ЛАБОРАТОРНАЯ РАБОТА № 13. ИЗУЧЕНИЕ ПРОТОКОЛОВ СТАТИЧЕСКОЙ МАРШРУТИЗАЦИИ **RIP, OSPF** С ИСПОЛЬЗОВАНИЕМ PACKET TRACER.

Цель работы: Изучение принципов динамической маршрутизации IP сетей на примере протоколов динамической маршрутизации RIP и OSPF с использованием программного обеспечения построения виртуальных сетей - Packet Tracer 5.0. Получение практических навыков по настройке маршрутизаторов Cisco 2811-28xx.

1 ОСНОВНЫЕ СВЕДЕНИЯ

Сетевой протокол IP является маршрутизируемым. Для передачи данных от компьютера одной локальной сети к компьютеру другой локальной сети, могут использоваться различные маршруты и маршрутизаторы. В сетях большого масштаба требуется максимально автономная прокладка маршрутов, для чего применяются различные протоколы маршрутизации.

Маршрутизация (routing) – процесс определения маршрута следования информации в сетях связи. Задача маршрутизации состоит в определении последовательности транзитных узлов для передачи пакета от источника до адресата. Определение маршрута следования и продвижение IP-пакетов выполняют специализированные сетевые устройства – **маршрутизаторы**. Каждый маршрутизатор имеет от двух и более сетевых интерфейсов, к которым подключены: 1) локальные сети, либо 2) маршрутизаторы соседних сетей. Выбор маршрута или другими словами интерфейса, маршрутизатор осуществляет на основе таблицы маршрутизации. Таблицы маршрутизации содержат информацию о сетях, и интерфейсов, через которые осуществляется подключение локально (непосредственно), а также содержатся сведения о маршрутах или путях, по которым маршрутизатор связывается с удаленными сетями, не подключенными локально.

Эти маршруты могут назначаться администратором статически или определяться динамически при помощи программного протокола маршрутизации.

Маршрутизатор (router, роутер) – сетевое устройство третьего уровня модели OSI, обладающее как минимум двумя сетевыми интерфейсами, которые находятся в разных сетях. Причем в сетях могут использовать различные технологии физического и канального уровней. Маршрутизатор может иметь интерфейсы: для работы по медному кабелю, оптическому кабелю, так и по беспроводным «линиям» связи.

2 ТАБЛИЦА МАРШРУТИЗАЦИИ

Каждый маршрутизатор принимает решения о направлении пересылки пакетов на основании таблицы маршрутизации. Таблица маршрутизации содержит набор правил – записей, состоящих из определенных полей. Каждое правило содержит следующие основные поля-компоненты:

- адрес IP-сети получателя,
- маску,
- адрес следующего узла, которому следует передавать пакеты,

- административное расстояние — степень доверия к источнику маршрута,
- метрику - некоторый вес - стоимость маршрута,
- интерфейс, через который будут продвигаться данные.

Например:

```
192.168.64.0/16 [110/49] via 192.168.1.2, 00:34:34, FastEthernet0/0.1

где 192.168.64.0/16 – сеть назначения,
    110/- административное расстояние
    /49 – метрика маршрута,
    192.168.1.2 – адрес следующего маршрутизатора, которому следует
                  передавать пакеты для сети 192.168.64.0/16,
    00:34:34 – время, в течение которого был известен этот маршрут,
    FastEthernet0/0.1 – интерфейс маршрутизатора, через который можно
                  достичь «соседа» 192.168.1.2.
```

Таблица маршрутизации может составляться двумя способами:

статическая маршрутизация — когда записи в таблице вводятся и изменяются вручную. Такой способ требует вмешательства администратора каждый раз, когда происходят изменения в топологии сети. С другой стороны, он является наиболее стабильным и требующим минимума аппаратных ресурсов маршрутизатора для обслуживания таблицы.

Динамическая маршрутизация (dynamic routing)— или адаптивная маршрутизация, когда записи в таблице обновляются автоматически при помощи одного или нескольких протоколов маршрутизации — **RIP, OSPF, IGRP, EIGRP, IS-IS, BGP**, и др.. Кроме того, маршрутизатор строит таблицу оптимальных путей к сетям назначения на основе различных критериев: количества промежуточных узлов, пропускной способности каналов, задержки передачи данных. Критерии вычисления оптимальных маршрутов чаще всего зависят от протокола маршрутизации, а также задаются конфигурацией маршрутизатора. Такой способ построения таблицы позволяет автоматически поддерживать таблицу маршрутизации в актуальном состоянии и вычислять оптимальные маршруты на основе текущей топологии сети. Однако динамическая маршрутизация оказывает дополнительную нагрузку на устройства, а высокая нестабильность сети может приводить к ситуациям, когда маршрутизаторы не успевают синхронизировать свои таблицы, что приводит к противоречивым сведениям о топологии сети в различных её частях и потере передаваемых данных.

Зачастую для построения таблиц маршрутизации используют теорию графов.

3 .Специальные термины и понятия.

Метрика –это числовое значение, вырабатываемое каким-либо алгоритмом для каждого маршрута в сети. Обычно, чем меньше метрика, тем маршрут приоритетнее.

Автономная система (Autonomous System — AS) — это группа сетей, которые находятся под единым административным управлением и в которых используются единая стратегия и правила маршрутизации. Автономная система

для внешних сетей представляется как некий единый объект. Её могут поддерживать один или несколько операторов, но чаще один. В соответствии с этой концепцией Интернет выглядит как набор взаимосвязанных автономных систем, каждая из которых состоит из взаимосвязанных сетей. Автономные системы определяют третий, верхний, уровень маршрутизации — маршрут сначала определяется как последовательность автономных систем, затем — как последовательность сетей, а уж затем ведет к конечному узлу.

Административное расстояние (Administrative Distance — AD) - это величина, характеризующая надежность источника информации о маршрутизации. Выражается числом в диапазоне от 0 до 255. Чем больше ее значение, тем менее доверительна полученная информация.

Вид	***Административное расстояние***
Напрямую подключенная сеть (directly connected)	0
Статический маршрут на интерфейс/следующую сеть	1
EIGRP	90
OSPF	110
RIP	120

Таблица 1: Административные расстояние для некоторых видов маршрутизации

Алгоритм выбора кратчайшего маршрута (Shortest Path First— SFT algorithm) — это выполняемые над базой данных вычисления, результатом которых является построение дерева SPF.

Шлюз по умолчанию (default gateway), шлюз последней надежды (last resort gateway) – адрес маршрутизатора, на который отправляется трафик для которого не нашлось отдельных записей в таблице маршрутизации. Для устройств, подключенных к одному маршрутизатору (как правило, это рабочие станции), использование шлюза по умолчанию – единственная форма маршрутизации. Шлюз последней надежды применяется обычно в устройствах (маршрутизаторах), где ситуация, в которой не найдется отдельного маршрута, является исключительной.

4 Протоколы маршрутизации

Протокол маршрутизации — это сетевой протокол, используемый маршрутизаторами для определения возможных маршрутов следования данных в составной компьютерной сети. Применение протокола маршрутизации позволяет избежать ручного ввода всех допустимых маршрутов, что, в свою очередь, снижает количество ошибок, обеспечивает согласованность действий всех маршрутизаторов в сети и облегчает труд администраторов.

Протоколы маршрутизации (их достаточно много), делятся на два класса:

- Протоколы внешнего шлюза (Exterior Gateway Protocol EGP)- □□□ это протоколы маршрутизации, предназначенный для

использования между автономными системами AS, управляемыми различными организациями. ***(под шлюзом имеется ввиду маршрутизатор)***

- Протокол внутреннего шлюза (Interior Gateway Protocol IGP) это протокол маршрутизации, предназначенный для использования в одной AS, управляемой или администрируемой одной организацией.

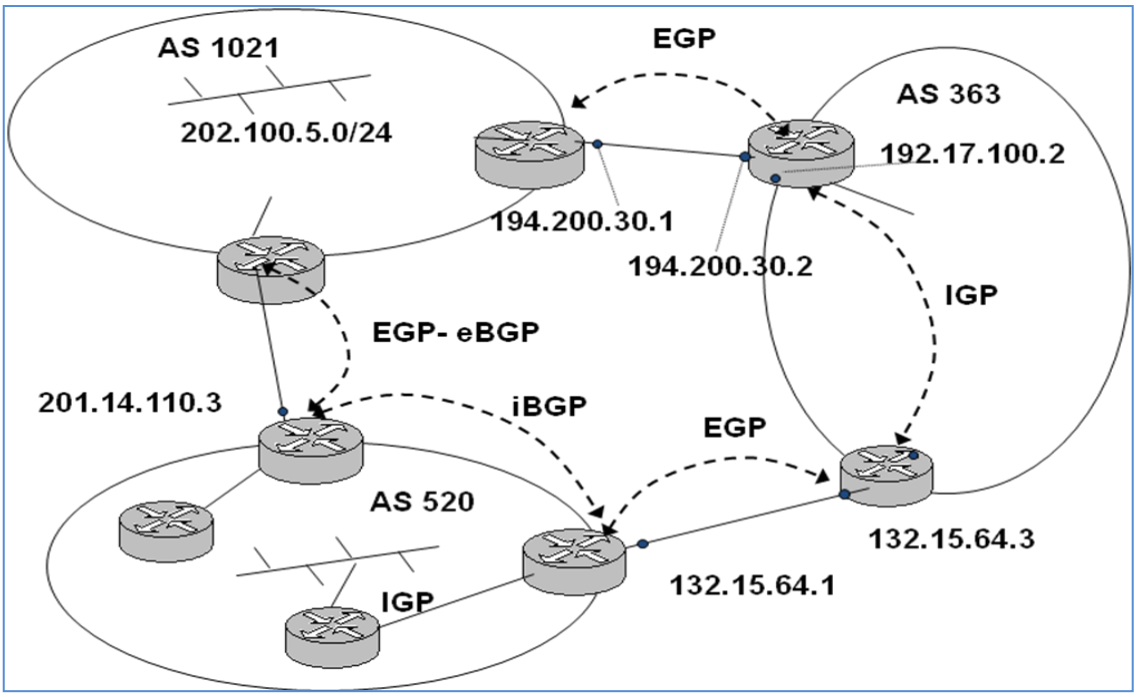

Рис 13.1. Автономные системы Internet.

На Рис 13.1. показаны три автономные системы AS, использующие для обмена информацией между AS протоколы внешнего шлюза EGP, а внутри AS протоколы внутреннего шлюза IGP.

В качестве протокола внешнего шлюза наиболее чаще используются протокол BGP версии v4.

К классу IGP относятся следующие протоколы маршрутизации протоколы:

- RIP и RIP V2;
- IGRP,
- EIGRP,
- OSPF,
- IS-IS.

5 Практическое выполнение задания:

Для выполнения лабораторной работы используется ПО Cisco Packet Tracer.

Запустите программу Cisco Packet Tracer.

5.1 Построение виртуальной сети. Базовая настройка маршрутизаторов и конфигурация устройств сети.

Для построения сети используем ранее созданный файл LP#12-GNN.pkt в лабораторной работе № 12.

5.1.1 Откройте файл LR#12-GNN.pkt с помощью ПО Cisco Packet Tracer и сохраните его как LR#13-GNN.pkt.

5.1.2 В области «Логическое пространство» добавьте ещё три маршрутизатора и обозначьте их как R5-GNN, R6-GNN, R7-GNN. В качестве дополнительных маршрутизаторов выбираем Router-PT-Empty, т.е. маршрутизатор - шасси с пустыми слотами.

5.1.3 Установите модули расширения (установку выполнять при выключенном питании):

5.1.4 На маршрутизаторах R5-GNN,R6-GNN,R7-GNN:

- **PT-ROUTER-NM-1FGE**- гигабитный оптический Ethernet для маршрутизаторов уровня доступа- по одному модулю для **R5, R7** и два для **R6;**
- **PT-ROUTER-NM-1FFE** предоставляет один интерфейс Fast-Ethernet для подключения оптического кабеля, 100BaseFX Ethernet, по одному модулю для **R5, R7** .
- **PT-ROUTER-NM-1CFE**- один интерфейс Fast-Ethernet для подключения медного кабеля по одному модулю для **R5,R6,R7**;
- **PT- ROUTER-NM-1SS- 1-о** портовый синхронный/асинхронный серийный сетевой модуль, один в маршрутизатор R6-GNN **только R6**.

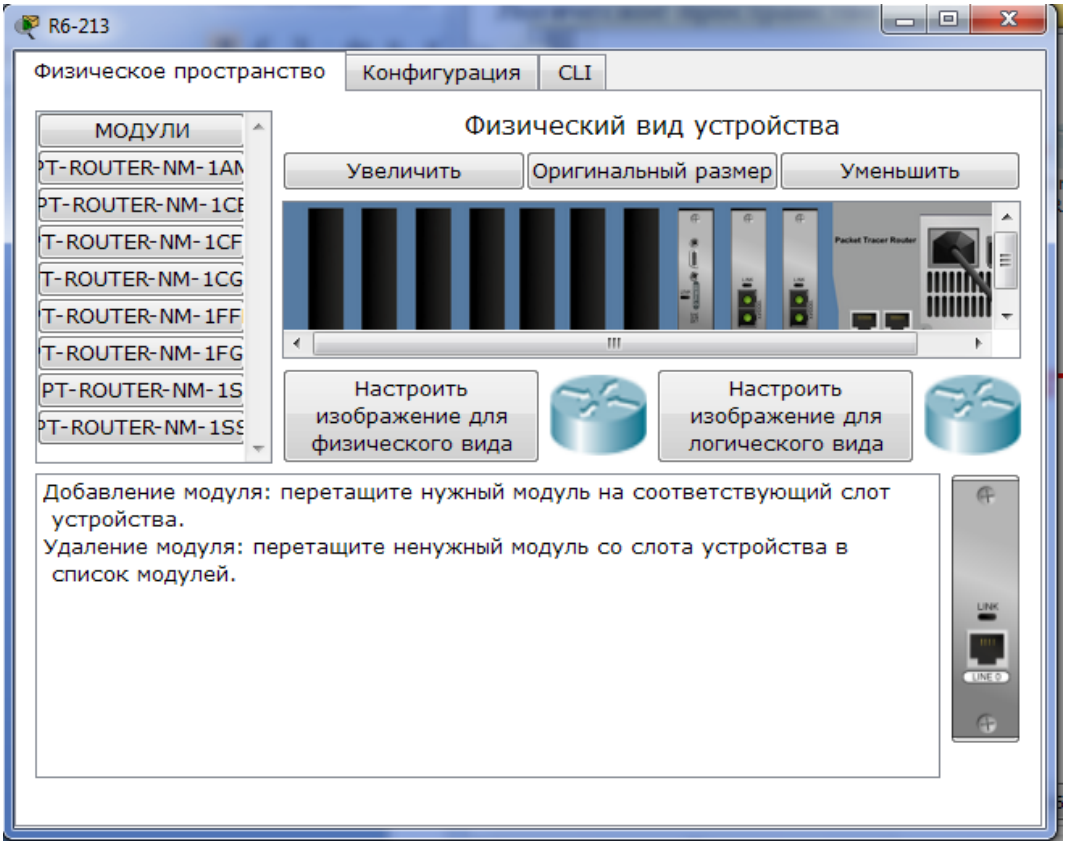

Рис.13.2. Установка модулей расширения в Маршрутизатор R6-GNN.

PT-ROUTER-NM-1FGE- предоставляет гигабитный оптический Ethernet для маршрутизаторов уровня доступа. Поддерживается маршрутизаторами серии Cisco 2691, Cisco 3660, Cisco 3725, и Cisco 3745. Этот модуль содержит один слот гигабитного конвертера интерфейса (GBIC), для использования любого стандартного оптического Cisco GBIC.

На маршрутизаторах R1-GNN, R4-GNN(отключив питание):

- Удалить модуль NM-4A/S, вместо него установить модуль NM-1FE-FX. NM-1FE-FX-предоставляет один интерфейс Fast-Ethernet для подключения ***оптического кабеля***;
- Установить модуль WIC-2T в слот 0/1, как показано на Рис 13.3. **Модуль WIC-2T 2-портовый** синхронный/асинхронный серийный сетевой модуль предоставляет гибкую поддержку многих протоколов с индивидуальной настройкой каждого порта в синхронный или асинхронный режим.
- Включить питание.

На маршрутизаторе R3-GNN (оставляем прежнюю конфигурацию – NM-4A/S):

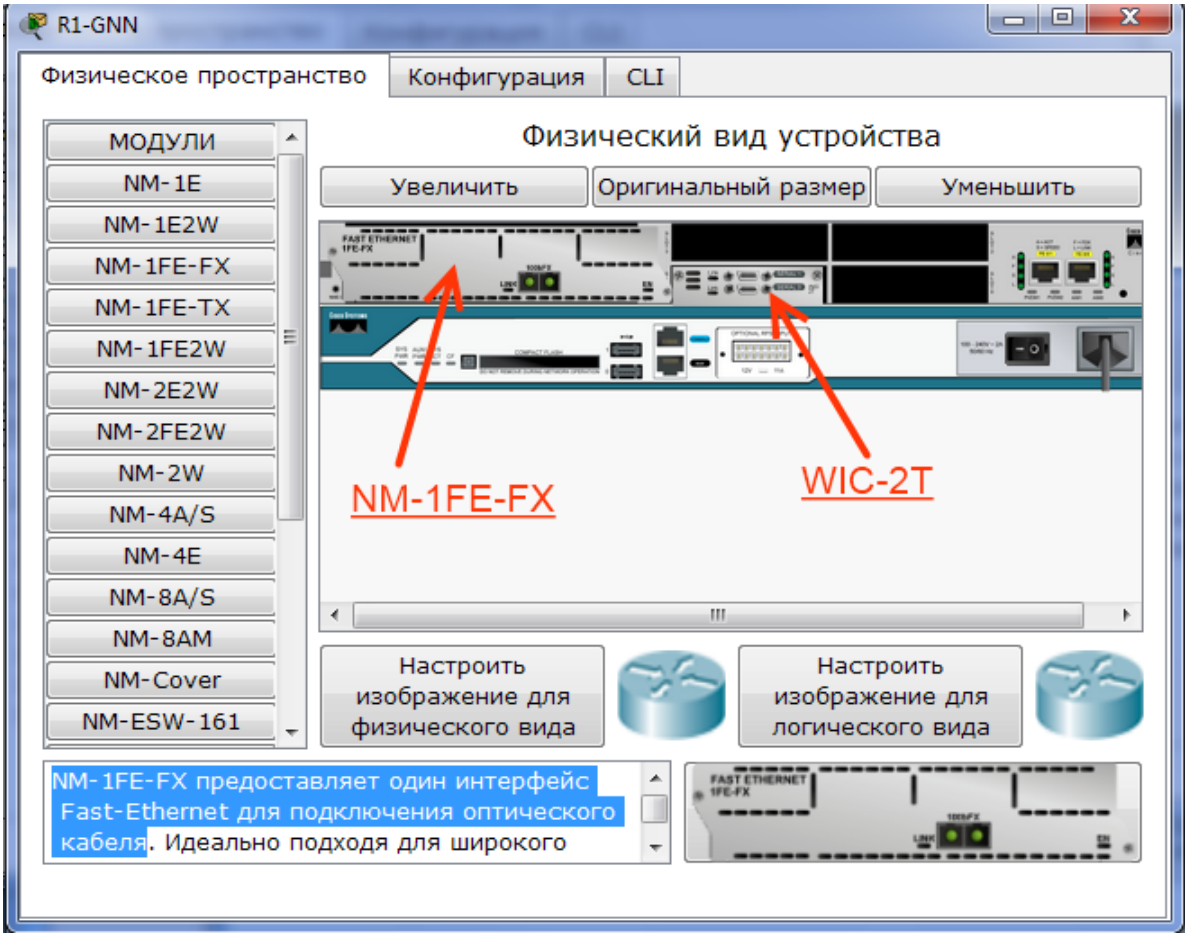

Рис.13.3. Установка модулей NM-1FE-FX и WIC-2T на R1-GNN и R4-GNN

5.1.5 Включаем питание на всех устройствах, добавляем необходимые устройства, чтобы получить топологию сети, изображенную на Рис.13.4.

5.1.6 Соединяем оптическим кабелем маршрутизаторы R1-R5, R4-R7, используя порты- интерфейсы Fast Ethernet. (оптические)

5.1.7 Также оптическим кабелем соединяем маршрутизаторы R5-R6-R7 между собой, используя интерфейсы Gigabit Ethernet.

5.1.8 Низко- скоростной интерфейс Serial Se2/0 Маршрутизатора R6 соединяем с интерфейсом Se1/3 маршрутизатора R3.

В области «Логическое пространство» создайте многоконтурную сеть аналогичную на данном ScreenShot (Рис.12.4).

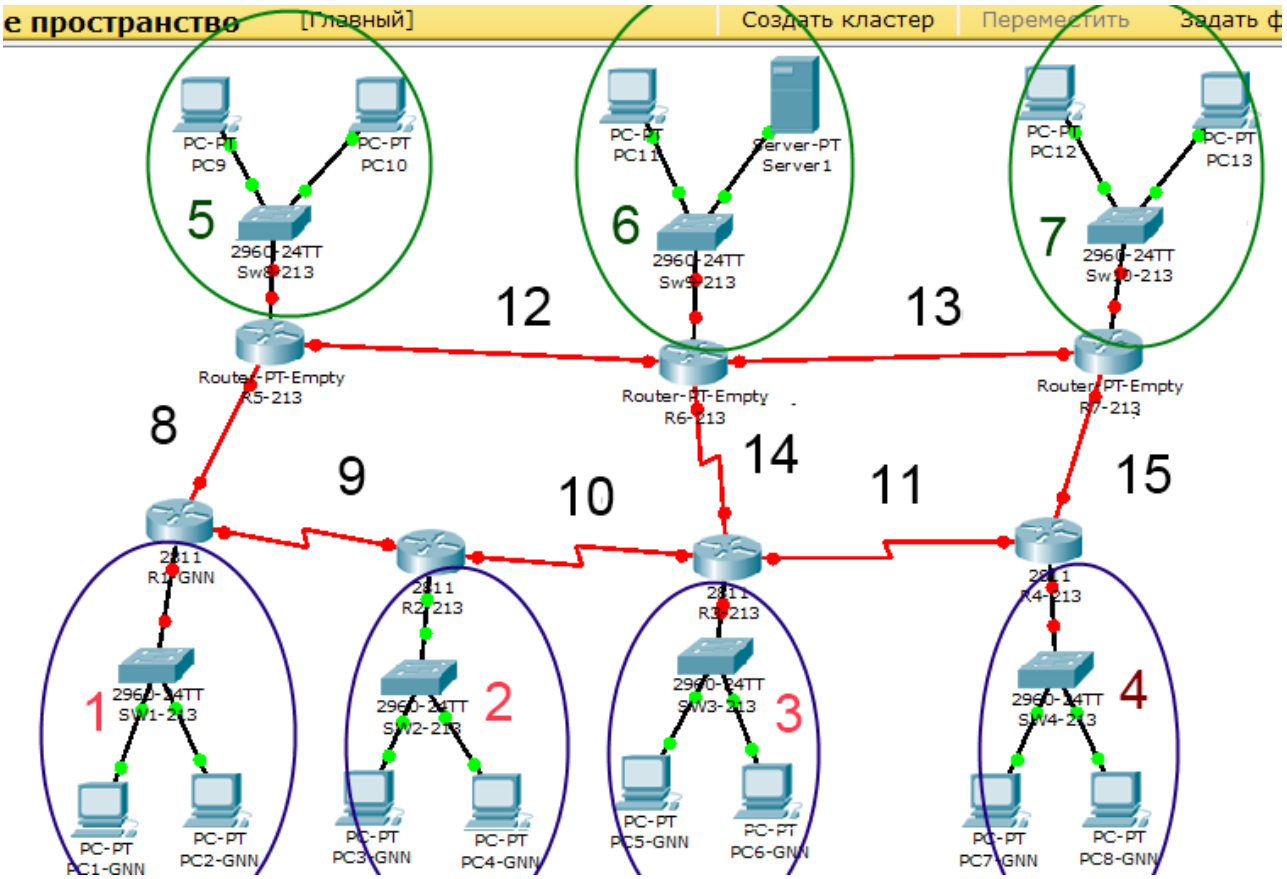

Рис.13.4 – Топология сети. Цифрами 1,2,3,4 и 5,6,7 обозначены IP сети независимых LAN сетей; Цифрами 8-15 подсети IP – WAN для линий связи между маршрутизаторами

5.1.9 После включения питания (на всех без исключени) необходимо изменить обозначения маршрутизаторов, согласно схемы Рис.13.4.

5.1.10 При обозначении коммутаторов, маршрутизаторов, компьютеров выполняем следующее правило, например:

Маршрутизатор Router-1 обозначается как, R1-GNN, где G-номер группы, NN-порядковый номер в журнале группы (ведущий ноль в данном случае пишется, например G-2,порядковый № 13, запишется как; router1 R1-213, а коммутатор обозначится как SW-1-213).

5.1.11 Настройку IP-адресов интерфейсов маршрутизаторов, подключенных к подсетям LAN с хостами проводить в соответствии с таблицей 13.1

Таблица 13.1 - Адреса сетей LAN и интерфейсов маршрутизаторов

	IP-адрес сети	**Интерфейсы**	**IP-адрес интерфейса**
Сеть1	192.100+G.NN.0/24	F0/0 R1-GNN	192.100+G.NN.1
Сеть2	192.100+G.10+NN.0/24	F0/0 R2-GNN	192.100+G.10+NN.1
Сеть3	192.100+G.20+NN.0/24	F0/0 R3-GNN	192.100+G.20+NN.1
Сеть4	192.100+G.30+NN.0/24	F0/0 R4-GNN	192.100+G.30+NN.1
Сеть5	192.100+G.40+NN.0/24	F2/0 R5-GNN	192.100+G.40+NN.1
Сеть6	192.100+G.50+NN.0/24	F3/0 R6-GNN	192.100+G.50+NN.1
Сеть7	192.100+G.60+NN.0/24	F2/0 R7-GNN	192.100+G.60+NN.1

При настройке, обязательно производите сверку номеров интерфейсов- куда и как они подключены. (см.Рис 13.4, Табл. 13.1 и Табл. 13.2),

При выполнении конфигурации интерфейсов необходимо ***учитывать следующее:*** обозначение (нумерация) интерфейса зависит от места установки модуля расширения. Для **Router-PT-Empty** - например, для маршрутизатора R6-GNN, интерфейс F3/0, обозначает 3-й слот шасси, 0-й порт. (см. Рис 13.5).

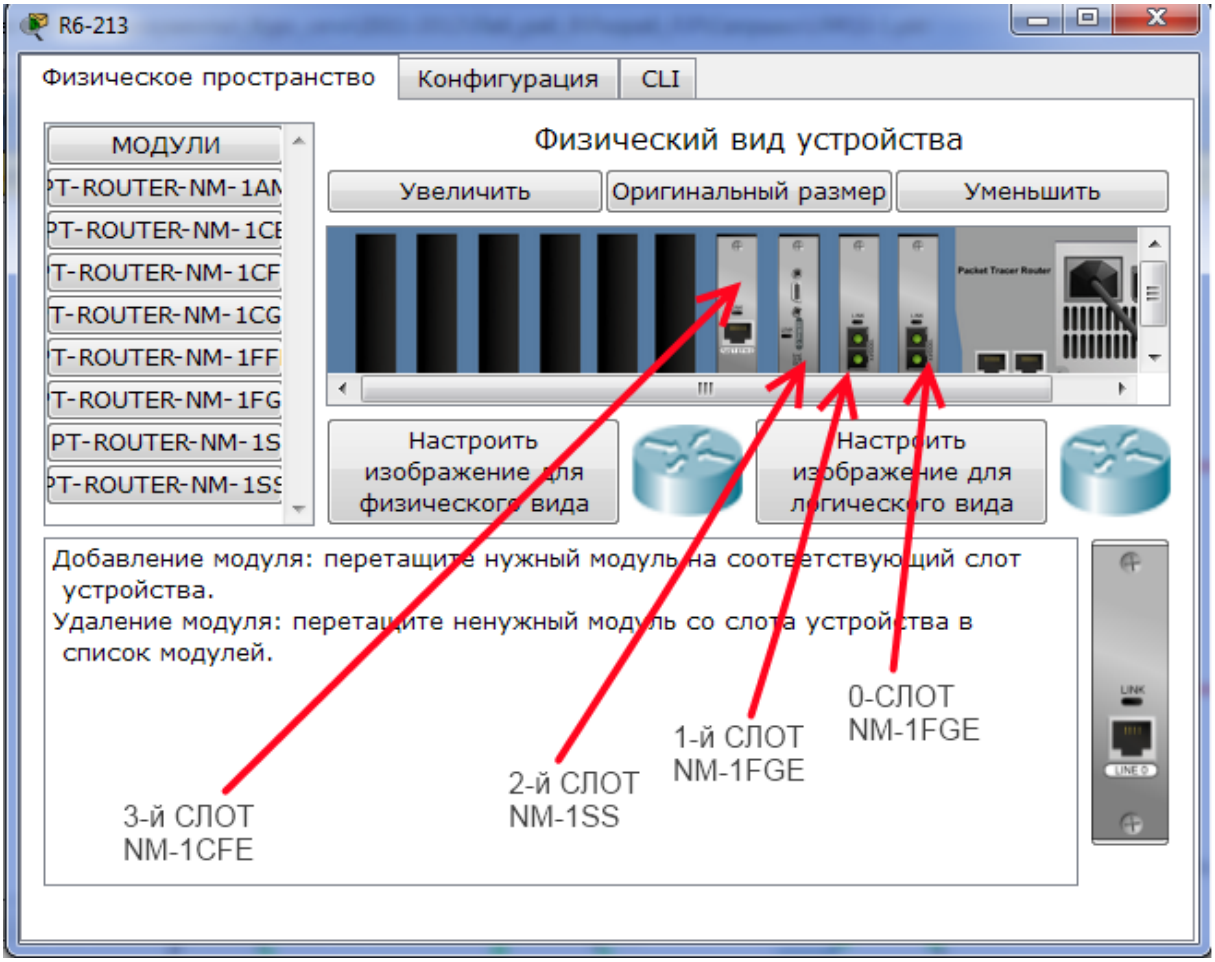

Рис.13.5 Расположение модулей расширения в маршрутизаторе R6-GNN.

В маршрутизаторе **Cisco 2811 используется следующий формат номеров** слотов/портов для **интерфейсных** модулей-карт: ***тип слота/слот/порт*** “0/слот/порт”. "0" обозначает слоты, встроенные в шасси маршрутизатора. Это относится к модулям типа HWIC, HWIC-D, WIC, VWIC, VIC, установленной непосредственно в слот шасси для HWIC. Так для WIC-2T значения будут в зависимости от места установки S0/1/0 и S0/1/0.

Для **сетевых модулей** типа NM-xx, HNM-xx, установленных в специальный ***слот маршрутизатора «для сетевых модулей», нумерация***, будет следующая:

«1/x» — таким образом, если это модуль NM-4A/S, порты обозначаться s1/0,s1/1,s1/2,s1/3. ***См. Рис. 13.6***.

В данный слот маршрутизатора можно также вставить плату расширения NM-2W, предоставляющую два дополнительных слота для модулей-карт с WAN интерфейсами, т.е. в слоты NM-2W можно установить например, два модуля WIC-2T. В этом случае серийные порты обозначаться как «s1/0/0 , s1/0/1» и «s1/1/0 , «s1/1/1».

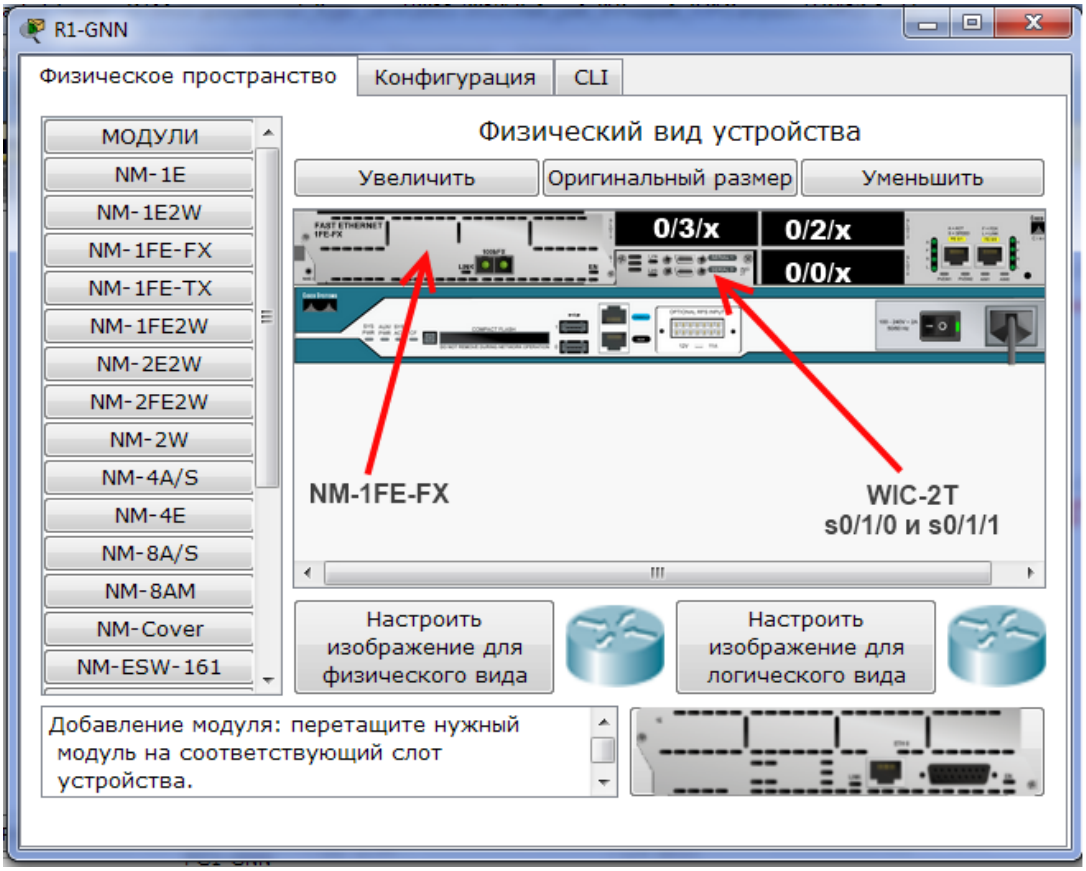

Рис.13.6

Нумерация слотов/портов в маршрутизаторе CISCO 2811

Таблица 13.2 - Адреса сетей WAN (8-15) и интерфейсов маршрутизаторов

	IP-адрес сети	**Интерфейсы**	**IP-адрес интерфейса**
Сеть8	200.8.8.0/30	F1/0 R1-GNN	200.8.8.1
		F1/0 R5-GNN	200.8.8.2
Сеть9	200.9.9.0/30	S0/1/1 R1-GNN	200.9.9.1
		S1/2 R2-GNN	200.9.9.2
Сеть10	200.10.10.0/30	S1/1 R2-GNN	200.10.10.1
		S1/2 R3-GNN	200.10.10.2
Сеть11	200.11.11.0/30	S1/0 R3-GNN	200.11.11.1
		S0/1/1 R4-GNN	200.11.11.2
Сеть12	200.12.12.0/30	G0/0 R5-GNN	200.12.12.1
		G1/0 R6-GNN	200.12.12.2
Сеть13	200.13.13.0/30	G0/0 R6-GNN	200.13.13.1
		G0/0 R7-GNN	200.13.13.2
Сеть14	200.14.14.0/30	S2/0 R6-GNN	200.14.14.1
		S1/3 R3-GNN	200.14.14.2
Сеть15	200.15.15.0/30	F1/0 R4-GNN	200.15.15.1
		F1/0-R7-GNN	200.15.15.2

5.1.12 НАСТРОЙКУ IP-АДРЕСОВ ИНТЕРФЕЙСОВ МАРШРУТИЗАТОРОВ, ПОДКЛЮЧЕННЫХ К СЕТЯМ WAN СО СМЕЖНЫМИ МАРШРУТИЗАТОРАМИ ПРОВОДИТЬ В СООТВЕТСТВИИ С ТАБЛИЦЕЙ 13.2

5.1.13 Настройка интерфейсов производится аналогично предыдущей Лаб.Раб. 12.

Перед настройкой интерфейсов каждого маршрутизатора на рабочем макете Cisco Packet Tracer «подписать» интерфейсы и их ip-адреса с помощью элемента 

1. Если маршрутизатор находится в стартовом пользовательском режиме, то необходимо ввести команду входа в привилегированный режим:

```
R1-213>enable
```

2. Далее вводим команду для входа в глобальный режим: *config terminal*.

```
R1-213#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
R1-213(config)#
```

3. Для того, чтобы отключить преобразование неправильно введенных команд в ip адрес или запрос DNS необходимо ввести команду ***no ip domain lookup***.
   В глобальном режиме введите команду ***no ip domain lookup***
4. Для входа в режим детального конфигурирования интерфейса, используется команда interface или int, например для R1-GNN интерфейс,

```
Router(config)#no ip domain lookup
Router(config)#
```

```
R1-213(config)#int f1/0
R1-213(config-if)#ip address 200.8.8.1 255.255.255.252
R1-213(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet1/0, changed state to down
R1-213(config-if)#
```

   включенный в подсеть № 8 (см.Рис 13.4 и Табл. 13.2) :
   Перед конфигурацией интерфейсов необходимо составить таблицы конфигурации по образцу таблиц 13.1 и 13.2 с конкретными значениями, при этом необходимо проводить сверку включенных портов модулей на действующем макете с введенным значением.
5. Посмотрите конфигурацию сконфигурированных интерфейсов f0/0, s1/1 и др. с помощью команды show running-config

Сохраните Screen Shot's Проверте полученные результаты со значениями в ранее созданных табицах, при необхлдимости внесите измененния.

Настройку интерфейсов для маршрутизаторов R3,R4,R6 выполнить с помошью CLI и представить ScreenShot's.

```
Router#show running-config
Building configuration...

Current configuration : 684 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
```

5.2 Конфигурирование протокола RIP

5.2.1 Проверьте отключены статические маршруты на маршрутизаторах R1-R4, используя вкладку «конфигурация» и кнопки «маршрутизация»-> «статическая». Отключите все статические маршруты. Это также можно сделать с помощью команды no ip route, например:

```
Router(config)#no ip route 200.50.50.0 255.255.255.0 200.60.60.11
```

5.2.2 Активация протокола маршрутизации RIP

RIP должен быть сначала активирован и лишь затем сконфигурирован.

Переходим в в режим глобального конфигурирования и вводим команду ***router rip*** для входа в режим конфигурирования протокола RIP:

```
R5-213#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
R5-213(config)#route rip
R5-213(config-router)#
```

5.2.3 Подключение соседних сетей.

Для запуска работы протокола RIP подключаем соседние сети:

```
R5-213(config)#route rip
R5-213(config-router)#network 200.8.8.0
R5-213(config-router)#network 200.12.12.0
R5-213(config-router)#network 192.102.53.0
R5-213(config-router)#exit
```

5.2.4 Просмотрите таблицы маршрутизации для каждого маршрутизатора.

Для просмотра таблицы маршрутизации на каждом маршрутизаторе вводим *show ip route.См.Рис 13.7*. ***на каждом маршрутизаторе***. Сделайте Screen Shot’s.

5.2.5 Просмотр настроек протокола RIP.

Посмотреть настройки протокола RIP можно с помощью команды ***show ip rip.***

См. Рис 13.8.

5.2.6 Проанализируйте результаты. Анализ и Screen Shot's отразите в отчете.

```
R7-213(config-router)#do show ip route
Codes: C - connected, S - static, I - IGRP, 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, E - EGP
       i - IS-IS, 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

R    192.102.13.0/24 [120/4] via 200.15.15.1, 00:00:04, FastEthernet0/0
                     [120/4] via 200.13.13.1, 00:00:09, GigabitEthernet1/0
R    192.102.23.0/24 [120/3] via 200.15.15.1, 00:00:04, FastEthernet0/0
                     [120/3] via 200.13.13.1, 00:00:09, GigabitEthernet1/0
R    192.102.33.0/24 [120/2] via 200.15.15.1, 00:00:04, FastEthernet0/0
                     [120/2] via 200.13.13.1, 00:00:09, GigabitEthernet1/0
R    192.102.43.0/24 [120/1] via 200.15.15.1, 00:00:04, FastEthernet0/0
R    192.102.53.0/24 [120/2] via 200.13.13.1, 00:00:09, GigabitEthernet1/0
R    192.102.63.0/24 [120/1] via 200.13.13.1, 00:00:09, GigabitEthernet1/0
C    192.102.73.0/24 is directly connected, FastEthernet2/0
R    200.8.8.0/24 [120/2] via 200.13.13.1, 00:00:09, GigabitEthernet1/0
R    200.9.9.0/24 [120/3] via 200.15.15.1, 00:00:04, FastEthernet0/0
                  [120/3] via 200.13.13.1, 00:00:09, GigabitEthernet1/0
R    200.10.10.0/24 [120/2] via 200.15.15.1, 00:00:04, FastEthernet0/0
                    [120/2] via 200.13.13.1, 00:00:09, GigabitEthernet1/0
R    200.11.11.0/24 [120/1] via 200.15.15.1, 00:00:04, FastEthernet0/0
R    200.12.12.0/24 [120/1] via 200.13.13.1, 00:00:09, GigabitEthernet1/0
     200.13.13.0/30 is subnetted, 1 subnets
C       200.13.13.0 is directly connected, GigabitEthernet1/0
R    200.14.14.0/24 [120/1] via 200.13.13.1, 00:00:09, GigabitEthernet1/0
     200.15.15.0/30 is subnetted, 1 subnets
C       200.15.15.0 is directly connected, FastEthernet0/0
R7-213(config-router)#
```

Рис.13.7 Просмотр таблицы маршрутизации на R7-213

Командный интерфейс IOS

```
rip
R1-213#show ip rip ?
  database  IP RIP database
R1-213#show ip rip database
192.102.13.0/24    auto-summary
192.102.13.0/24    directly connected, FastEthernet0/0
192.102.23.0/24    auto-summary
192.102.23.0/24
    [1] via 200.9.9.2, 00:00:21, Serial0/1/1
192.102.33.0/24    auto-summary
192.102.33.0/24
    [2] via 200.9.9.2, 00:00:21, Serial0/1/1
192.102.43.0/24    auto-summary
192.102.43.0/24
    [3] via 200.9.9.2, 00:00:21, Serial0/1/1
200.9.9.0/30    auto-summary
200.9.9.0/30    directly connected, Serial0/1/1
200.10.10.0/24    auto-summary
200.10.10.0/24
    [1] via 200.9.9.2, 00:00:21, Serial0/1/1
200.11.11.0/24    auto-summary
200.11.11.0/24
    [2] via 200.9.9.2, 00:00:21, Serial0/1/1
200.14.14.0/24    auto-summary
200.14.14.0/24
    [2] via 200.9.9.2, 00:00:21, Serial0/1/1
200.15.15.0/24    auto-summary
200.15.15.0/24
    [3] via 200.9.9.2, 00:00:21, Serial0/1/1
R1-213#
```

Рис.13.8 Результат конфигурации протокола RIP (RIP database).

5.2.7 *Добавьте маршрут по умолчанию для маршрутизатора R3-GNN*

И просмотрите после этого с помощью команды *show ip route* таблицы маршрутизации маршрутизаторов R3-GNN и R2-GNN. Проанализируйте, что означают записи со звездочками. ***Анализ и Screen's отразите в отчете.***

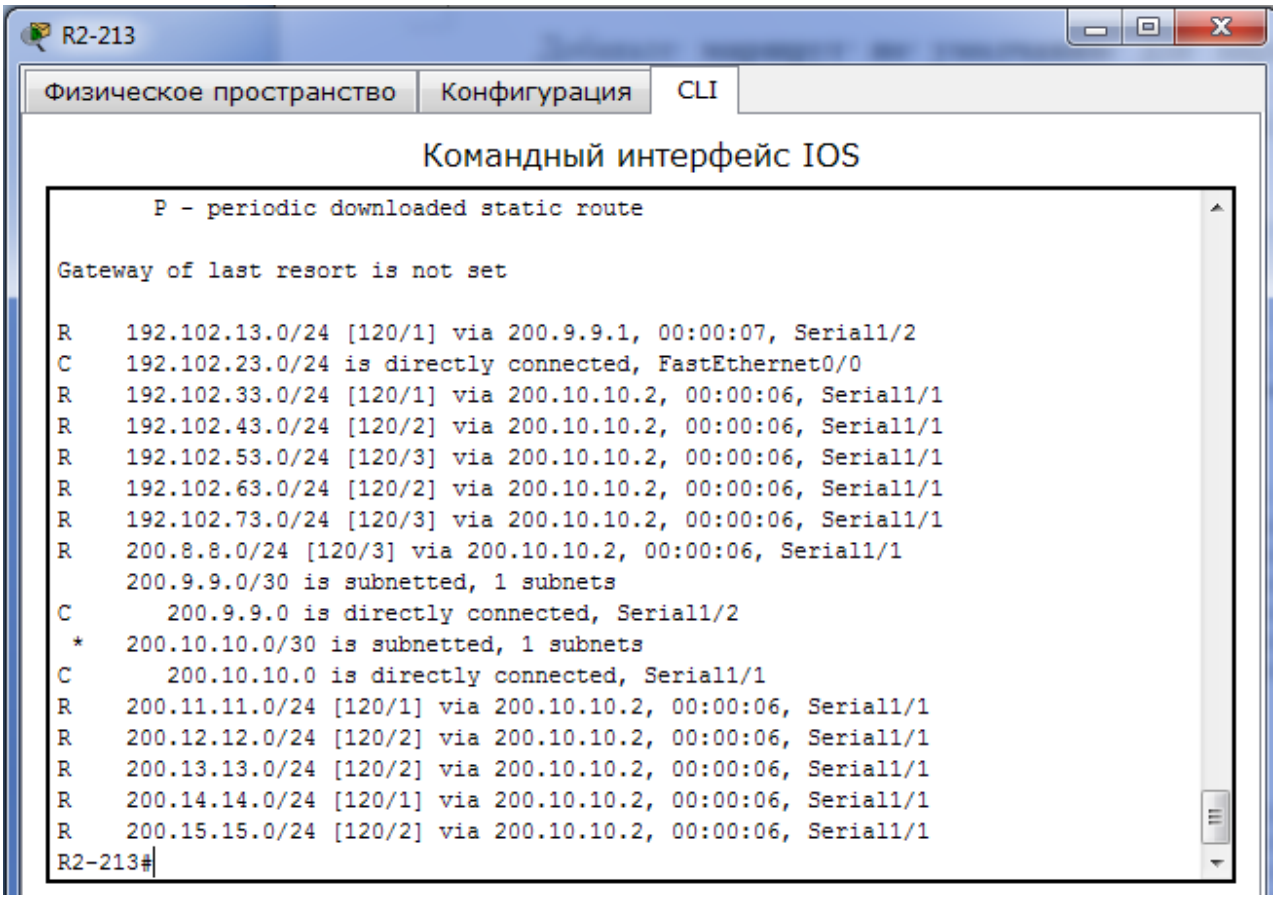

Рис 13.9.Добавление маршрута по умолчанию

5.2.8 *Проверьте работоспособность сети и таблицы маршрутизации*

с использованием команд ping и traceroute которые проверяют обеспечение IP-связи между маршрутизаторами и всей сети в целом.

```
R3-213>ping 192.102.13.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.102.13.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 47/56/63 ms
```

Значки "!!!!!" означают, что связь между маршрутизатором router3-GNN и интерфейсом 192.102.13.1 маршрутизатора R1-GNN удовлетворительная, 100% запросов и ответов (5 из пяти) переданы без искажений. При отсутствии возможности прозвонить узел или интерфейс вместо символов "!!!!!" будет сформирована последовательность из пяти точек – "...".

Убедитесь в работоспособности все компьютеров с помощью команды ping во все сети, представьте ScreenShot’s.

При защите Л.Р. иметь полностью оформленный отчет и рабочий файл PacketTracer с именем LR#13-GNN.pkt.

5.2.9 *Сконфигурируйте рабочие станции –хосты сети, и проверте работоспособность составной WAN сети в целом.*

выбрав IP- адреса, соответствующие в адресном пространстве сетям 1, 2, 3, … 7 (Таблица 13.1). На каждом PC(1-2), в качестве шлюза установить IP – адрес «своего» маршрутизатора. Используя команды ping и traceroute проверьте прохождение пакетов между PC принадлежащих разным сетям.

5.2.10 *Сохраните файл рабочего макета под именем LR#13-RIP-GNN, для предоставления вместе с отчетом.*

5.3 *Конфигурирование протокола OSPF*

Рассмотрим базовое конфигурирование протокола OSPF.

5.3.1 *Откройте ранее сохранённый файл рабочего макета под именем LR#13-RIP-GNN и сохраните его под именем LR#13-OSPF-GNN*

5.3.2 *Очистите таблицы маршрутизации, созданные по протоколу RIP для каждого маршрутизатора.*

Для этого откройте вкладку «Конфигурация» выбранного маршрутизатора далее нажмите кнопку «Маршрутизация»-> «RIP» и в окне «Маршрутизация RIP» удалите все маршруты.

5.3.3 *Отключение RIP протокола на каждом маршрутизаторе.*

Откройте вкладку CLI, войдите в глобальный режим конфигурирования и

```
R1-213(config-router)#exit
R1-213(config)#no router rip
```

далее введите команду ***no router rip*** Убедитесь, что RIP протокол остановлен полностью с помощью команды ***show ip rip database.*** Должны получить пустую строку.

5.3.4 *Разрешение (подключение) протокола OSPF.*

Чтобы разрешить маршрутизатору работать с протоколом OSPF, используется основная команда конфигурирования ОС IOS ***router ospf ID,*** где ID идентификатор OSPF процесса – число от 1 до 65535. Выбираем 1 (можно любое из указанного диапазона)

```
R1-213(config)#router ospf 1
R1-213(config-router)#
```

5.3.5 *Идентификация сетевых адресов, интерфейсов и областей AS включаемых в работу по протоколу OSPF.*

Для задания этой информации используется команда ***network***, которая имеет такой формат:

Rxx(config-router)#network <ip address> <wildcard bits> area <area address>,

где ***ip address*** –адрес непосредственно подключенной сети;

wildcard bits- подстановочная маска -4-х байтовое число, равное обратному значению маски сети;

area- целочисленное число –идентификатор области AS, может быть в формате наподобие IP-адреса, т.е. десятичные 4-е цифры, разделенные точками.

При выполнение необходимо, находясь в режиме конфигурации роутера R1-GNN(config-router), для каждой непосредственно подключенной сети ввести: IP адрес сети, подстановочную маску и идентификатор области AS, в которой расположен маршрутизатор.

Например: для маршрутизатора R3-213 вводим команду:

R3-213(config-router)# *network 192.102.33.0 0.0.0.255 area 0.*

192.102.33.0-адрес сети, подключенной к маршрутизатору R3,через интерфейс Fast Ethernet3/0***, 0.0.0.255***- подстановочная маска***, 0***- идентификатор области AS.

```
R3-213>enable
R3-213#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
R3-213(config)#router ospf 1
R3-213(config-router)#network 192.102.33.0 0.0.0.255 area 0
R3-213(config-router)#network 200.10.10.0 0.0.0.3 area 0
R3-213(config-router)#network 200.11.11.0 0.0.0.3 area 0
R3-213(config-router)#network 200.14.14.0 0.0.0.3 area 0
R3-213(config-router)#end

%SYS-5-CONFIG_I: Configured from console by console
R3-213#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R3-213#
```

5.3.6 *Выполняем пункт 5.3.5 для всех маршрутизаторов сети.*

5.3.7 *Проверим конфигурацию OSPF.*

Проверим настроенную нами конфигурацию OSPF с помощью команды ***R1#show ip protocols*** см.рис 13.10.

5.3.8 *Проверим таблицу конфигурации маршрутизатора.*

с помощью команды show ip route. см.рис 13.11

5.3.9 *Проверьте работоспособность сети в целом*

Отправите Simple PDU  от произвольного хоста к хосту другой сети, а также с помощью команд ***ping*** и ***traceroute*** от хоста к хосту.

В отчете представить Screen Shot’s, а также пояснения и анализ работы сети

.

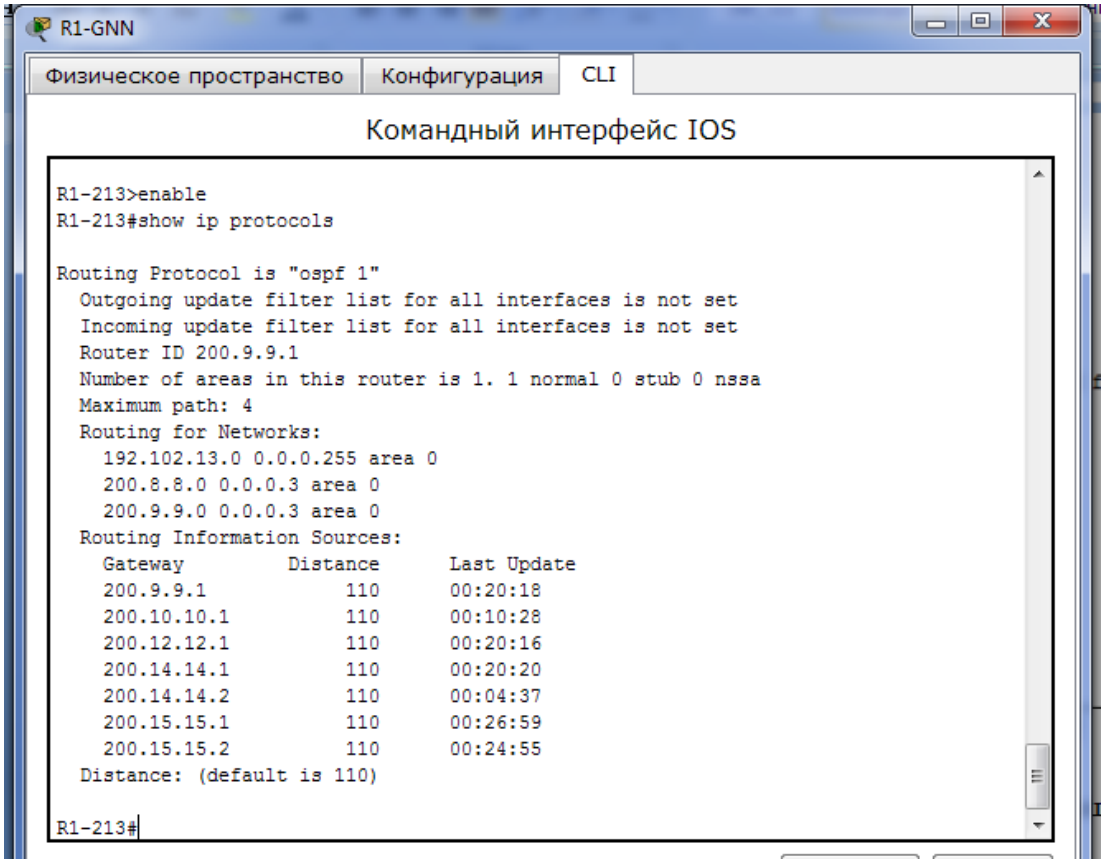

Рис.13.10 Проверка конфигурации OSPF протокола.

Рис 13.11 таблица конфигурации маршрутизатора с протоколом **ospf**

Основные особенности, характеристики динамической маршрутизации.

5.3.10 Протокол RIP. (Routing Information Protocol)

Протокол маршрутной информации (Routing Information Protocol — RIP) один из первых протоколов, разработанный в начале 80-х годах компанией Xerox.

RIP – протокол дистанционно-векторной маршрутизации, использующий для нахождения оптимального пути алгоритм Беллмана-Форда, в стандартах Интернета RFC был первоначально определен в документе RFC 1058 в 1988 году. Наиболее существенны его следующие характеристики:

- RIP является дистанционно-векторным протоколом маршрутизации;
- в качестве метрики при выборе маршрута используется количество переходов - hop's –количество транзитных маршрутизаторов;
- если количество переходов становится больше 15, пакет отбрасывается;
- стандартно обновления маршрутизации (routing updates) рассылаются широковещательным способом каждые 30 секунд.
- Используются версии RIP-1 и улучшенная версия RIP-2.

RIP – это простой протокол требует меньше вычислительных ресурсов, в частности гораздо меньше памяти, чем современные протоколы маршрутизации.

Вторая версия протокола – протокол RIP v2 была разработана в 1994 году, и претерпела значительную эволюцию: от основанного на классах протокола маршрутизации RIP первой версии (RIPv1) к бесклассовому протоколу RIP второй версии (RIPv2).

Принцип дистанционно-векторного протокола:

1. RIP является дистанционно-векторным протоколом. Каждый маршрутизатор, использующий протокол RIP, периодически широковещательно рассылает своим соседям специальный пакет-вектор, содержащий расстояния (измеряются количеством переходов –hop's, отображается в метрике) от данного маршрутизатора до всех известных ему сетей.

2. Маршрутизатор получивший такой вектор, наращивает компоненты вектора на величину расстояния от себя до данного соседа и дополняет вектор информацией об известных непосредственно ему самому сетях или сетях, о которых ему сообщили другие маршрутизаторы. Дополненный вектор маршрутизатор рассылает всем своим соседям.

3. Маршрутизатор выбирает из нескольких альтернативных маршрутов маршрут с наименьшим значением метрики, а маршрутизатор, передавший информацию о таком маршруте помечается как следующий (next hop). Алгоритм RIP допускает возникновение петель маршрутизации, которые могут быть вызваны рассинхронизацией таблиц на роутерах, из-за отказов в линии связи, ошибках в канале или отрицательными вершинами графа при расчете оптимального пути (следствие алгоритма Беллмана-Форда).

Чтобы исправить положение в RIP были введены дополнительные функции:

- Ограничение количества переходов данный маршрут перестанет рассматриваться (метод poison reverse);
- Отмена маршрута;
- Расщепление горизонта (split horizon);

- Временное удерживание изменений.
- Мгновенные обновления (triggered update).

***Максимальное количество транзитных переходов** (ограничение количества переходов).*

Стандартом RIP, максимальное количество транзитных переходов (хопов-метрика) установлено равное 15. Это один из первых методов, предотвращающий бесконечное «блуждание» пакетов по сети.

Число переходов отображается в метрике пакета маршрутизации и наращивается при каждом переходе через транзитный узел маршрутизатор, т.е. метрика наращивается на единицу. Если метрика маршрутизации примет значение равное 16 (бесконечно большая), пакет помечается как недоставленный и отбрасывается; данный маршрут перестанет рассматриваться (метод poison reverse).

***Предотвращение петель в маршрутизации с помощью расщепления горизонта* (split horizon).**

На Рис 13.12 показан пример возникновения петли: В данном случае (маршрутизаторы будем обозначать, как М-А,М-Б и т.д.):

- маршрутизатор М-А получив информацию от М-Д, что четь 1 не доступна посылает обновления к М-Б и М-Г;
- но чуть позже на маршрутизатор М-Б поступает пакет обновления от М-В, что сеть 1 доступна с метрикой 4;
- После получения последнего сообщения маршрутизатор М-Б неправильно заключает, что у М-В по-прежнему имеется действительный маршрут к сети 1. Маршрутизатор М-Б отсылает сообщения об обновлении маршрутизатору А, извещая его о новом маршруте к сети 1.
- Получив его, устройство А делает вывод о том, что оно может переслать информацию в сеть 1 через М-Б. В свою очередь маршрутизатор М-Б заключает, что он может посылать информацию в сеть 1 через М-В, а маршрутизатор В решает, что он может послать информацию в сеть 1 через маршрутизатор Г. В такой ситуации любой пакет будет двигаться по кольцевому маршруту (петле) между этими маршрутизаторами.

Расщепление горизонта пытается предотвратить такую ситуацию. Согласно этому методу, при поступлении сообщения об обновлении маршрутов для сети 1

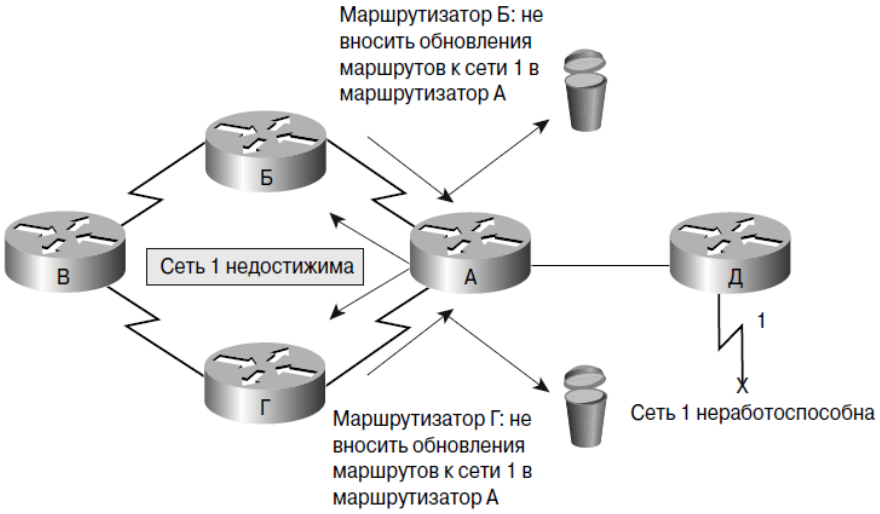

Рис 13.12 Образование петли и Расщепление горизонта

от маршрутизатора М-А маршрутизаторы М-Б и М-Г не могут посылать информа-

цию о сети 1 в обратном направлении, т.е. маршрутизатору М-А, как показано на рис. 13.12. Таким образом, *расщепление горизонта (split horizon)* не позволяет распространять неверную информацию маршрутизации и уменьшает объем передаваемых служебных сообщений.

Отмена маршрута

В RIP также реализована корректировка, отменяющая маршрут. Отмена маршрута (route poisoning) происходит тогда, когда некоторому пути в таблице маршрутов присваивается значение 16 для количества переходов. После такого присваивания путь становится невидимым или недостижимым. Отмена маршрута может быстро предотвратить появление петли маршрутизации.

Route poisoning возникает, если маршрутизатор непрерывно получает обновления маршрутов, в которых метрика (стоимость) некоторого пути возрастает. В этом случае маршрутизатор определяет, что возникла петля маршрутизации. Тогда маршрутизатор устанавливает в своей таблице маршрутов метрику пути, равную 16, и инициирует обновление маршрутов. Это обновление предупреждает все соседние устройства о том, что путь «испорчен» и не должен использоваться.

Таймер временного удерживания изменении.

Таймеры временного удерживания изменений (hold-down timers) используются вместе с другими возможностями RIP. Такой таймер применяется для того, чтобы задать количество времени, в течение которого какой-то определенный путь не может быть обновлен. Когда маршрутизатор обнаруживает недоступный канал, инициируется обновление таблицы маршрутов. Тогда маршрутизатор устанавливает для этого маршрута таймер временного удерживания изменений. Таймер не допускает обновления таблицы маршрутов данного маршрутизатора потенциально недействительной информацией, полученной от соседнего устройства (которое могло еще не получить корректировку). После того как время удерживания истекает, маршрутизатор снова получает возможность обновлять путь.

Предотвращение петель маршрутизации посредством мгновенных обновлений (triggered update в маршрутизаторах CISCO) .

Данный метод не описан в стандартах RFC, но широко применяется многими компаниями, изготавливающими сетевые устройства.

Протокол RIP рассылает регулярно сообщения обновлений каждые 30 секунд. Однако мгновенные обновления (triggered update) рассылаются немедленно в ответ на какое-либо изменение в таблице маршрутизации. Маршрутизатор, который обнаружил изменение в топологии, немедленно рассылает сообщение-обновление смежным маршрутизаторам. Такие маршрутизаторы в свою очередь также генерируют мгновенные обновления, оповещая о переменах своих соседей. При выходе какого-либо маршрута из строя сообщение отправляется, не дожидаясь истечения времени таймера обновления. Использование мгновенных обновлений в сочетании с механизмами удаления маршрутов гарантирует, что все маршрутизаторы будут оповещены об отказавших маршрутах до истечения времени любого таймера хранения информации.

Дистанционно - векторные протоколы, и в том числе прокол RIP обладает ***ещё одним существенным недостатком – большим временем конвергенции***

(сходимости сети). Для уменьшения этого времени существуют также определенные методы и технологии. Последний описанный метод **мгновенных обновлений triggered update** помимо предотвращения петель, позволяет также ускорить обновления при изменении топологии сети.

Таймеры RIP Cisco.

Ускорить время конвергенции, можно изменив параметры системы таймеров управления RIP протокола.

Параметры таймеров RIP Cisco могут быть изменены администратором.

В процессе маршрутизации RIP использует четыре таймера: таймер обновления (корректировки маршрутов), таймер временного удерживания изменений, тайм-аут маршрута и таймер удаления маршрута. Все четыре таймера связаны со способом обновления таблиц маршрутов и тем интервалом, через который маршрутизатор делает эти обновления. Каждый таймер имеет значение по умолчанию, которое может быть заменено на более подходящее для конкретной сети. Для установки таймеров RIP используйте команду timers basic. Структура этой команды такова:

#timers basic <routing update timer> <route timeout> <hold-down timer> <route removal> (см. 1.5**ниже**) (IOS_Timers)

Например, чтобы задать определенные значения времени с помощью команды timers basic, следует выполнить в режиме конфигурирования протокола маршрутизации такие команды:

Router(config-router)#***timers basic 30 180 45 270***

В данном примере для таймера обновления маршрутов было установлено значение 30 секунд, то есть данный маршрутизатор RIP отправляет регулярно обновления своей таблицы маршрутов каждые 30 секунд. Тайм-аут для маршрута был установлен равным 180 секундам. Это означает, что если обновление от какого-то маршрутизатора не поступило в течение 180 секунд, то такой маршрутизатор будет помечен. Таймер временного удерживания изменений (hold-down timer- замораживания …) установлен равным 45 секундам. Так как этот таймер определяет время, в течение которого маршрутизатор не может производить никаких корректировок, то он должен быть отрегулирован так, чтобы не совпадать ни с каким существующим таймером корректировки.

Наконец, таймер удаления пути установлен равным 270 секундам. Любой маршрутизатор, обновление от которого не получено в течение этого времени, считается недостижимым и удаляется из таблицы маршрутов.

Стандартно время удержания (<***route timeout***>) в протоколе RIP составляет 180 секунд. В течение этого времени не разрешается обновление внутренних маршрутов. Для ускорения конвергенции время таймера удержания может быть уменьшено, однако такое уменьшение требует осторожности. Идеальным решением является установка этого периода удержания чуть большим максимального времени обновления маршрутов в конкретной объединенной сети.

Помимо таймеров, Cisco предоставляет **ряд необязательных параметров** для настройки RIP. Многие из них могут быть установлены вручную, тем самым можно удовлетворить потребности практически любой среды. К ним относятся:

• **Таймеры RIP**

• Отмена и назначение адресов/интерфейсов для обновления (анонсов), т.е. для определения направления обмена таблицами маршрутизации; (нежелательные анонсы);

• Версию RIP, которая совместима с другими реализациями и продуктами других производителей.

Нежелательные анонсы.

Довольно часто возникает необходимость запретить передачу информации обновлений маршрутов с какого-либо интерфейса, т.е. удалить нежелательные анонсы обновлений. Такая ситуация может возникнуть, например, когда маршрутизатор корпоративной сети имеет интерфейс связанный с провайдером Интернет. Чтобы отменить отправку обновлений применяется команда passive-interface: ***Router(config-router) #passive-nterface <interface> <interface number>***

```
R6-213(config-router)#passive-interface fa3/0
R6-213(config-router)#
```

Работа с различными версиями RIP.

Версии 1 и 2 протокола RIP частично совместимы.

Стандартно RIPv1может получает пакеты протоколов RIPv1 и RIPv2, однако рассылает только пакеты протокола RIPv1. Используя маршрутизатор Cisco можно сконфигурировать его как на получение, так и на отправку только пакетов одной из версий RIP, либо одновременно первой и второй версии. Для того чтобы сконфигурировать маршрутизатор Cisco с применением первой или второй версии или их комбинации применяется команды:

- **Для глобальной конфигурации роутера** –

(config router)#version {1 | 2},

- **Для конфигурации конкретного интерфейса:**

(config if)#ip rip send version {1 | 2},

(config if)#ip rip receive version {1 | 2}

(config if)#ip rip {send | receive} version 1 2.

Данная настройка необходима в случаях, когда в сети используются маршрутизаторы разных производителей, например простой роутер для маленькой сети с RIPv1, подключенный к провайдеру, где Cisco и RIPv2.

Указанные выше технологии служат как для борьбы с петлями, так и для устранения других недостатков RIPv1 и улучшения функциональности: рассинхронизацией таблиц, уменьшением времени сходимости таблиц (временем конвергенции), уменьшения служебного трафика, и достижения более гибкой возможности конфигурации.

Таблица маршрутов RIP.

Протокол маршрутизации порождает таблицу маршрутов, в которой хранится вся информация, необходимая маршрутизатору для перемещения данных. Обычно такая таблица находится в ОЗУ маршрутизатора (а не во флэш памяти). Благодаря этому маршрутизатор может быстро получить доступ к таблице и (при необходимости) сделать изменения.

Типичная таблица маршрутов маршрутизатора Cisco, работающего с RIP, представлена в табл. 13.3

Поля таблицы:

1. ***Сеть:*** адрес сети назначения.
2. ***Следующий переход:*** IP-адрес маршрутизатора, который является следующим звеном при перемещении к адресату.
3. ***Стоимость:*** также называется ***метрикой,*** представляет количество переходов после «следующего», необходимых для достижения адресата.
4. ***Таймер:(см.(IOS_Timers))*** поле на самом деле представляет три разных таймера, используемых RIP. Таймер обновления маршрутов (***routing update timer***) указывает интервал между обновлениями. Обычно RIP отсылает копию своей таблицы маршрутов каждые 30 секунд. Второй таймер – это тайм-аут для маршрута-таймера удержания (***route timeout***). Если от какой-то конкретной сети обновление маршрутов не получено в течение 180 секунд, то маршрут помечается как недостижимый. Последний таймер – таймер удаления маршрута (***route removal timer***). Таймер удаления маршрута удаляет из таблицы маршрутов любой маршрут, который не обновлялся в течение последних 240 секунд.
5. ***Флаги:*** в поле хранятся различные необязательные данные (RIP используется нечасто).

Таблица 13.3. Пример таблицы маршрутов.

Сеть	Следующий переход	Метрика	Таймер	Флаги
153.19.88.0	Маршрутизатор A	2	30-180-240	
198.63.35.0	Маршрутизатор B	6	30-180-240	
153.19.89.0	Маршрутизатор C	1	30-180-240	

Особенности протокола RIP.

Маршрутизаторы, использующие RIP, отправляют соседним устройствам копии своих таблиц маршрутов каждый раз по истечении таймера обновления ***(routing update timer)*** маршрутов, равного по умолчанию 30 сек. Соседние маршрутизаторы в свою очередь, также отправляют информацию о вновь сформированной таблице, и так до тех пор, пока все маршрутизаторы сети (области AS) получат изменения топологии сети.

Построение таблицы маршрутизации.

Построение таблицы маршрутизации происходит поэтапно.

На первом этапе – в момент инициализации (включения роутера) создаётся минимальная таблица маршрутизации. Она содержит информацию только о непосредственно подсоединенных сетях, благодаря уже настроенным интерфейсам.

Этап 2 — рассылка минимальной таблицы соседям.

После инициализации каждого маршрутизатора он начинает посылать своим соседям сообщения протокола RIP, в которых содержится его минимальная таблица.

RIP-сообщения передаются в дейтаграммах протокола UDP и включают два параметра для каждой сети: ее IP-адрес и расстояние до нее от передающего сообщение маршрутизатора. Соседями, являются маршрутизаторы, интерфейсы которых непосредственно включены к данному маршрутизатору.

Этап 3 — получение RIP-сообщений от соседей и обработка полученной информации.

После получения RIP сообщений соседний маршрутизатор наращивает каждое полученное поле метрики на единицу и запоминает, через какой порт, и от какого маршрутизатора получена новая информация.

Далее маршрутизатор начинает сравнивать новую информацию с той, которая хранится в его таблице маршрутизации. Если уже имеется запись с совпадающими значениями сетей назначения, то протокол RIP замещает запись при условиях: - 1) в новой записи метрика меньше, чем в имеющейся; 2) если в новой записи метрика больше (хуже), но информация пришла от того же маршрутизатора, на основании которого была создана прежняя запись, то худшая информация замещает лучшую.

Этап 4 — рассылка новой таблицы соседям

Каждый маршрутизатор отсылает новое RIP-сообщение всем своим соседям. В этом сообщении он помещает данные обо всех известных ему сетях — как непосредственно подключенных, так и удаленных, о которых маршрутизатор узнал из RIP-сообщений.

Этап 5 — получение RIP-сообщений от соседей и обработка полученной информации.

Этап 5 повторяет этап 3 — маршрутизаторы принимают RIP-сообщения, обрабатывают содержащуюся в них информацию и на ее основании корректируют свои таблицы маршрутизации

Инициировать обновление маршрутов RIP могут три события: истечение времени корректировки маршрутов (таймер update routing), изменение состояния канала и непосредственный запрос RIP на обновление. Первое событие отражается в поле таблицы маршрутов RIP. По умолчанию таймер корректировки маршрутов устанавливается в 30 секунд. Когда это время проходит, маршрутизатор отправляет копию своей таблицы маршрутов каждому своему непосредственному соседу(устройству, с которым он соединен напрямую). Соседи используют информацию для обновления собственных таблиц маршрутов и порождения своих собственных корректировок.

Второе событие происходит, если канал связи между двумя маршрутизаторами (или между маршрутизатором и сетью) оказывается поврежденным, тогда непосредственно связанный с этим каналом маршрутизатор обновляет свою таблицу и незамедлительно отправляет корректировку соседям. В случае обновления, вызванного изменением сети, отправляется только та часть таблицы маршрутов, которая подверглась изменению. Соседние маршрутизаторы обновляют соответствующие части своих таблиц и продолжают передавать корректировки.

Наконец, третье событие происходит, когда маршрутизатор Cisco, использующий RIP, запрашивает обновление у определенного маршрутизатора. Обычно это делается по истечении срока временного удерживания изменений ***route timeout***. Когда маршрутизатор получает запрос на обновление, запрашивающей стороне отсылается вся таблица маршрутов.

В настоящее время используются RIPv1 как *Classful Routing Protocol – RIP* Version 1 (**RIP v1**) и более совершенный бесклассовый маршрутизирующий протокол *Classless Routing Protocol – RIP* Version 2 (**RIP v2**).

При использовании протокола **RIP v1** , всегда необходимо помнить, что сетевые адреса, как основной параметр маршрутизации, является адресами с

применением классов (classful –сети класса A,B,C, D и E), а не масок. Это означает, что ***RIP v1***-протокол, например, используя сети класса B (172.16.0.0), не сможет разделить на более мелкие подсети с 24 битами маски, т.е. когда третий октет используется для адресации подсетей, а четвертый – для адресации узлов каждой подсети. Таким образом, подсети 172.16.1.0, 172.16.2.0…172.16.N.0, будут рассматриваться как единая сеть 172.16.0.0.

Протокол *RIP* v2 дополнительно включает следующие функции:

- способность переносить дополнительную информацию о маршрутизации пакетов;
- для обновления используется multicast вместо broadcast;
- механизм аутентификации для обеспечения безопасного обновления таблиц маршрутизации;
- поддержка масок подсети переменной длины (VLSM)

Протоколы RIPv1 и RIPv2 непригодны для работы в больших сетях, так как засоряет сеть интенсивным трафиком, а узлы сети оперируют только векторами-расстояний, не имея точной информации о состоянии каналов и топологии сети. Сегодня даже в небольших сетях протокол вытесняется превосходящими его по возможностям протоколами EIGRP (протокол Cisco) и OSPF.

Протокол OSPF.

OSPF (Open Shortest Path First) – протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала (link-state). Был разработан IETF в 1988 году и основан на алгоритме Дейкстра для поиска кратчайшего пути. В качестве метрики OSFP использует коэффициент качества обслуживания (стоимость канала или cost). Отслеживание состояния канала требует отправки объявлений о состоянии канала (link-state advertisment, LSA) на активные интерфейсы всех доступных маршрутизаторов зоны. В этих объявлениях содержится описание всех каналов маршрутизатора, отношения соседства и стоимость каждого канала. Для вычисления стоимости канала используется отношение 10^8/ширина_канала. Для отправки объявлений OSPF использует multicast сообщения (в отличие от RIP). LSA сообщения отправляются только если произошли какие-либо изменения в сети, но раз в 30 минут LSA сообщения отправляются в принудительном порядке. Протокол реализует деление автономной системы на зоны (areas). Маршрутизаторам, принадлежащим одной зоне, не известна детальная топология других зон. Использование зон позволяет снизить нагрузку на сеть и процессоры маршрутизаторов (уменьшение объема расчетов по SPF), уменьшить размер таблиц маршрутизации.

Различают следующие типы зон:

• Магистральная (backbone) – формирует ядро сети OSPF

• Стандартная (standart) – зона, которая создается по умолчанию. Принимает обновления каналов, суммарные и внешние маршруты.

• Тупиковая (stub) – не принимает информацию о внешних маршрутах для автономной системы, но принимает маршруты других зон. Для передачи информации за пределы автономной зоны использует маршрут по умолчанию.

• Полностью тупиковая (totlly stubby) – не принимает информацию как о внешних маршрутах автономной системы, так и маршруты других зон. Использует шлюз по умолчанию.

Маршрутизаторы внутри зон также делятся на типы:

• Внутренний (internal) – маршрутизатор, все интерфейсы которого принадлежат одной зоне.

• Пограничный (area border, ABR) – соединяет одну или больше зон с магистральной.

• Магистральный (backbone) – хотя бы один интерфейс маршрутизатора данного типа принадлежит к магистральной зоне.

• Пограничный маршрутизатор автономной системы (AS boundary, ASBR) – обменивается информацией с маршрутизаторами в других автономных системах. Может быть как внутренним, пограничным, так и магистральным.

OSPF быстро реагирует на изменения в сети, рассылая модификации при изменениях в сетевой топологии всем маршрутизаторам в пределах некоторой области сети. **OSPF** предназначен для работы в больших гибких составных сетях и **может** работать с оборудованием разных фирм-производителей, поэтому получил широкое распространение.

Административное расстояние протокола **OSPF** равно 110. Протокол используется внутри определенной области, в которой маршрутизаторы разделяют маршрутную информацию между собой. Таких областей может быть несколько, среди которых нулевая область является главной или единственной.

Протоколы Link-state создают таблицы маршрутизации на основе информации, хранящейся в **специальной базе данных (link-state database)**, а также в **таблице данных соседних устройств (neighbor table)**. При этом алгоритм Дейкстры (Dijkstra) обеспечивает выбор кратчайшего пути (shortest *path*) к адресату назначения. Протокол OSPF не проводит периодический обмен объемными обновлениями (update) маршрутной информации и характеризуется быстрой сходимостью (convergence).

Для обмена маршрутной информацией между устройствами протокол **OSPF** использует пять типов пакетов:

1. Пакет Hello.
2. Пакет описания базы данных DataBase Description – DBD.
3. Пакет запроса Link-State Request – *LSR*.
4. Пакет обновлений Link-State Update – *LSU*.
5. Пакет подтверждения Link-State *Acknowledgment* – LSAck.

Hello-пакеты используются, чтобы устанавливать и поддерживать **отношения смежности** между соседними устройствами. Hello-пакеты содержат **идентификатор устройства** (*Router ID*), который по сути является адресом одного из интерфейсов маршрутизатора. На этапе формирования смежности устанавливаются 3 значения:

1. Период времени обмена Hello-пакетами (Hello *Interval*).
2. Период времени (Dead *Interval*), по истечению которого связь считается потерянной, если за это время не было получено ни одного Hello-пакета.
3. Тип сети (Network Type).

Различают три типа сетей:

1. Широковещательные с *множественным доступом* (*Broadcast* multiaccess), например Ethernet.
2. Сети типа "точка-точка" (Point-to-point).

3. Нешироковещательные с *множественным доступом* (NonBroadcast Multi-Access – NBMA), например, сети *Frame Relay, ATM*.

Поэтапное описание работы протокола:

1. Все маршрутизаторы обмениваются специальными Hello-пакетами через все интерфейсы, на которых активирован протокол OSPF. Таким образом, определяются маршрутизаторы-соседи, разделяющие общий канал передачи данных. В дальнейшем hello-пакеты посылаются с интервалом раз в 30 секунд.

2. Маршрутизаторы пытаются перейти в состояние соседства со своими соседями. Переход в данное состояние определяется типом маршрутизаторов и типом сети по которой происходит обмен hello-пакетами, по зонному признаку. Пара маршрутизаторов в состоянии соседства синхронизирует между собой базу данных состояния каналов.

3. Каждый маршрутизатор посылает объявление о состоянии канала своим соседям, а каждый получивший такое объявление записывает информацию в базу данных состояния каналов и рассылает копию объявления другим своим соседям.

4. При рассылке объявлений по зоне, все маршрутизаторы строят идентичную базу данных состояния каналов.

5. Каждый маршрутизатор использует алгоритм SPF для вычисления графа (дерева кратчайшего пути) без петель, который будет описывать кратчайший путь к каждому известному назначению с собой в качестве корня.

6. Каждый маршрутизатор строит собственную маршрутизацию, основываясь на построенном дереве кратчайшего пути.

5.3.11 Border Gateway Protocol (BGP)

BGP (протокол граничного шлюза) - основной протокол динамической маршрутизации в Интернете.

BGP, в отличие от других протоколов динамической маршрутизации, предназначен для обмена информацией о маршрутах не между отдельными маршрутизаторами, а между целыми автономными системами, и поэтому, помимо информации о маршрутах в сети, переносит также информацию о маршрутах на автономные системы. BGP не использует технические метрики, а осуществляет выбор наилучшего маршрута исходя из правил, принятых в сети.

BGP поддерживает бесклассовую адресацию и использует суммирование маршрутов для уменьшения таблиц маршрутизации. С 1994 года действует четвёртая версия протокола, все предыдущие версии являются устаревшими.

BGP является протоколом прикладного уровня и функционирует поверх протокола транспортного уровня TCP (порт 179).

BGP, наряду с DNS, является одним из главных механизмов, обеспечивающих функционирование Internet.

6 Контрольные вопросы:

1) В чем заключается задача маршрутизации? Что такое протокол маршрутизации?
2) Специальные термины и понятия: метрика, Автономная система, Административное расстояние, Алгоритм выбора SPF, шлюз по умолчанию
3) Протоколы маршрутизации. Классы, автономные системы AS. Какие протоколы применяются между AS и внутри AS? Дать краткие характеристики.

4) Какие протоколы относятся к дистанционно-векторной маршрутизации?
5) Какие протоколы относятся к протоколам, использующим алгоритмы состояния связи.?
6) Принцип дистанционно-векторного протокола по этапно?
7) Основные ограничения протокола RIP и какие методы применялись для устранения этих ограничений? Расскажите подробно о каждом.
8) Как образуются петли в сети, с применением протокола RIP?
9) Таймеры RIP Cisco, функции и назначение, команды конфигурации.
10) Нежелательные анонсы RIP. Какой командой можно их устранить, с привязкой к конкретному интерфейсу?
11) Какие версии RIP Вы знаете? Совместимость версий RIP. С помощью какой команды можно инициализировать ту или иную версию и и для чего она нужна?
12) Таблица маршрутизации протокола RIP? Поля таблицы, по этапное построение таблицы маршрутизации.
13) Назовите три основных события обновления таблицы. Рассказать о каждом подробно.
14) Какой тип IP-адресации используются в RIP ver.1 и ver.2
15) Какие дополнительные функции включает протокол RIPv2.
16) Где лучше применять протокол RIP?
17) На каком алгоритме основан протокол OSPF?
18) Что является метрикой OSPF и как она вычисляется?
19) Что такое LSA, для чего используются и как часто они появляются в сети?
20) На какие подразделы – области делится AS с OSPF?
21) Какие типы зон Вы знаете?
22) Как делятся по типам маршрутизаторы зон?
23) Какой идентификатор присваивается основной или единственной зоне?
24) На основе каких данных создают таблицы протоколы Link-state?
25) Назовите пять типов пакетов для обмена маршрутной информацией между устройствами OSPF?
26) Какие типы сетей различают в протоколе OSPF?
27) Поэтапное описание работы протокола OSPF.
28) Протокол BGP- назначение, функции.
29) Какую информацию формирует и переносит протокол BGP?
30) Какой тип IP-адресов использует протокол BGP?
31) К какому уровню OSI относится **BGP протокол?**

7 ДОПОЛНИТЕЛЬНЫЕ МАТЕРИАЛЫ:

1. В.Г. Олифер, Н.А. Олифер Компьютерные сети, 3-е издание, 2009г. Стр.602…638: 667-698.
2. Программа сетевой академии CISCO CCNA 1 и 2 Вспомогательное руководство. 3-е издание. Стр.757-797.
3. Димарцио Д. Ф. Маршрутизаторы Cisco. Пособие для самостоятельного изучения. СПб: Символ□Плюс, 2003. – 512 с., ил.