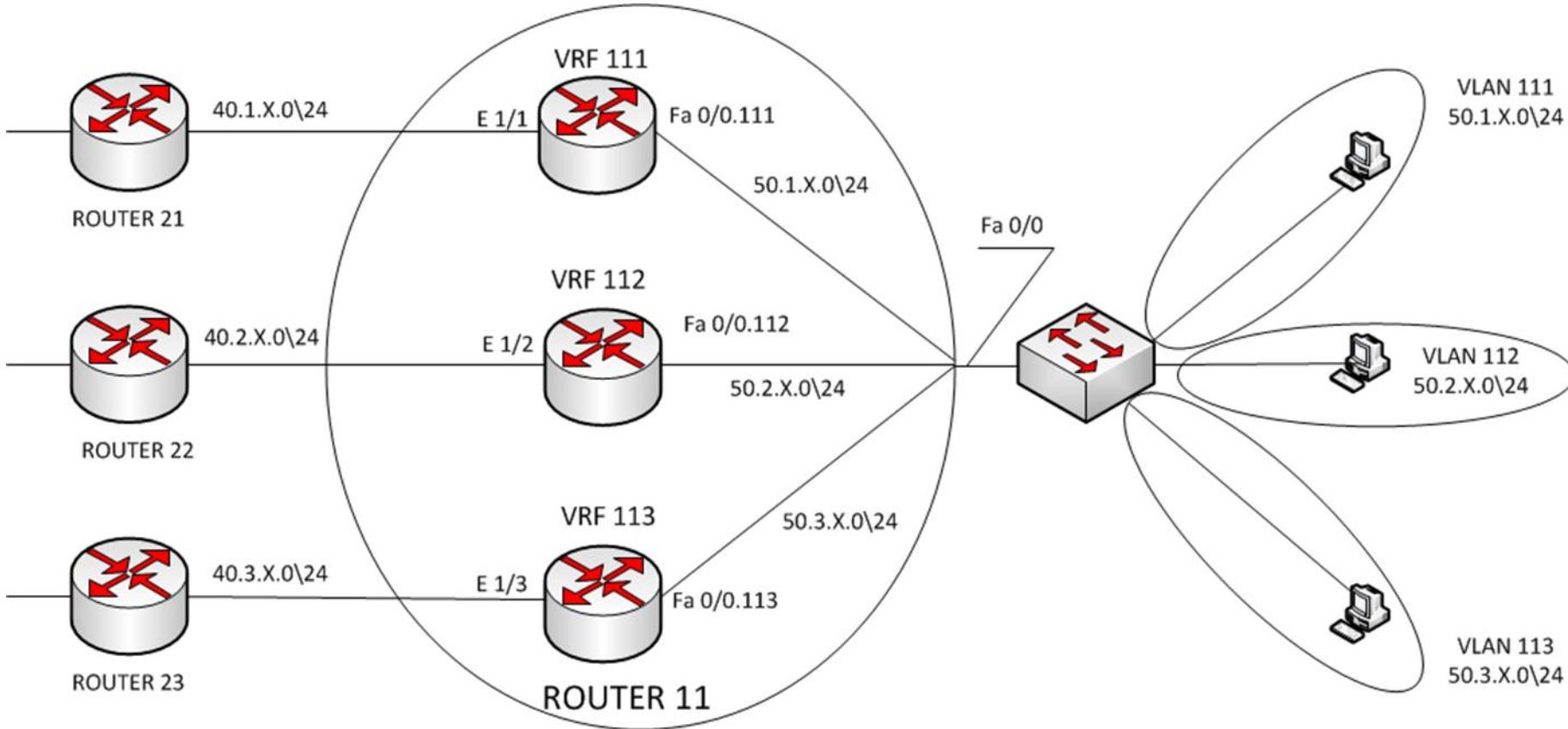
Физическая топология



Логическая топология



Настройка VRF в коммуникационном оборудовании



В ходе практического занятия изучены теоретические положения по реализации технологии виртуализации на коммуникационном оборудовании, порядок настройки коммуникационного оборудования:

настройка интерфейсов для виртуализации;

настройка протокола маршрутизации для виртуализации;

Знания, полученные на этом занятии необходимы обучаемым при отработке заданий учений проводимых на кафедре на 5 году обучения и в повседневной деятельности по предназначению (Эксплуатации МПО (коммуникационного оборудования), ТСКП).

На следующих занятиях будут рассматриваться вопросы фильтрации трафика.

На самостоятельной подготовке необходимо дополнительно изучить основные принципы и параметры настройки vrf в маршрутизаторах.

1. Назначение и основные возможности технологии виртуализации в коммуникационном оборудовании.
2. Порядок настройки технологии виртуализации.
3. Настройка VRF в коммуникационном оборудовании.