ГОСУДАРСТВЕННОЕ УЧРЕЖДЕНИЕ  
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ  
«БЕЛОРУССКО-РОССИЙСКИЙ УНИВЕРСИТЕТ»

Кафедра «Автоматизированные системы управления»

АППАРАТНОЕ И ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ЭВМ И СЕТЕЙ.

***Методические указания   
к выполнению лабораторных работ   
для студентов специальности 1-53 01 02   
«Автоматизированные системы обработки информации»***

**Маршрутизация в IP-сетях. Технологии глобальных сетей**.

**Сети Frame Relay**.

Могилев 2015

УДК 621.01

ББК 34.4

И 87

Рекомендовано к опубликованию

Центром менеджмента качества образовательной деятельности

ГУ ВПО «Белорусско-Российский университет»

Одобрено кафедрой «Автоматизированные  системы  управления»

«11» ноября 2015 г., протокол № 4

 Составитель ст. преподаватель В. Т. Садовский

Рецензент канд. техн. наук, доц. С. В. Болотов.

Методические указания к выполнению   
лабораторных работ для студентов специальности 1-53 01 02   
 «Автоматизированные системы обработки информации»

Учебное издание

АППАРАТНОЕ И ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ЭВМ И СЕТЕЙ

Интеллектуальные функции коммутаторов LAN-Ethernet.

|  |  |
| --- | --- |
| Ответственный за выпуск | С. К. Крутолевич |
| Технический редактор | А. Т. Червинская |
| Компьютерная верстка | Н. П. Полевничая |

Подписано в печать.                        Формат 60х84/16. Бумага офсетная. Гарнитура Таймс.

Печать трафаретная. Усл.-печ. л.       Уч.-изд. л.        Тираж 31 экз. Заказ №

Издатель и полиграфическое исполнение

Государственное учреждение высшего профессионального образования

«Белорусско-Российский университет»

Свидетельство о государственной регистрации издателя, изготовителя, распространителя печатных изданий № 1/156 от 24.01.2014.

пр. Мира, 43, 212000, г. Могилев,

|  |  |
| --- | --- |
|  | © ГУ ВПО «Белорусско-Российский  университет», 2015 |

Лабораторная работа № 12. Изучение протокола статической маршрутизации с использованием оборудования CISCO.

**Цель работы:** Изучение принципов маршрутизации IP сетей на примере протоколов статической маршрутизации с использованием программного обеспечения построения виртуальных сетей - Packet Tracer 6.0. Получение практических навыков по настройке маршрутизаторов Cisco 2901.

# 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. 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, подключенных локально (непосредственно), и интерфейсов, через которые осуществляется подключение, 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. На физическом и канальном уровне наиболее часто используются технологии Ethernet, FastEthernet, GigabitEthernet, 10GEthernet, Toking Ring, FDDI, PPP, Frame Relay, X.25, SDH, PDH,DWDM и др.

Рис 12.1 Маршрутизатор Linksys для дома и малого офиса со встроенным коммутатором и точкой доступа

На сетевом уровне используются сетевые протоколы: IPv4, IPv6, IPX, Frame Relay, ATM, X.25. Маршрутизаторы различаются по области их применения. Маршрутизаторы для дома и небольшого офиса имеют малый размер, просты в настройке. Зачастую в них встроен коммутатор Ethernet и беспроводная точка доступа WiFi.

Высокопроизводительные промышленные маршрутизаторы выпускаются в 19 дюймовых Unit корпусах для монтажа в серверную стойку. Представляют собой шасси с установленными модулями/блоками. Их функциональность, как правило, можно расширить с помощью установки дополнительных модулей. Такие маршрутизаторы отличает высокая скорость обработки пакетов, многофункциональность, возможность передачи данных в различных физических средах (за счет сменных модулей) и использования различных стандартных протоколов, а также мульти сервисность и высокая стоимость.



Рис 12.2 Профессиональные маршрутизаторы CISCO серии 2900 для филиалов крупной корпоративной сети.





Рис 12.3 Маршрутизатор CISCO 2901 для установки в 19'' стойку, обеспечивающий мульти сервисный сервис ISR фирмы CISCO.

# Средства маршрутизации

Каждый маршрутизатор принимает решения о направлении пересылки пакетов на основании таблицы маршрутизации. Таблица маршрутизации содержит набор правил. Каждое правило в наборе описывает шлюз или интерфейс, используемый маршрутизатором для доступа к определенной сети.

Маршрут состоит из четырех основных компонентов (полей записи):

* значение получателя (адрес сети назначения);
* маска;
* интерфейс (порт);
* адрес шлюза;
* стоимость маршрута или метрика маршрута.

Чтобы переслать сообщение получателю, маршрутизатор извлекает IP-адрес получателя из пакета и находит соответствующее правило в таблице маршрутизации. Значения получателей в таблице маршрутизации соответствуют адресам сетей получателей.

Чтобы определить наличие маршрута к IP-адресу получателя в таблице, маршрутизатор сначала определяет число битов, задающих адрес сети получателя. Затем маршрутизатор ищет в таблице маску подсети, присвоенную каждому из потенциальных маршрутов. Маршрутизатор применяет каждую из масок подсети к IP-адресу получателя в пакете и сравнивает полученный адрес сети с адресами отдельных маршрутов в таблице:

1. при обнаружении совпадающего адреса пакет пересылается на соответствующий интерфейс или к соответствующему шлюзу;

2. если адрес сети соответствует нескольким маршрутам в таблице маршрутизации, маршрутизатор использует маршрут с наиболее точным или наиболее длинным совпадающим фрагментом адреса сети;

3. иногда для одной сети адресата существует несколько маршрутов с равной стоимостью: маршрут, используемый маршрутизатором, выбирается на основе правил протокола маршрутизации;

4. в отсутствие совпадающих маршрутов маршрутизатор направляет сообщение на шлюз, указанный в маршруте по умолчанию, если он настроен.

Появление записей в таблице маршрутизации происходит в основном из трех источников:

1. ***Программного обеспечения стека протокола TCP/IP.*** Это записи с особыми IP-адресами: как 127.0.0.0, 224.0.0.0.; записи с адресами, предназначенные для обработки широковещательных рассылок (записи имеющие маску 255.255.255.255), а также записи о непосредственно подключенных сетях и маршрутах по умолчанию (данная информация- результат конфигурирования интерфейсов маршрутизатора ).
2. ***Записи с адресами сетей назначения, сформированные вручную администратором с помощью утилиты (команды) ip route***. Такие записи называются ***статическими***. Они имеют неограниченный срок жизни.
3. И, наконец, третьим источником записей могут быть ***протоколы маршрутизации, такие как RIP, OSPF, BGP.*** Такие записи всегда являются динамическими, то есть имеют ограниченный срок жизни.

Для маршрутизатора желательно поддерживать маршруты к каждому возможному адресу назначения, но при большем количестве сетей, достичь этого полностью невозможно, и часто прибегают к маршруту по «умолчанию». Маршрут по «умолчанию» или «маршрут последней надежды» -это маршрут с адресом куда перенаправляются все пакеты не определенные таблицей маршрутизации.

# Специальные термины и понятия.

**Метрика** – числовой коэффициент, влияющий на выбор маршрута в компьютерных сетях. Как правило, определяется количеством хопов (ретрансляционных переходов) до сети назначения или параметрами канала связи. Чем метрика меньше, тем маршрут приоритетнее.

**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.

**Автономная система (AS)** – группа маршрутизаторов, обменивающаяся маршрутной информацией при помощи одного протокола.

**Шаблонная маска (wildcard mask)** – маска, указывающая на количество хостов сети. Является дополнением для маски подсети. Вычисляется по формуле для каждого из октетов маски подсети как 255-маска\_подсети. Например, для сети 192.168.1.0 и маской подсети 255.255.255.242 шаблонная маска будет выглядеть как 0.0.0.13. Шаблонная маска используется в настройке некоторых протоколов маршрутизации, а так же является параметром ограничений в списках доступа.

**Административное расстояние (administrative distance)** – коэффициент надежности маршрута, используемый на маршрутизаторах компании Cisco. Приоритет имеет тот маршрут, который обладает меньшим административным расстоянием. В случае двух одинаковых маршрутов с одинаковым административным расстоянием рассматривается метрика маршрута. Таким образом, использование административных расстояний позволяет резервировать маршруты.

|  |  |
| --- | --- |
| ***Источник данных о маршруте*** | ***Административное расстояние*** |
| Непосредственно подключенная сеть | 0 |
| Статический маршрут | 1 |
| Суммарный маршрут EIGRP | 5 |
| Внешний протокол BGP | 20 |
| Внутренний протокол EIGRP | 90 |
| Протокол IGRP | 100 |
| Протокол OSPF | 110 |
| Маршрут от одной промежуточной системы к другой (IS-IS) | 115 |
| Протокол RIP | 120 |
| Протокол внешнего шлюза (EGP) | 140 |
| Внешний протокол EIGRP | 170 |
| Внутренний протокол BGP | 200 |
| Неизвестный источник | 255 |

**Петля маршрутизации** – явление, возникающее, когда маршрутизатор отсылает пакет на адрес назначения, а получивший такой пакет маршрутизатор, возвращает его обратно. Таким образом, получается петля. Для борьбы с подобными петлями в TCP/IP предусмотрен механизм TTL. Протоколы маршрутизации так же предлагают способы борьбы с петлями.

# Протоколы маршрутизации

Протокол маршрутизации — это сетевой протокол, используемый маршрутизаторами для определения возможных маршрутов следования данных в составной компьютерной сети.

**Статическая маршрутизация** – вид маршрутизации, при котором информация о маршрутах заносится в таблицы маршрутизации каждого маршрутизатора вручную администратором сети. Статические маршруты не изменяются до тех пор, пока администратор не перенастроит их вручную. В таблице маршрутизации эти маршруты обозначаются буквой **S**. Символом **С** в таблице маршрутизации помечены непосредственно присоединенные к маршрутизатору сети.  Маршрутизатор задействует административное расстояние каждого маршрута, чтобы определить лучший путь к адресату. Меньшее административное расстояние означает более надежный источник. Данный вид маршрутизации **имеет ряд недостатков**:

* Плохая масштабируемость, так как при добавлении N сети потребуется сделать 2\*(N+1) записей о маршрутах.
* при достаточно большой сегментации составной сети (N подсетей > 5) таблица маршрутизации на каждом из маршрутизаторов будет сильно отличаться от таблиц на других устройствах.
* Отсутствует возможность адекватно отреагировать на ошибки и отказы оборудования канального и сетевого уровня (когда передача данных невозможна, а порт маршрутизатора по-прежнему находится в активном состоянии(up).
* Ввод всей информации вручную является весьма трудоемкой задачей и влечет за собой необходимость документирования этих маршрутов.
* При изменении топологии сети требуется вручную менять правила маршрутизации, т.е. переконфигурировать таблицу маршрутизатора.
* Все эти проблемы решаются (передачей служебной широковещательной информации в сеть) **в протоколах динамической** маршрутизации, о которых речь пойдет ниже.

***Но есть и положительные качества***:

* Легкость конфигурации Метод статической маршрутизации является довольно простым для понимания и настройки и по праву считается наименее сложным методом маршрутизации.
* Отсутствует обмен служебной информацией между маршрутизаторами о топологии сетей, таким образом и дополнительная нагрузка на сеть в виде широковещательного служебного трафика, характерного для динамических протоколов маршрутизации.
* При использовании статических записей процессору маршрутизатора не требуется производить никаких расчетов, связанных с определением маршрутов.

***Статическая маршрутизация продолжает успешно использоваться при****:*

* организации работы компьютерных сетей небольшого размера (1-2 маршрутизатора
* на компьютерах (рабочих станциях) внутри сети. В таком случае обычно задается маршрут шлюза по умолчанию.
* В целях безопасности- когда необходимо скрыть некоторые части составной корпоративной сети;
* Если доступ к подсети обеспечивается одним маршрутом, то вполне достаточно использовать один статический маршрут. Такой тип сети (подсети) носит названия тупиковой сети (stub network).

**Статическая маршрутизация по умолчанию** означает, что если пакет предназначен для сети, которая не перечислена в таблице маршрутизации, то маршрутизатор отправит пакет по заданному по умолчанию маршруту. При этом маршрутизатор направляет пакеты к следующему маршрутизатору, когда тот в таблице не задан явно. Заданные по умолчанию маршруты устанавливаются как часть статической конфигурации.

# Практическое выполнение задания:

Для выполнения лабораторной работы используется ПО Cisco Packet Tracer.

Запустите программу Cisco Packet Tracer.

## Базовая настройка маршрутизаторов и устройств сети

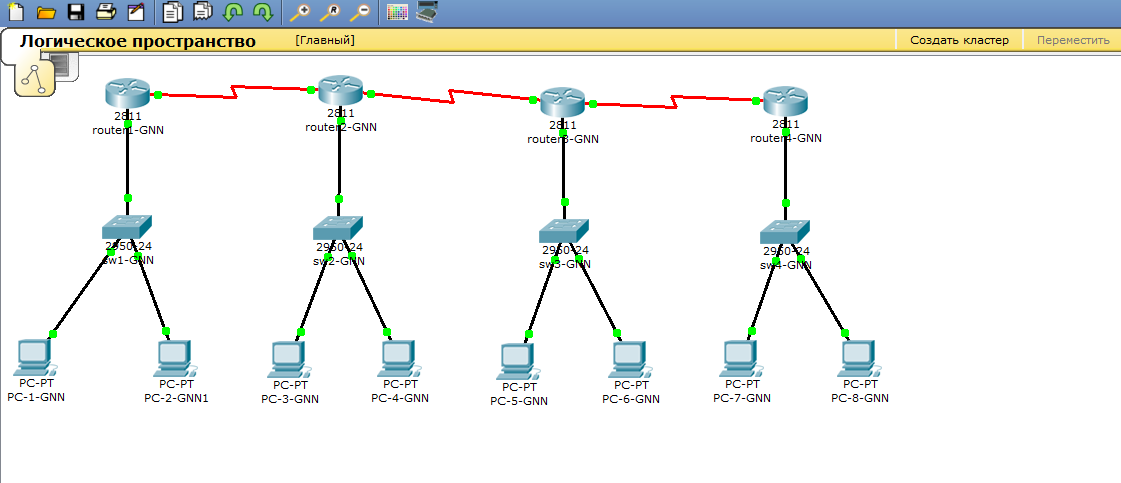
В области «Логическое пространство» создайте иерархическое дерево сети, аналогичное дереву на данном ScreenShot (Рис.12.2).

Рис.12.2 – Топология сети

**5.1.** При обозначении коммутаторов, маршрутизаторов, компьютеров выполняем следующее правило, например коммутатор SW-1 ***обозначается как***,

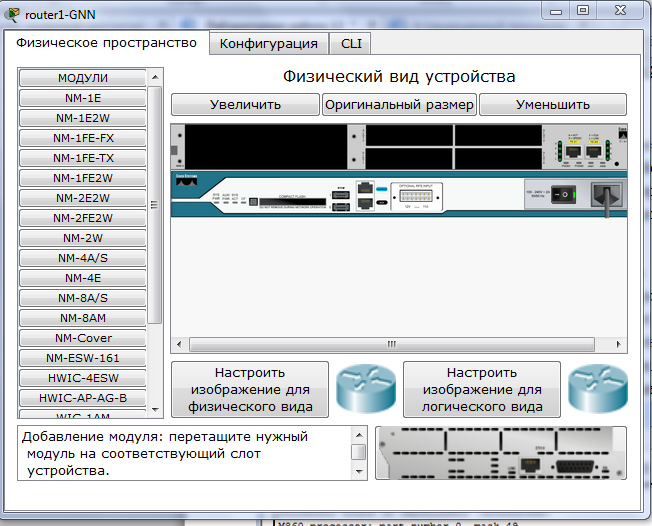
***SW-1-GNN, G-номер группы, NN-порядковый номер в журнале группы (ведущий ноль в данном случае пишется, например G-2,порядковый № 13, запишется как SW-1-213; router1 обозначится как R1-GNN.***

**5.2.** Конструкция выбранного маршрутизатора (2811) предусматривает наличие 2-х интерфейсов Fast Ethernet, для увеличения количества интерфейсов надо установить плату расширения. Выбираем из списка сетевой модуль Cisco NM-4A/S на 4 асинхронных/синхронных последовательных порта.

*Модуль Cisco NM-4A/S позволяет иметь 4 низкоскоростных последовательных соединений через DB-60 коннекторы, поддерживающие 5 типов интерфейсов (RS-232, RS-449, RS-530, V.35, X.21) и в режиме DTE и в DCE. Такие соединения могут быть сконфигурированы вплоть до 115.2 kbps на асинхронный трафик или 128 kbps на синхронный.*

Для этого нужно выключить маршрутизатор. Выбрать плату и установить ее в свободный разъем. После установки необходимо включить маршрутизатор. На рисунках 1 и 2 показан пример добавления платы NM-4A-S в router1-GNN.

Из имеющегося списка можно выбрать более скоростную плату (модуль), например NM-1FE-FX, данный модуль, предоставляет один интерфейс Fast-Ethernet для подключения оптического кабеля. В этом случае можно достичь скорости 100Mb/s, но придется использовать оптический кабель. Cisco 2811 поддерживает множество других модулей, так например WIC-2A/S поддерживает два последовательных соединения T1/E1, асинхронный и синхронный трафик. Подключается напрямую к слоту WIC.

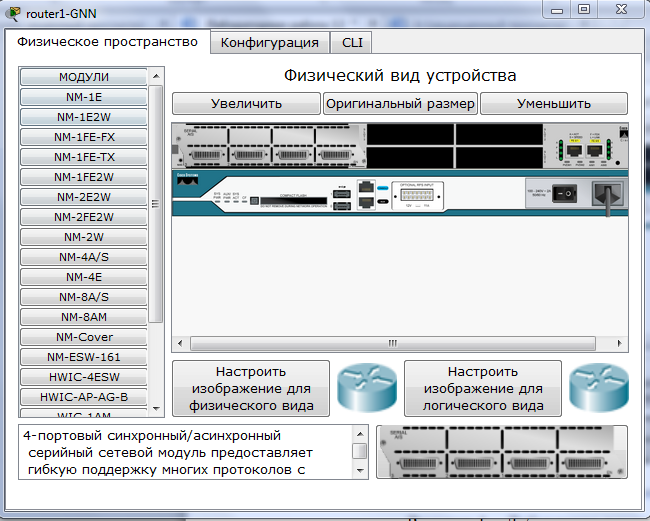


***Кнопка питания (включена по умолчанию)***

**Тянем сюда**

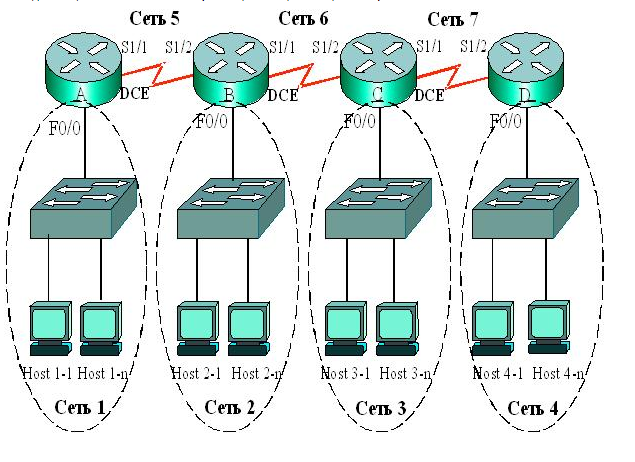
**Требуемый модуль (плата)**

**Рис12.3 – Добавление модуля NM-4A/S**



**Рис12.4 – Установленная плата NM-4A/S**

Аналогичные действия повторить для остальных маршрутизаторов.



**Рис12.5 – Упрощенная схема сети с указанием портов и разбиением на подсети**

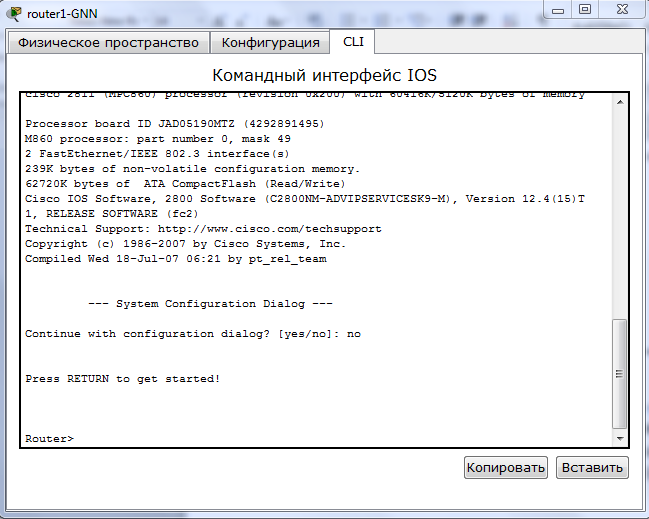
**Конфигурирование интерфейсов маршрутизаторов**

Таблица 12.1 - Адреса сетей 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 | 200.50.50.0/30 | S1/1 R1-GNN | 200.50.50.11 |
|  |  | S1/2 R2-GNN | 200.50.50.12 |
| Сеть6 | 200.60.60.0/30 | S1/1 R2-GNN | 200.60.60.11 |
|  |  | S1/2 R3-GNN | 200.60.60.12 |
| Сеть7 | 200.70.70.0/30 | S1/1 R3-GNN | 200.70.70.11 |
|  |  | S1/2 R4-GNN | 200.70.70.12 |

**Настройку IP-адресов интерфейсов проводить в соответствии с таблицей 12.1!**

**5.3.** После начальной загрузки маршрутизатора *операционная система* предложит продолжить *конфигурирование* в диалоговом режиме, от которого следует отказаться (*Continue* *with* *configuration* *dialog*? [yes/no]: **no** ). Аналогичная *запись* появляется и при работе с реальными устройствами. В некоторых версиях операционных систем затем необходимо подтвердить завершение диалогового режима.

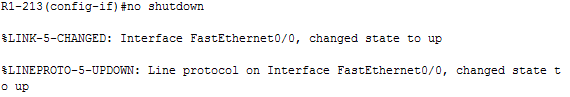


**5.4.** Для входа в **привилегированный режим** вводим *команду* *enable,*а затем для входа в **глобальный режим** *команду* *config terminal (conf term)*.



**5.5** Для того чтобы войти в режим детального конфигурирования интерфейса, используется *команда* interface (либо сокращенный ее вариант *int*) в глобальном режиме конфигурации. Например, при конфигурировании интерфейса Fast Ethernet с номером 0, входящим в состав слота 0, используется *команда*

**5.6** Установка IP-адреса интерфейса 192.102.13.1 c маской 24 производится следующей командой:

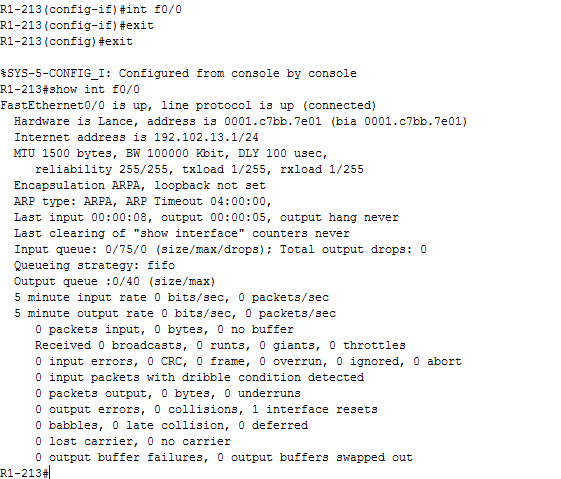
**5.7** По умолчанию все интерфейсы выключены. Включение интерфейса производится по команде *no shutdown*, а выключение – командой *shutdown*:

**5.8** Конфигурацию интерфейса можно просмотреть по команде ***show interfaces и show running-config*** (сокращенно ***sh int и sh run*** ). *По* команде sh int производится *верификация* всех интерфейсов маршрутизатора.

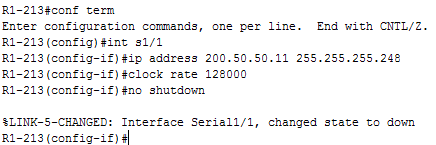
*Верификация* одного конкретного интерфейса производится по команде sh int с указанием проверяемого устройства. Ниже приведена часть распечатки команды sh int f0/0, по которой проводится проверка конфигурации интерфейса **Fast Ethernet 0/0**:

***R1-213>sh int f0/0***

Результат выполнения данной команды представлен ниже:

Из распечатки следует, что:

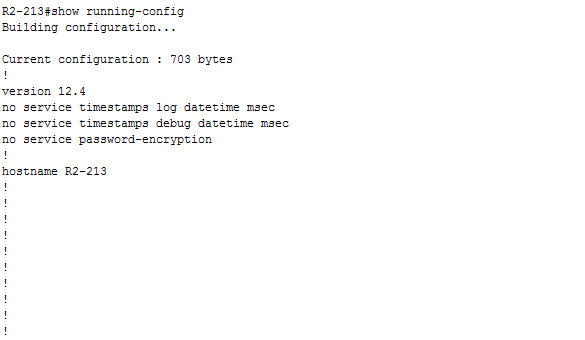
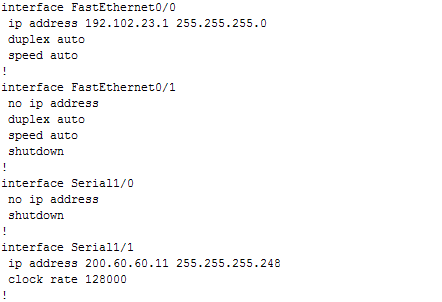
* Интерфейс включен (*Fast Ethernet* 0/0 is up), и протокол на нем – тоже (*line* *protocol* is up),
* МАС-*адрес* интерфейса *Fast Ethernet* 0/0 будет 0001.c7bb.7e01,
* IP-*адрес* – 192.102.13.1/24, где число 24 означает маску 255.255.255.0, максимальный размер кадра:
* *MTU* – 1500 *байт*,
* ширина полосы – 100 Мбит/с (BW 100000 Kbit),
* задержка – 100 мкс (DLY 100 usec),
* надежность – максимальная (*reliability* 255/255),
* передача и прием (*txtload* 1/255 и rxload 1/255). .

**5.9**  При конфигурировании *последовательного интерфейса*, имеющего *DCE*-подключение, например интерфейса s1/1 маршрутизатора R1-GNN, задается не только IP-*адрес*, но и *скорость передачи* данных в битах в секунду с помощью команды *clock rate*:

*Команда* *clock rate* определяет, что *интерфейс* s1/1 маршрутизатора R1\_GNN является ведущим (**DCE**) в соединении "*точка-точка*" с интерфейсом s1/2 маршрутизатора R2\_GNN.

Конфигурация остальных маршрутизаторов аналогична:

**5.10** Посмотрите конфигурацию сконфигурированных интерфейсов f0/0, s1/1, s1/2 и других с помощью *команды show running-config:*





**5.11.**  Повторите пункты 5.1-5.10 для остальных маршрутизаторов, установив для них IP-адреса в соответствии с таблицей 12.1 Для маршрутизаторов R2-GNN, R3-GNN конфигурируются два последовательных интерфейса s1/2 и s1/2 а для маршрутизатора R1 интерфейс s1/1, а для R4 –s1/2, т.к. они пограничные. Смотрите **Рис12.5**, на котором указаны интерфейсы и подсети.

**Для каждого шага по п. 5.1-5.10 сохраняйте ScreenShot's. в отчете**

**5.12.**  Установите IP-адрес для всех конечных устройств (Host).

При работе с пакетом *Packet* *Tracer* задание параметров узла производится следующим образом:

1. "Кликнуть" конфигурируемый узел, например, первый узел Сети 1.
2. Во всплывшем окне выбрать опцию "Desktop", затем "IP Configuration" и затем в новом окне установить IP-адрес узла, *маску подсети* и адрес шлюза в соответствии с Таблица 12.2.

Таблица 12.2. Адреса составной сети

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Сеть** | **Адрес сети** | **Шлюз по умолчанию** | **IP-адрес узла1** | **IP-адрес узла2** |
| ***Сеть1*** | **192.100+G.NN.0/24** | **192.100+G.NN.1** | **192.100+G.NN.2** | **192.100+G.NN.3** |
| ***Сеть2*** | **192.100+G.10+NN.0/24** | **192.100+G.10+NN.1** | **192.100+G.10+NN.2** | **192.100+G.10+NN.3** |
| ***Сеть3*** | **192.100+G.20+NN.0/24** | **192.100+G.20+NN.1** | **192.100+G.20+NN.2** | **192.100+G.20+NN.3** |
| ***Сеть4*** | **192.100+G.30+NN.0/24** | **192.100+G.30+NN.1** | **192.100+G.30+NN.2** | **192.100+G.30+NN.3** |

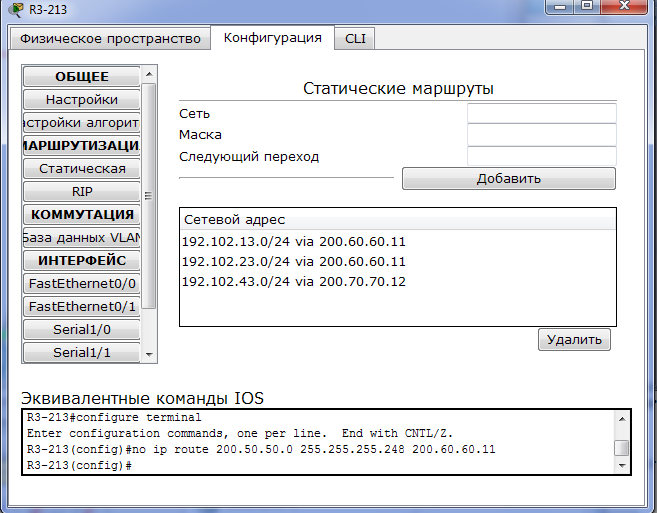
## Конфигурирование статической маршрутизации

Адрес входного интерфейса следующего маршрутизатора на пути к адресату также называют **шлюзом по умолчанию**. Например, для пакетов, попавших в маршрутизаторR2-GNN, шлюзами по умолчанию будут:

1. интерфейс s1/1 маршрутизатора R1-GNN с адресом 200.50.50.11,
2. интерфейс s1/2 маршрутизатора R3-GNN с адресом 200.60.60.12.

### Формирование таблицы статической маршрутизации.

Для ввода таблицы маршрутизации необходимо на вкладке Конфигурация выбрать Маршрутизация - статическая. На Рис 12.6 показан пример ввода таблицы маршрутизации для маршрутизатора R3-GNN.

**Рис 12.6 – Добавление записи в таблицу маршрутизации маршрутизатора R3-GNN**

Маршрутизатор **R3-GNN** является транзитным, поэтому в него вводим информацию о всех сетях, к которым необходимо обеспечить доступ.

В данной таблицу должны быть следующие записи (адреса сетей, которые напрямую не связаны с данным маршрутизатором):

|  |  |  |
| --- | --- | --- |
| Номер сети | Адрес сети | Адрес шлюза |
| Сеть1 | 192.102.13.0 | 200.60.60.11 |
| Сеть 2 | 192.102.23.0 | 200.60.60.11 |
| Сеть 4 | 192.102.43.0 | 200.70.70.12 |

Таблицу маршрутизации можно формировать используя CLI с помощью команды ip route 192.168.13.0 255.255.255.0 200.60.60.11 для R3.

### Сформируйте таблицу маршрутизации для маршрутизатора R2 с помощью CLI.

Представте ScreenShot's для каждой записи.

### Просмотрите таблицу маршрутизации с помощью команды show ip route.

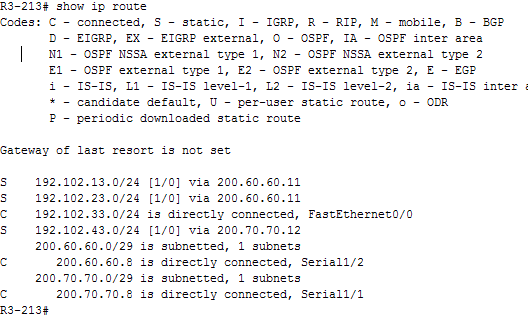
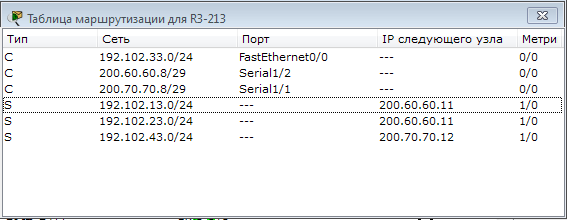
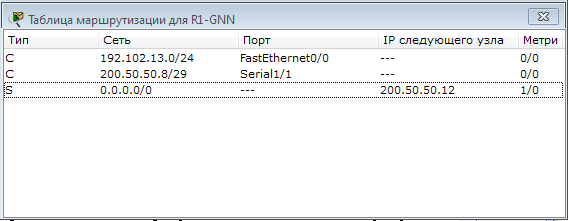
Таблица маршрутизации для маршрутизатора R3-GNN представлена на Рис12.7. Приведенные в распечатке значения [1/0] представляют собой "административное расстояние" и метрику.

Рис12.7 – Таблица маршрутизации R3-GNN

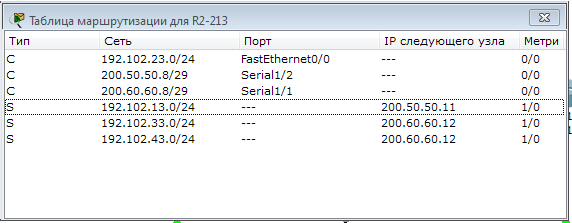
Данную таблицу можно получить другим способом – щелкнув на панели справа от рабочей области по значку , а затем по соответствующему маршрутизатору, выбрав в появившемся контекстном меню «Таблица маршрутизации».

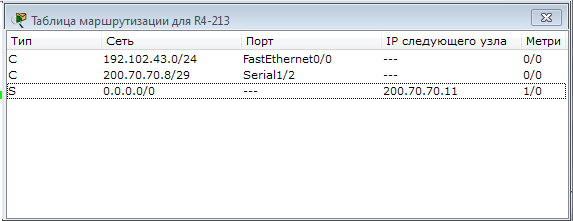
**Рис.12.8 – Таблица маршрутизации R3-GNN**

**2.7.3** Выполните пункты 5.2.1-5.2.3 для остальных маршрутизаторов.



**Рис.12.9 – Таблица маршрутизации R1-GNN**

**Рис.12.10 – Таблица маршрутизации R2-GNN**



**Рис. 12.11 – Таблица маршрутизации R4-GNN**

### Формирование таблицы для конечных маршрутизаторов

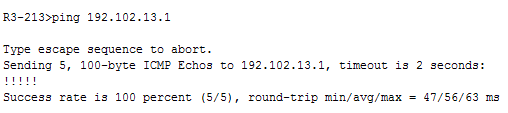
Для конечных маршрутизаторов можно сформировать таблицу с использованием маршрута по умолчанию. ip route 0.0.0.0 0.0.0.0 <ip address int> (ip –адресс внешнего интерфейса). В процессе конфигурирования маршрутизации по умолчанию в адресе и маске сети (и подсети) задействуют все **нули**, которые означают **все сети и все маски**. Подобная маршрутизация устанавливается для тупиковых маршрутизаторов, т. е. она может быть установлена для маршрутизаторов R1-GNN и R4-GNN (**Рис12.5**), потому что через них лежит единственный путь в составную сеть и из нее. Например, для всех пакетов, попавших в маршрутизатор R1-GNN, маршрут по умолчанию будет через его порт s1/1, т. е. шлюзом будет входной интерфейс маршрутизатора R2-GNN с адресом 200.50.50.12.

Сеть, т.е. компьютеры будет работать. Подайте команду с PC7-GNN на PC1-GNN, зафикструйте в ScreenShot’s. Попробуйте подать команду ping 192.102.13.1 с R4 в CLI- получите отрицательный результат.

Добавьте к существующим записям не обходимые записи для остальных сетей. Повторите ввод команды ping с R4 to R1 и наоборот. ScreenShot’s.

### Проверьте работоспособность сети и таблицы маршрутизации  с использованием команд ping и traceroute,

которые проверяют обеспечение IP-связи между маршрутизаторами и всей сети в целом.



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#12-GNN.pkt.

# Контрольные вопросы:

1. В чем заключается задача маршрутизации?
2. Что такое маршрутизатор?
3. Какие технологии используются маршрутизатором на физическом и канальном уровне? Дать краткую характеристику перечисленным выше технологиям.
4. Перечислите основные компоненты маршрута.
5. С помощью каких команд можно сконфигурировать маршрут по умолчанию?
6. Что такое административное расстояние? Перечислите его значения для нескольких видов маршрутизации.
7. Что такое петля маршрутизации? Как с ней бороться?
8. Что такое статическая маршрутизация? Что в ней обозначается буквами C и S?
9. Назовите шесть признаков относящихся к недостаткам статической маршрутизации
10. Назовите три положительных признака относящихся статической маршрутизации.
11. В каких случаях применяется статической маршрутизации.
12. Конструктивные особенности маршрутизатора Cisco 2811.
13. Что такое *NM-4A/S;?*
14. Найти в сети Интернет модули расширения для Cisco 2811 и привести их основные характеристики (3-5 модулей).
15. Какие команды нужно выполнить, что бы войти в привилегированный и глобальный режимы.
16. Приведите команды для конфигурации интерфейсов маршрутизатора Cisco.
17. Какими командами можно просмотреть конфигурацию интерфейсов.
18. Каким образом формируется таблица маршрутизации (показать Packet Tracer, также с помощью команды CLI);
19. Для чего необходим маршрут по умолчанию, как его установить.
20. Как проверить работоспобность сети?

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

Лабораторная работа № 13. Изучение протоколов динамической маршрутизации **RIP, OSPF** с использованием Packet Tracer 6 и маршрутизатора CISCO 2901.

**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 6.2. Получение практических навыков по настройке маршрутизаторов Cisco 2901.

# Основные сведения

Сетевой протокол IP является маршрутизируемым.

**Маршрутизация (routing)** – процесс определения маршрута следования информации в сетях связи.

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.

# 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.

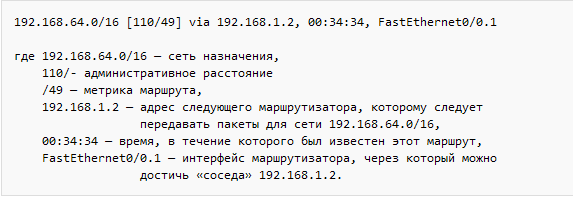
Например:

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.

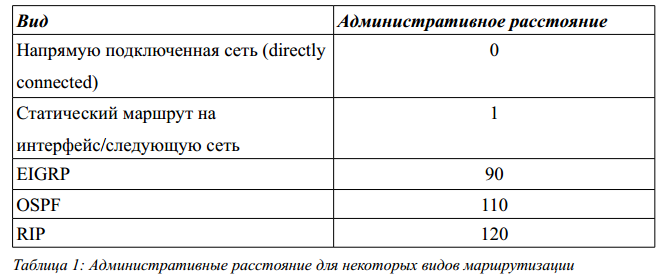
**Динамическая маршрутизация** (dynamic routing)— или адаптивная маршрутизация, когда записи в таблице обновляются автоматически при помощи одного или нескольких протоколов маршрутизации — **RIP, OSPF, IGRP, EIGRP, IS-IS, BGP**, и др.. Кроме того, маршрутизатор строит таблицу оптимальных путей к сетям 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.

# .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.

**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.

# 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:

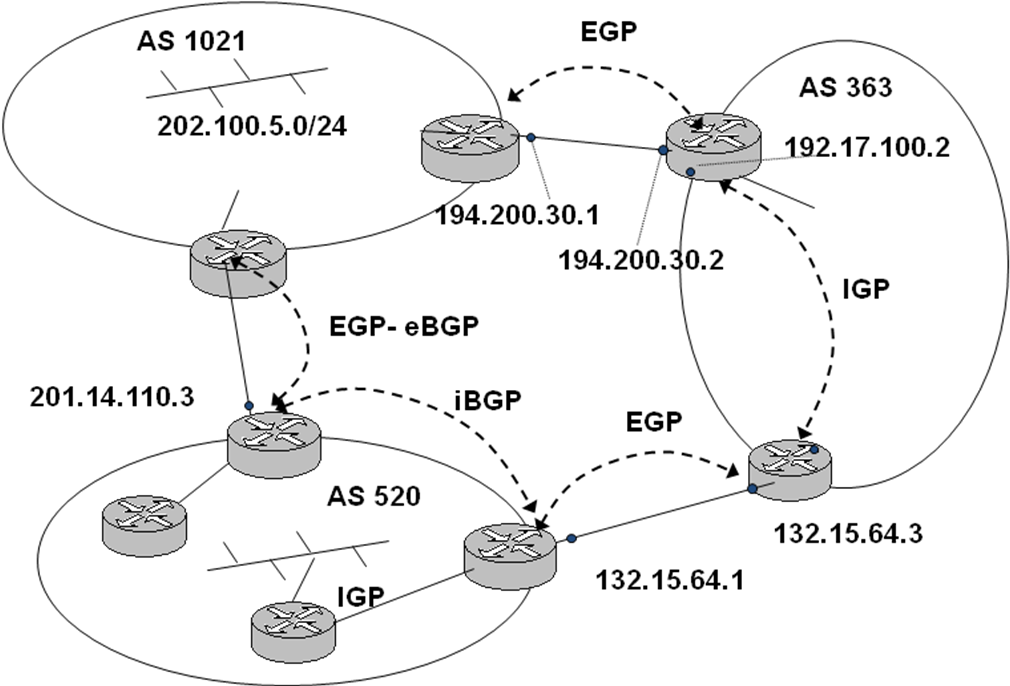
* Протоколы внешнего шлюза (Exterior Gateway Protocol EGP)- это протоколы маршрутизации, предназначенный для использования между автономными системами AS, управляемыми различными организациями. ***(под шлюзом имеется ввиду маршрутизатор)***
* Протокол внутреннего шлюза (Interior Gateway Protocol IGP) 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.

# Практическое выполнение задания:

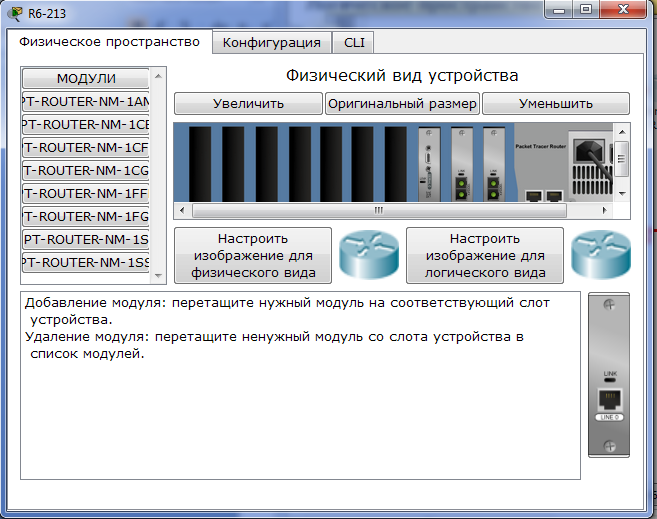
Для выполнения лабораторной работы используется ПО Cisco Packet Tracer.

Запустите программу Cisco Packet Tracer.

## 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.

* + 1. Откройте файл LR#12-GNN.pkt с помощью ПО Cisco Packet Tracer и сохраните его как LR#13-GNN.pkt.
    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.
    3. Установите модули расширения (установку выполнять при выключенном питании):
    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**.

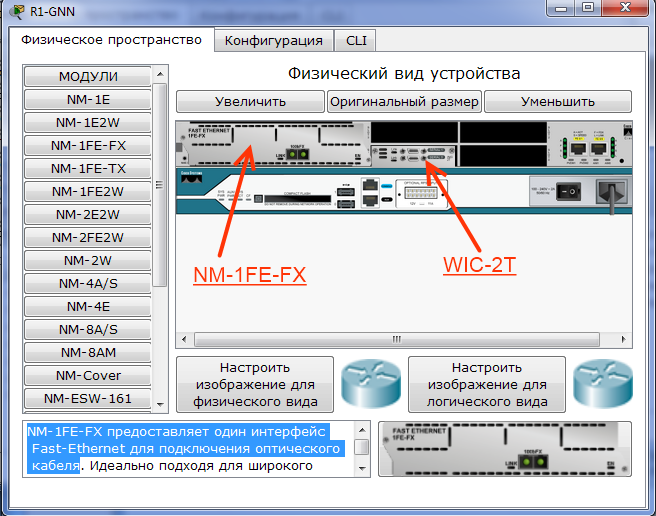
Рис.13.2. Установка модулей расширения в Маршрутизатор R6-GNN.

***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):***

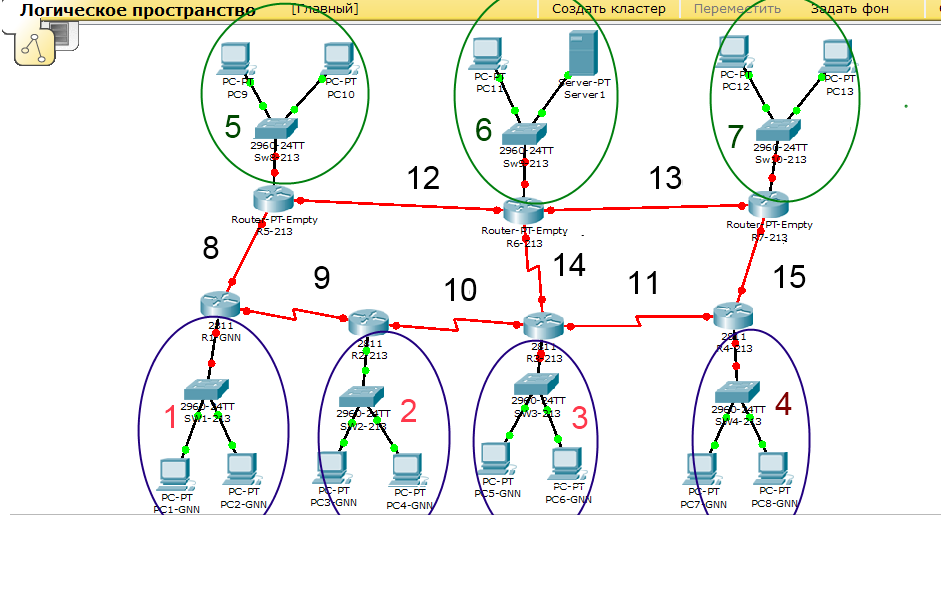
* Удалить модуль NM-4A/S, вместо него установить модуль NM-1FE-FX. NM-1FE-FX-предоставляет один интерфейс Fast-Ethernet для подключения ***оптического кабеля***;
* Установить модуль WIC-2T в слот 0/1, как показано на Рис 13.3. **Модуль WIC-2T 2-портовый** синхронный/асинхронный серийный сетевой модуль 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

* + 1. Включаем питание на всех устройствах, добавляем необходимые устройства, чтобы получить топологию сети, изображенную на Рис.13.4.
    2. Соединяем оптическим кабелем маршрутизаторы R1-R5, R4-R7, используя порты- интерфейсы Fast Ethernet. (оптические)
    3. Также оптическим кабелем соединяем маршрутизаторы R5-R6-R7 между собой, используя интерфейсы Gigabit Ethernet.
    4. Низкоскоростной интерфейс Serial Se2/0 Маршрутизатора R6 соединяем c 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

* + 1. После включения питания (на всех без исключени) необходимо изменить обозначения маршрутизаторов, согласно схемы Рис.13.4.
    2. 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).***

* + 1. 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),

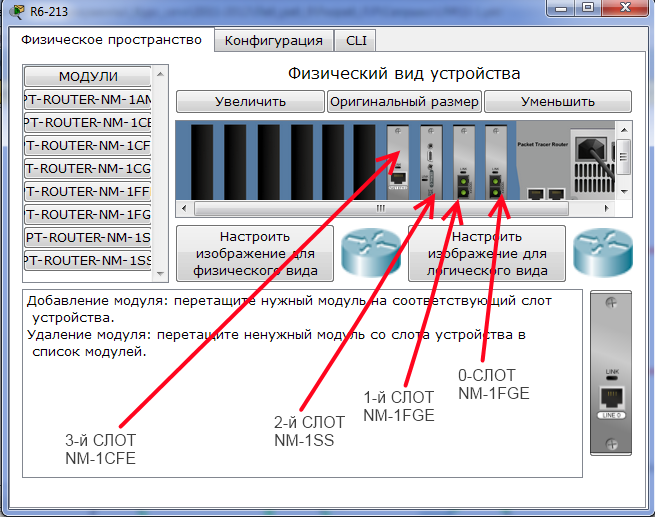
При выполнении конфигурации интерфейсов необходимо ***учитывать следующее:*** обозначение (нумерация) интерфейса зависит от места установки модуля расширения. Для **Router-PT-Empty** - например, для маршрутизатора R6-GNN, интерфейс F3/0, обозначает 3-й слот шасси, 0-й порт. (см. Рис 13.5).

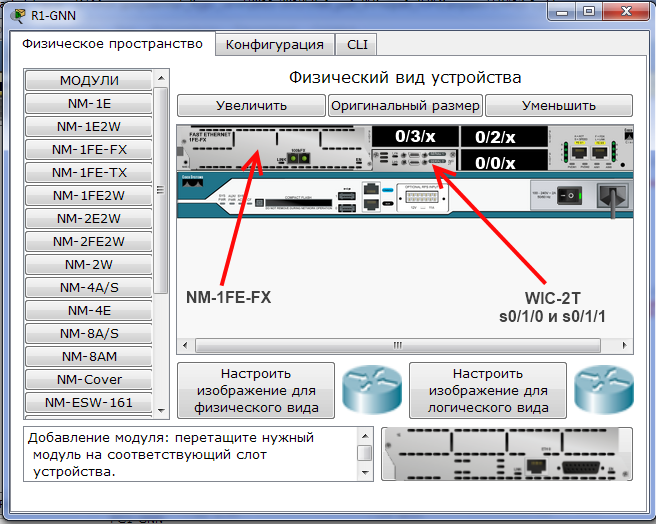
Рис.13.5 Расположение модулей расширения в маршрутизаторе R6-GNN.

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/х»** ─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***

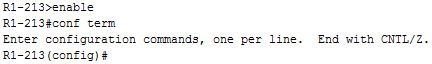
***Нумерация слотов/портов в маршрутизаторе CISCO 2811***

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

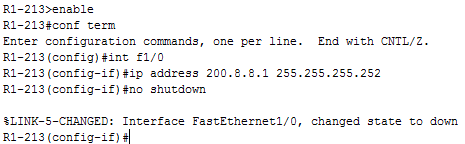
|  |  |  |  |
| --- | --- | --- | --- |
|  | **IP-адрес сети** | **Интерфейсы** | **IP-адрес интерфейса** |
| Сеть8 | 200.8.8.0/30 | F1/0 R1-GNN | 200.8.8.1 |
| F1/0 R5-GNN | 200.8.8.2 |
| Сеть9 | 200.9.9.0/30 | S0/1/1 R1-GNN | 200.9.9.1 |
| S1/2 R2-GNN | 200.9.9.2 |
| Сеть10 | 200.10.10.0/30 | S1/1 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 | F3/0 R6-GNN | 200.13.13.1 |
| F0/0 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 |
| F0/0-R7-GNN | 200.15.15.2 |

* + 1. Настройку IP-адресов интерфейсов маршрутизаторов, подключенных к сетям WAN со смежными маршрутизаторами проводить в соответствии с таблицей 13.2
    2. 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:
2. Далее вводим команду для входа в глобальный режим: *config terminal*.
3. Для того, чтобы отключить преобразование неправильно введенных команд в ip адрес или запрос DNS необходимо ввести команду ***no ip domain lookup***.

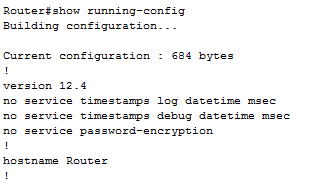
В глобальном режиме введите команду ***no ip domain lookup***

1. Для входа в режим детального конфигурирования интерфейса, используется команда interface или int, например для R1-GNN интерфейс, 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.

1. 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.***

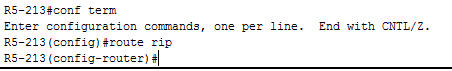
## Конфигурирование протокола RIP

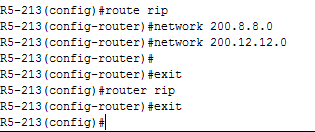
### Проверьте отключены статические маршруты на маршрутизаторах R1-R4, используя вкладку «конфигурация» и кнопки «маршрутизация»-> «статическая». Отключите все статические маршруты. Это также можно сделать с помощью команды no ip route, например:



* + 1. 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:

* + 1. Подключение соседних сетей.

Для запуска работы протокола RIP подключаем соседние сети:

* + 1. 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.

Рис.13.7 Просмотр таблицы маршрутизации на R7-213

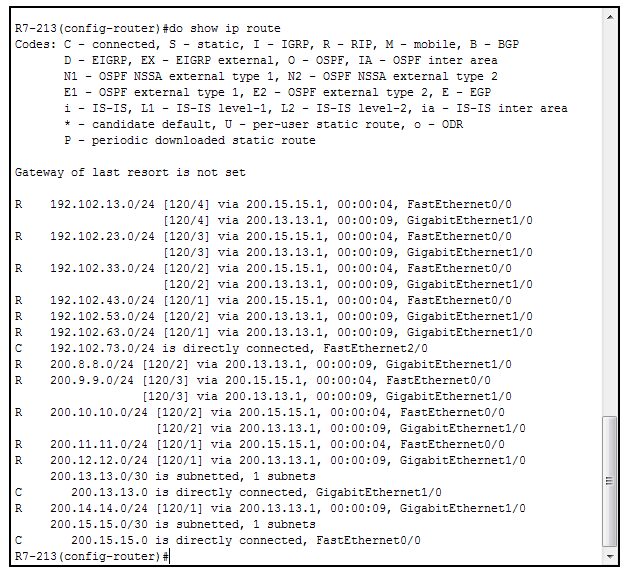
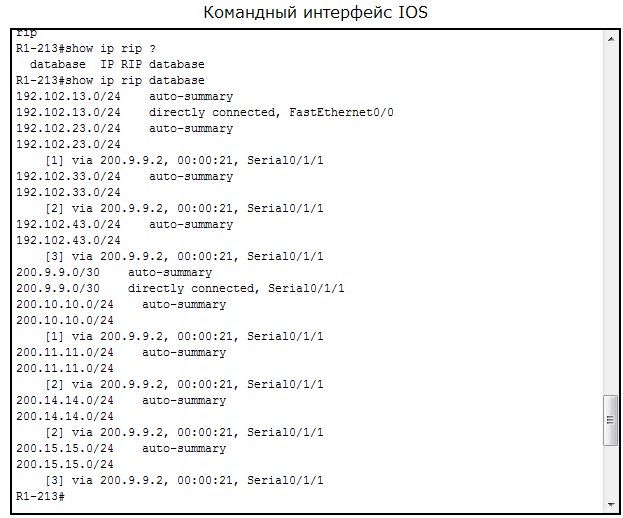
* + 1. Просмотр настроек протокола RIP. с помощью команды show ip rip

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

* + 1. Проанализируйте результаты. Анализ и Screen Shot's отразите в отчете.
    2. Добавьте маршрут по умолчанию для маршрутизатора R3-GNN

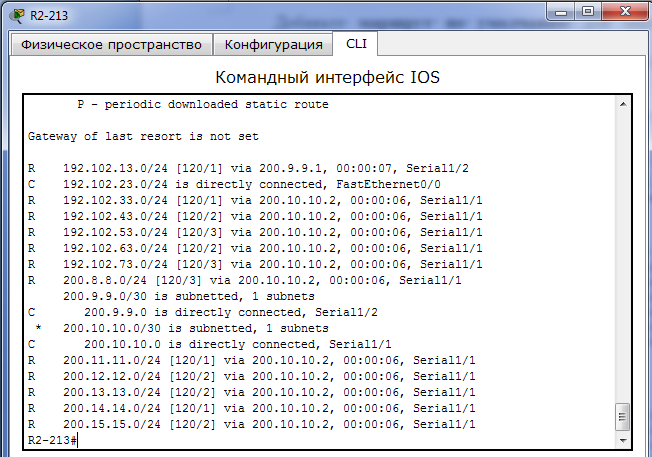
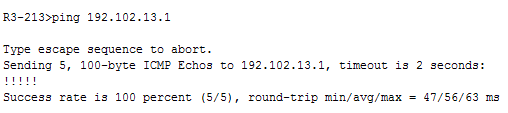
И просмотрите после этого с помощью команды *show ip route* таблицы маршрутизации маршрутизаторов R3-GNN и R2-GNN. Проанализируйте, что означают записи со звездочками. ***Анализ и Screen's отразите в отчете.***

Рис 13.9.Добавление маршрута по умолчанию

* + 1. Проверьте работоспособность сети и таблицы маршрутизации

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

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.

* + 1. 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.

* + 1. Сохраните файл рабочего макета под именем LR#13-RIP-GNN, для предоставления вместе с отчетом.

## Конфигурирование протокола OSPF

Рассмотрим базовое конфигурирование протокола OSPF.

* + 1. Откройте ранее сохранённый файл рабочего макета под именем LR#13-RIP-GNN и сохраните его под именем LR#13-OSPF-GNN
    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.

* + 1. Отключение RIP протокола на каждом маршрутизаторе.

Откройте вкладку CLI, войдите в глобальный режим конфигурирования и далее введите команду ***no router rip*** Убедитесь, что RIP протокол остановлен полностью с помощью команды ***show ip rip database.*** Должны получить пустую строку.

* + 1. 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)

* + 1. 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;

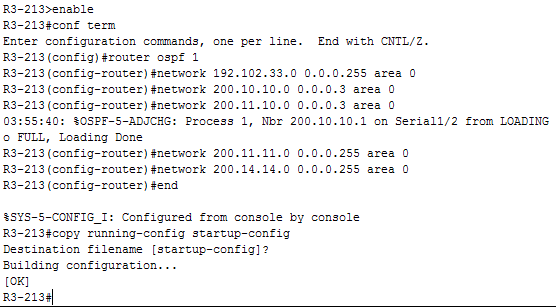
***area***- целочисленное число –идентификатор области AS, может быть в формате наподобие IP-адреса, т.е. десятичные 4-е цифры, разделенные точками.

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.

* + 1. Выполняем пункт 5.3.5 для всех маршрутизаторов сети.
    2. Проверим конфигурацию OSPF.

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

* + 1. Проверим таблицу конфигурации маршрутизатора.

с помощью команды show ip route. см.рис 13.11

* + 1. 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.

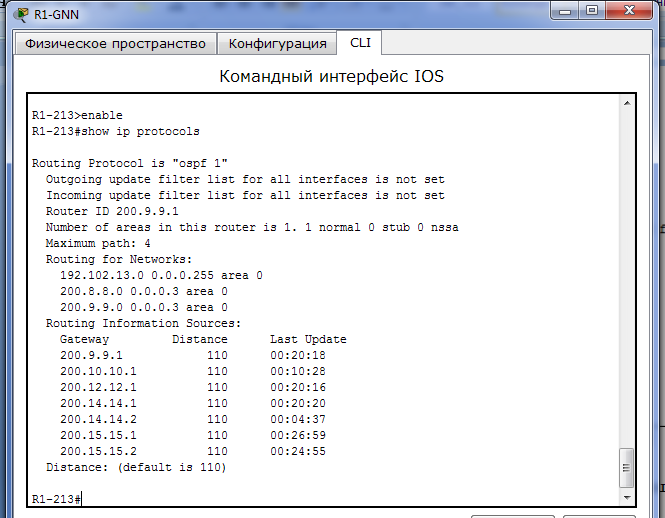
В отчете представить Screen Shot’s, а также пояснения и анализ работы сети.

Рис.13.10 Проверка конфигурации OSPF протокола.

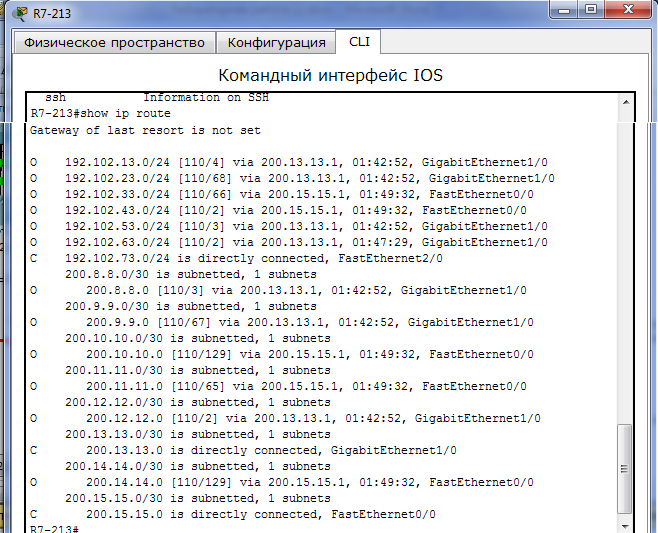


Рис 13.11 таблица конфигурации маршрутизатора с протоколом **ospf**

**Основные особенности, характеристики динамической маршрутизации.**

### Протокол RIP. (Routing Information Protocol)

**Протокол маршрутной информации (Routing Information Protocol — RIP*)***один изпервых 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 от маршрутизатора М-А маршрутизаторы М-Б и М-Г не могут посылать информа­цию 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.

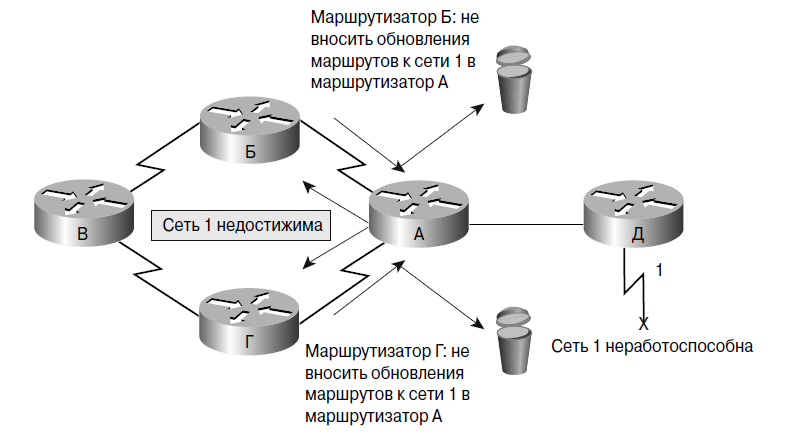


Рис 13.12 Образование петли и Расщепление горизонта

***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.

***Tаймеры 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. ) (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>

***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** –

(configrouter)#version {1 | 2},

* **Для конфигурации конкретного интерфейса:**

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

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

(configif)#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.)*** 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 А | 2 | 30-180-240 |  |
| 198.63.35.0 | Маршрутизатор В | 6 | 30-180-240 |  |
| 153.19.89.0 | Маршрутизатор С | 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.

### 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.

# 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. Tаймеры 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?**

# 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 самостоятель-ного изучения. СПб: СимволПлюс, 2003. – 512 с., ил.

Лабораторная работа № 14 Изучение протоколов глобальных сетей. Конфигурирование Frame Relay и статических маршрутов. Получение практических навыков по настройке маршрутизаторов Cisco 2901

**Цель работы:** Ознакомиться с принципами работы протоколов глобальных сетей на примере протокола Frame Relay и эмулятора CISCO Packet Tracer. Получение практических навыков по настройке маршрутизаторов Cisco 2901.

**Оборудование:** Персональный компьютер, включенный в сеть IP, Microsoft Windows, приложение CISCO Packet Tracer

# Основные сведения

CISCO Packet Tracer. - это визуальное моделирование сетей на основе оборудования CISCO: маршрутизаторов (1841, 2620XM, 2621XM, 2811), коммутаторов (2950-24, 2950Т, 2960), концентраторов, повторителей, беспроводных точек доступа, компьютеров, модемного Dial-up и WiFi соединения, DSL-модемов, кабельных модемов. Поддерживается эмуляция основных сетевых протоколов LAN, WAN: Ethernet, TCP/IP, ARP, **Frame Relay,** ICMP, HTTP, DHCP, TFTP, DNS и пр. Конфигурирование и настройка данного оборудования осуществляется через виртуальную консоль CLI (Command-Line Interface) в операционной системе IOS (Internetwork Operating System) или через графическое отображение в окне. ***Каждый тип оборудования включает в себе пустое шасси и ряд модулей, которые можно установить.***

# Протокол Frame Relay

## Общие сведения о технологии Frame Relay.

Разработкой и исследованием стандартов FR занимаются три организации:

1. ***Frame Relay Forum (FRF)*** - международный консорциум, включающий в себя свыше 300 поставщиков оборудования и услуг, среди которых 3Com, Northern Telecom, Digital, Cisco, Netrix, Ascom Tinieplex, Newbridge Networks, Zilog и др.;
2. ***American National Standards Institute (ANSI***, Американский национальный институт по стандартизации);
3. **Международный союз электросвязи (ITU-T).**

На сегодняшний день в глобальных сетях помимо IP технологии применяются технологии Frame Relay и ATM. Данные технологии объединяет то, что они ***основаны на технике виртуальных каналов***.

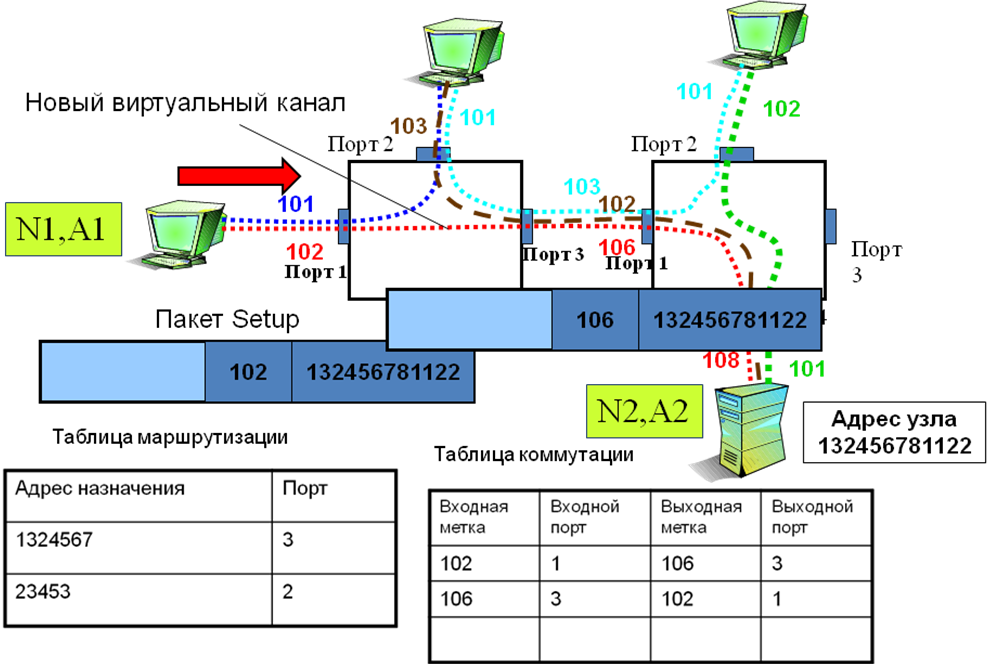


Рис. 14-1. Коммутация в глобальных сетях - техника виртуальных каналов.

1 этап – установление виртуального канала функциями 3-го уровня (X.25 в сетях X.25, Q.2931 в АТМ, Q.933 в FR)

Ранее широко применявшаяся технология Х.25, из-за избыточности и слишком больших накладных расходов практически не применяется и представляют, сегодня только исторический интерес

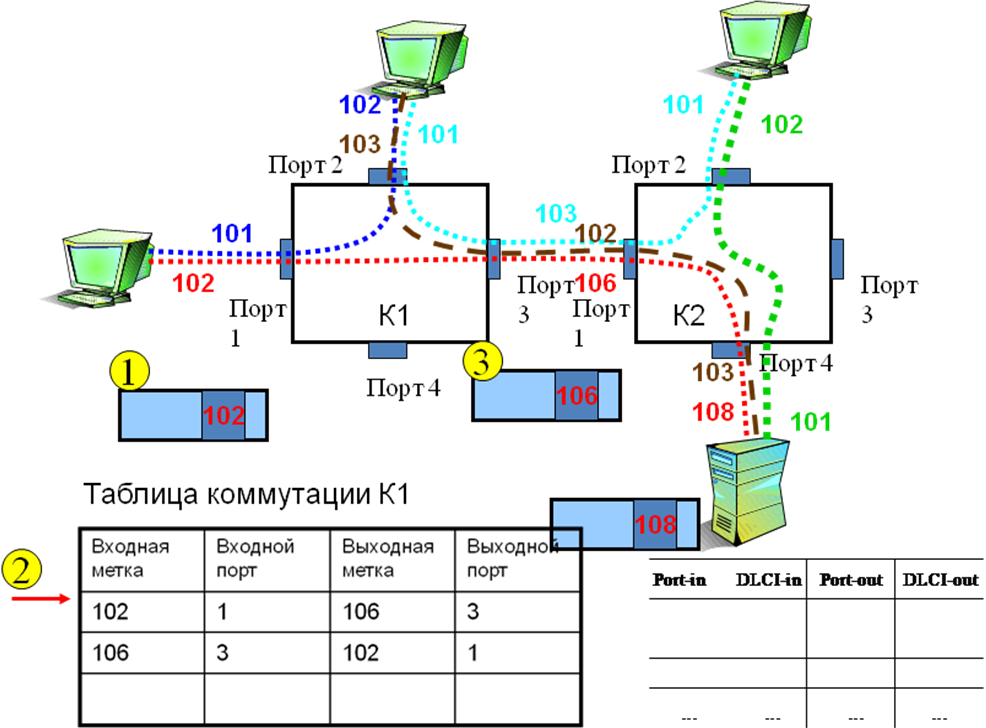


Рис. 14-2. Прохождение кадров FR по виртуальным каналам.

Протокол Frame Relay является одним из основных телекоммуникационных протоколов глобальных сетей с 1993 г. и поддерживается рядом стандартов: (I.122, ITU-T (Q.922,Q933); ANSI T1S1.2; RFC-1490, -1315, -1604). Сети Frame Relay ориентированы на передачу пульсирующего трафика компьютерных сетей и обеспечивают такую передачу лучше по сравнению с сетями Х.25. Frame Relay обеспечивает передачу данных на скоростях от 64k/s(56k/s) -до 2,048Mb/s(1,5Мбит/с), на практике применяется и на больших скоростях до 45Mb/s. Особенностью этой технологии является то что, она освобождена от многих избыточных функций, присущих Х.25, а выполняет только тот минимум, который необходим для доставки кадров адресату. Технология FR рассчитана на высокоскоростные и надежные цифровые каналы, которые стали широко применятся с середины 80-х годов. Протокол FR использует два уровня модели OSI: физический и канальный, тогда как X.25 ещё и сетевой. Остальные уровни должны реализоваться программно. Такая схема и минимальный набор функций заметно удешевляет интерфейс и позволяет передавать данные с меньшими накладными расходами. Frame Relay гарантирует большее быстродействие, чем X.25. **Протокол вводит понятие committed information rates (CIR - оговоренные скорости передачи), обеспечивая каждому приложению гарантированную полосу пропускания.** Если приложение не использует полностью выделенную полосу, другие приложения могут поделить между собой свободный ресурс.

Основанный на технологии виртуальных каналов FR, поддерживает как постоянные виртуальные каналы –PVC (Рис. 14-2), так и коммутируемые SVC (Рис. 14-1).

Для реализации протокола FR стандартом предусмотрено ряд протоколов, собранных в стек протоколов FR. Стек протоколов Frame Relay состоит из двух слоев: слоя управления и слоя данных:

* **Протоколы слоя управления (Control)** выполняют работу по установлению виртуального соединения - каналы SVC.
* **Протоколы слоя данных** передают кадры по уже установленному виртуальному соединению - каналы PVC и SVC. (см. Рис 14-3).

Протокол слоя данных LAP-F (Link Access Procedure or Frame mode bearer services) называемый в рекомендациях ITU-T аббревиатурой Q.922, соответствуют канальному уровню OSI. Существует две версии протокола LAP-F:

* Протокол **LAP-F core** является основным во всех сетях Frame Relay. Этот протокол обеспечивает минимум средств, но в этом случае сеть будет предоставлять только услуги постоянных виртуальных каналов PVC.
* Протокол **LAP-F control**, обеспечивающий восстановление кадров по алгоритму скользящего окна, необходим для того, чтобы сеть оказывала услуги Frame Switching (коммутации кадров).

Протокол LAP-F (стандарт Q.922 ITU-T) работает на любых каналах сети ISDN, а также на каналах типа T1/E1.

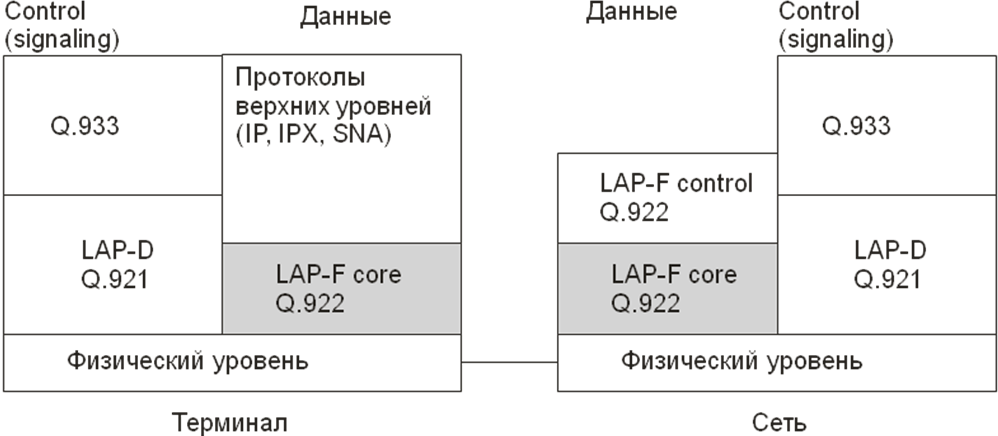


Рис. 14-3. Cтек протоколов технологий Frame Relay и Frame Switching

Терминальное оборудование посылает в сеть кадры LAP-F, в любой момент времени считая, что виртуальный канал в сети коммутаторов уже проложен. При использовании PVC оборудованию Frame Relay нужно поддерживать только протокол LAP-F core.

Особенностью технологии Frame Relay при использовании LAP-F core, является отказ от коррекции обнаруженных в кадрах искажений. В этом режиме (LAP-F core), который фактически практикуется в сегодняшних сетях Frame Relay, кадры передаются без преобразования и контроля, как и в коммутаторах локальных сетей. Протокол Frame Relay подразумевает, что конечные узлы будут обнаруживать и корректировать ошибки за счет работы протоколов транспортного или более высоких уровней. За счет этого сети Frame Relay обладают весьма высокой производительностью, так как кадры в коммутаторах не подвергаются преобразованию, а сеть не передает квитанции подтверждения между коммутаторами на каждый пользовательский кадр, как это происходит в сети Х.25. Пульсации трафика передаются сетью Frame Relay достаточно быстро и без больших задержек.

## Структура кадров Frame Relay.

Структура кадров Frame Relay основана на протоколе LAP-D*/*HDLC, но имеются отличия: поле адреса существенно изменило свой формат, а поле управления вообще отсутствует. Новый заголовок Frame Relay имеет длину 2 байта (16 битов) и использует следующий формат:

**Рис. 14.4.** Формат кадра LAP-F

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
| DLCI (старшая часть) | | | | | | C/R | EA |
| DLCI (младшая часть) | | | | FECN | BECN | DE | EA |

**Рис14.5.** Двух- байтовый заголовок кадра Frame Relay (адрес)

**Флаг**

Поля флагов обозначают начало и конец каждого кадра. Все кадры начинаются и заканчиваются комбинацией "флаг": "01111110b"- 0x7e. С целью предотвращения имитации комбинации "флаг" при передаче кадра проверяется все его содержание между двумя флагами и вставляется бит "0" после каждой последовательности, состоящей из пяти идущих подряд бит "1". Данная процедура (bit stuffing) обязательна при формировании любого кадра FR. На приемном конце биты "0" отбрасываются

**Заголовок**

Двухбайтовый заголовок содержит ряд полей, назначение которых описано ниже:

***Поле DLCI (Data Link Connection Identifier)***

10-битовое поле DLCI, разделенное на две части (6 и 4 бита), является важнейшей частью заголовка кадра Frame Relay. DLCI представляют собой идентификатор канала передачи данных, определяют абонентский адрес в сети FR; и адресует логическое соединение, мультиплексируемое в физический канал. В базовом варианте Frame Relay (без расширения LMI) значение DLCI имеет локальный смысл, т.е. два устройства на разных концах одного соединения могут использовать разные значения DLCI для общего виртуального канала. Базовый размер поля DLCI позволяет задействовать до 1024 виртуальных соединений. Для оконечных устройств пользователя отводится только 976 DLCI-адресов. Определенные номера являются служебными. Согласно стандартам адресное пространство DLCI распределяется следующим образом:

* 0 - используется для виртуального канала локального интерфейса администрирования (LMI);
* 1-15 — зарезервированы;
* 16-991 — используются абонентами для нумерации каналов PVC и SVC;
* 992-1007 — используются сетевой транспортной службой;
* 1008-1022 - зарезервированы;
* 1023 — используется для управления канальным уровнем.

Frame Relay (FR) предусматривает 2-х (базовый), 3-х и 4-х байтовые форматы заголовков (Стандарты ANSI T1.618 и ITU-T Q.922) и синхронную передачу данных.

***Однобитовое поле(EA - Extended Address)***

***EA*** - бит расширения адреса. DLCI содержится в 10 битах, входящих два октета заголовка. Однако возможно расширение заголовка на целое число дополнительных октетов с целью расширения адреса, состоящего более чем из 10 бит. EA устанавливается в конце каждого октета заголовка; если он имеет значение "1", то это означает, что данный октет в заголовке последний. Стандарт FRF рекомендует использовать заголовки, состоящие из 2 октетов. В этом случае значение бита EA первого октета будет соответствовать "0", а второго - "1";

***Однобитовое поле C/R***

Обозначает тип кадра - команда (command) или отклик (response). Этот  
признак является унаследованным и используется в протокольных операциях HDLC. Зарезервировано для возможного применения в различных протоколах более высоких уровней управления узлами FR. Этот бит не используется базовым протоколом FR и "прозрачно пропускается" аппаратно-программными средствами сети FR;

***Однобитовые поля FECN и BECN.***

Бит прямого уведомления FECN (Forward Explicit Congestion Notification) и бит обратного уведомления BECN (Backward Explicit Congestion Notification) используются для оповещения пользовательских устройств о явных перегрузках в линии. Для поля **FECN (прямое явное уведомление о насыщении)** устанавливается значение «**1»** в кадрах, передаваемых в направлении от источника к получателю (downstream) при возникновении перегрузки на пути передачи данных. В этом случае все узлы нисходящего потока и подключенные к ним пользовательские устройства узнают о насыщении (перегрузки) в линии.

Поле - бит **BECN (обратное явное уведомление о насыщении)** - устанавливается значение «**1»** сетью Frame Relay в кадрах, передаваемых в направлении, обратном тому, где возникает насыщение.

Оба бита индикации насыщения позволяют протоколам вышележащих уровней принять соответствующие меры по управлению потоком данных. Эти уведомления говорят отправителю о необходимости снижения скорости передачи данных.

***Поле –бит (DE - Discard Eligibility) Возможность отбрасывания.***

бит разрешения сброса (Discard Eligibility - DE) устанавливается в "1" в случае явной перегрузки и указывает на то, что данный кадр может быть уничтожен в первую очередь. Бит DE устанавливает либо АКД, либо ООД (т. е. пользователю предоставлено право выбирать, какими кадрами он может "пожертвовать"). Однако при перегрузках узлы коммутации сети FR уничтожают не только кадры с битом DE.

***Поле Data (Информационное поле)***

содержит данные пользователя и состоит из целого числа октетов. Его максимальный размер определен стандартом FRF и составляет 1600 октетов, минимальный размер - 1 октет, но возможны и другие максимальные размеры (вплоть до 4096 октетов) Содержание информационного поля пользователя передается неизменным.

***Поле (Frame Check Sequence - FCS)***

***FCS*** - Проверочная последовательность кадра используется для обнаружения возможных ошибок при его передаче и состоит из 2 октетов. Данная последовательность формируется аналогично циклическому коду HDLC.

Все указанные поля должны присутствовать в каждом кадре FR, который передается между двумя оконечными пользовательскими системами.

Одним из основных отличий протокола FR от HDLC является то, что он не предусматривает передачу управляющих сообщений (нет командных или супервизорных кадров, как в HDLC). Для передачи служебной информации используется специально выделенный канал сигнализации. Другое важное отличие - отсутствие нумерации последовательно передаваемых (принимаемых) кадров. Дело в том, что протокол FR не имеет никаких механизмов для подтверждения правильно принятых кадров.

## Поддержка качества обслуживания

В технологию Frame Relay изначально на уровне стандартов определены параметры качества обслуживания, которые может заказать пользователь, заключив соглашение с провайдером FR. Такое соглашение обычно называется «Типовым соглашение об уровне обслуживания – SLA (Service Level Agreement)».

Для каждого виртуального соединения стандартом определяется несколько параметров, влияющих на качество обслуживания.

**CIR** (Committed Information Rate)- согласованная информационная скорость, с которой сеть будет передавать данные пользователя.

**Bс** (Committed Burst Size)- согласованный объем пульсации, то есть максимальное количество байтов, которое сеть будет передавать от этого пользователя за интервал времени Т.

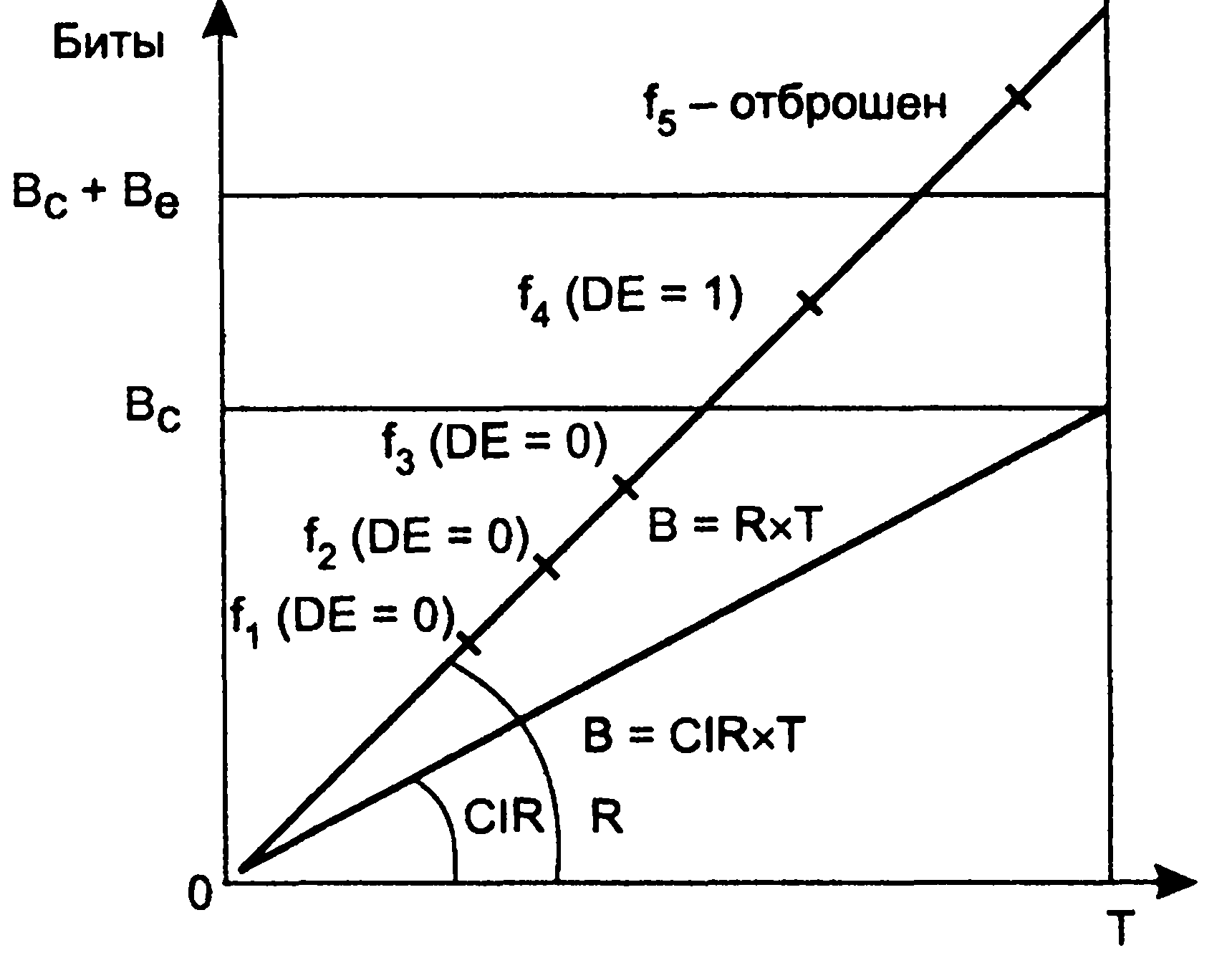
**Be** (Excess Burst Size)- дополнительный объем пульсации, то есть максимальное количество байтов, которое сеть будет пытаться передать сверх установленного значения Вс за интервал времени Т.

Если эти величины определены, то время Т определяется формулой: Т =Bс/CIR.

Обычно для контроля пульсаций трафика выбирается время Т равное 1 -2 секунды при передаче данных, и в диапазоне десятков-сотен миллисекунд при передаче голоса.

Соотношение между параметрами CIR, Bc, Be и Т иллюстрирует рис. 14-6 (R —скорость в канале доступа; f1-f5 — кадры).

Основным параметром, по которому абонент и сеть заключают соглашение при  
установлении виртуального канала, является согласованная скорость передачи данных. Для постоянных виртуальных каналов это соглашение является частью контракта на пользование услугами сети. При установлении коммутируемого виртуального канала SVC соглашение о качестве обслуживания заключается автоматически с помощью протокола Q.933 — требуемые параметры CIR, Вс и Bе передаются в пакете запроса на установление соединения.

**Рис.** 14.6. Реакция сети на поведение пользователя

Скорость передачи данных измеряется на контрольном интервале времени Т, на котором проверяются условия соглашения. В общем случае пользователь не должен в этом интервале передавать в сеть данные со средней скоростью, превосходящей CIR. Если же он нарушает соглашение, то сеть не гарантирует доставку кадра и помечает этот кадр признаком готовности к удалению (Discard Eligibility, DE), равным “**1”**. Однако кадры, отмеченные таким признаком, удаляются из сети только в том случае, если коммутаторы сети испытывают перегрузки. Если же перегрузок нет, то кадры с признаком DE = 1 доставляются адресату.

Такое щадящее поведение сети соответствует случаю, когда общее количество данных, переданных пользователем в сеть за период Т, не превышает значения Вс + Be. Если же этот порог превышен, то кадр не помечается признаком DE, а немедленно удаляется.

Рисунок 14.6. иллюстрирует случай, когда за интервал времени Т в сеть по виртуальному каналу поступило 5 кадров Средняя скорость поступления данных в сеть составила на этом интервале R бит/с. и она оказалась выше CIR. Кадры f1, f2 и f3 доставили в сеть данные, суммарный объем которых не превысил порог Вс, поэтому эти кадры ушли дальше транзитом с признаком DE = 0. Данные кадра f4 прибавленные к данным кадров f1, f2 и f3, уже превысили порог Вс, но еще не превысили порога Вс + Be, поэтому кадр f4 также ушел дальше, но уже с признаком DE=1. Данные кадра f5, прибавленные к данным предыдущих кадров, превысили порог Вс + Be, поэтому этот кадр был удален из сети.

Для контроля соглашения о параметрах качества обслуживания все коммутаторы сети Frame Relay поддерживают алгоритм «дырявого ведра» (leaky bucket). Этот алгоритм относится к классу алгоритмов «ведра маркеров». Он позволяет контролировать среднюю скорость и пульсацию трафика и является более жестким, чем ведро маркеров.

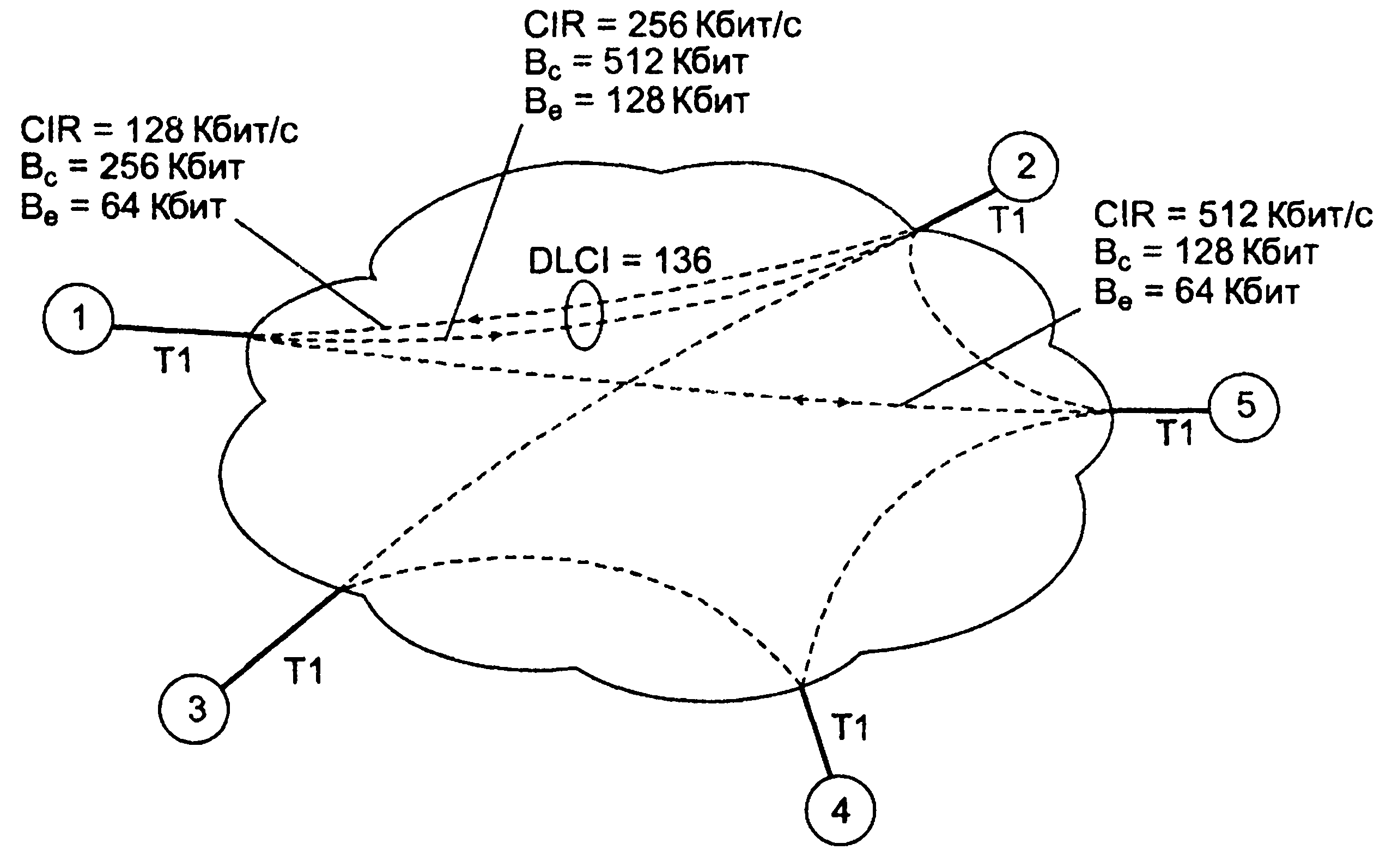
Алгоритм поддерживает счетчик С поступивших от пользователя байтов. Каждые Т секунд этот счетчик уменьшается на величину Вс (или же сбрасывается в 0, если значение счетчика меньше, чем Вс). Все кадры, данные которых не увеличили значение счетчика свыше порога Вс, пропускаются и сеть со значением признака DE = 0. Кадры, данные которых привели к значению счетчика, большему Вс, но меньшему Вс + Be, также передаются в сеть, но уже с признаком DE = 1. И наконец, кадры, которые привели к значению счетчика, большему Вс + Be, отбрасываются коммутатором.

Пользователь может договориться о поддержании не всех параметров качества обслуживания для данного виртуального канала, а только некоторых.

Например, можно использовать только параметры CIR и Вс. Этот вариант дает более качественное обслуживание, так как кадры никогда не отбрасываются коммутатором сразу. Коммутатор только помечает кадры, которые превышают порог Вс за время Т, признаком DE = 1. Если сеть не сталкивается с перегрузками, то кадры такого канала всегда доходят до конечного узла, даже если пользователь постоянно нарушает договор с сетью.

Популярен еще один вид заказа на обслуживание, при котором оговаривается только порог Be, а скорость CIR полагается равной нулю. Все кадры такого канала сразу же отмечаются признаком DE = 1, но отправляются и сеть, а при превышении порога Bе отбрасываются. Алгоритм ведра маркеров разрешает трафику и периоды пониженной активности накапливать объем пульсации, а затем использовать эти накопления в периоды всплесков трафика. В алгоритме дырявого ведра такой возможности нет, так как счетчик С сбрасывается в ноль принудительно в конце каждого периода Т независимо от того, сколько байтов поступило от пользователя в сеть в течение этого периода.

На рис. 14.7 приведен пример сети Frame Relay с пятью удаленными региональными отделениями корпорации.

**Рис.** 14.7. Пример обслуживания в сети Frame Relay****

Обычно доступ к сети осуществляется по каналам с пропускной способностью, большей, чем CIR. Но при этом пользователь платит не за пропускную способность канала, а за заказанные величины CIR, Вс и Be. Так, при использовании в качестве линии доступа канала E1 и заказа обслуживания со скоростью CIR. равной 128 Кбит/с, пользователь будет платить только за скорость 128 Кбит/c, а скорость канала E1 в 2,048 Мбит/с окажет влияние на верхнюю границу возможной пульсации Вс + Be.

Параметры качества обслуживания могут быть разными для разных направлений виртуального канала. Так, на рисунке абонент 1 соединен с абонентом 2 виртуальным каналом с DLCI = 136. При направлении от абонента 1 к абоненту 2 канал имеет среднюю скорость 128 Кбит/с с пульсациями Вс = 256 Кбит (интервал Т составил 1 с) и Be = 64 Кбит. А при передаче кадров в обратном направлении средняя скорость уже может достигать значения 256 Кбит/с с пульсациями Вс = 512 Кбит и Вс = 128 Кбит.

Механизм резервирования средней пропускной способности и максимальной пульсации является основным механизмом обеспечением параметров QoS в сетях Frame Relay.

В технологии Frame Relay **определен еще и дополнительный** (необязательный) механизм управления потоком. Это механизм оповещения конечных пользователей о том, что в коммутаторах сети возникли перегрузки (переполнение необработанными кадрами). **Бит FECN** (Forward Explicit Congestion Notification - прямое явное уведомление о перегрузке) кадра извещает об этом принимающую сторону. На основании значения этого бита принимающая сторона должна с помощью протоколов более высоких уровней (TCP/IP, SPX и т. п.) известить передающую сторону о том, что та должна снизить интенсивность отправки пакетов в сеть.

**Бит BECN** (Backward Explicit Congestion Notification — обратное явное уведомление о перегрузке) извещает о переполнении в сети передающую сторону и является рекомендацией немедленно снизить скорость передачи. Бит BECN обычно отрабатывается на уровне устройств доступа к сети Frame Relay — маршрутизаторов, мультиплексоров и устройств CSU/DSU. Протокол Frame Relay не требует от устройств, получивших кадры с установленными битами FECN и BECN, немедленного прекращения передачи в данном направлении, как, например, происходит в сетях Х.25. Эти биты должны служить указанием для протоколов более высоких уровней (TCP, SPX, NCP и т. п.) о снижении темпа передачи пакетов. Так как регулирование потока и принимающей, и передающей сторонами инициируется в разных протоколах по-разному, то разработчики протоколов Frame Relay учли оба направления снабжения предупреждающей информацией о переполнении сети.

## Коммутируемый виртуальный канал.

При создании коммутируемого виртуального канала параметры качества обслуживания передаются в сеть с помощью протокола Q.931. Этот протокол устанавливает виртуальное соединение с помощью нескольких служебных пакетов.

Абонент сети frame relay, который хочет установить коммутируемое виртуальное соединение с другим абонентом, должен передать в сеть по каналу D (если используется сеть ISDN) сообщение SETUP, которое имеет несколько параметров, в том числе:

* DLCI;
* адрес назначения (в формате Е.164, Х.121 или ISO 7498) (аналогичен телефонному номеру в международном формате- в данном сл. Номер сети + номер абонента);
* максимальный размер кадра в данном виртуальном соединении;
* запрашиваемое значение CIR для двух направлений;
* запрашиваемое значение Вс для двух направлений;
* запрашиваемое значение Be для двух направлений.

Коммутатор, с которым соединен пользователь, сразу же передает пользователю пакет CALL PROCEEDING - вызов обрабатывается. Затем он анализирует параметры, указанные в пакете, и если коммутатор может их удовлетворить (располагая, естественно, информацией о том, какие виртуальные каналы на каждом порту он уже поддерживает), то пересылает сообщение SETUP следующему коммутатору. Следующий коммутатор выбирается по таблице маршрутизации. Протокол автоматического составления таблиц маршрутизации для технологии frame relay не определен, поэтому может использоваться фирменный протокол производителя оборудования или же ручное составление таблицы. Если все коммутаторы на пути к конечному узлу согласны принять запрос, то пакет SETUP передается в конечном счете вызываемому абоненту. Вызываемый абонент немедленно передает в сеть пакет CALL PROCEEDING и начинает обрабатывать запрос. Если запрос принимается, то вызываемый абонент передает в сеть новый пакет - CONNECT, который проходит в обратном порядке по виртуальному пути. Все коммутаторы должны отметить, что данный виртуальный канал принят вызываемым абонентом. При поступлении сообщения CONNECT вызывающему абоненту он должен передать в сеть пакет CONNECT ACKNOWLEDGE.

Сеть также должна передать вызываемому абоненту пакет CONNECT ACKNOWLEDGE, и на этом соединение считается установленным. По виртуальному каналу могут передаваться данные. Далее данные передаются по протоколу LAP-F.

## Интерфейс локального управления (LMI).

Интерфейс локального управления (LMI) является расширением базового стандарта Frame Relay, разработанный международный консорциум ***Frame Relay Forum (FRF)***, при активном участии корпорации CISCO и др. корпораций.

LMI интерфейс был разработан, в первую очередь, с целью предоставления пользователю информации о состоянии и конфигурации PVC. LMI применяется только в оконечном аппаратно-программном обеспечении пользователя и выполняет следующие функции:

* Определения оперативного состояния различных PVC: уведомление абонента о включении, наличии и отключении PVC;
* Информирование маршрутизатора о доступных PVC; (уведомление абонента о готовности заранее сконфигурированного PVC);
* последовательный опрос сетевых устройств для подтверждения целостности соединения;
* возможность активизации трех типов LMI (в зависитмости от разных стандартов) командами маршрутизатора, например для CISCO: ansi, cisco и q933a.

Данные функции являются основными, их назначение и выполнение заключаются в следующем, а именно: Сообщения о состоянии виртуального канала (основная функция) обеспечивают обмен информацией и синхронизацию между сетью и устройством пользователя. Такие сообщения периодически предоставляют данные об образовании новых и удалении уже существующих постоянных виртуальных каналов, а также обычно информируют об их целостности. Сообщения о состоянии виртуального канала предотвращают пересылку данных "в никуда", т.е. по исчезнувшим постоянным виртуальным каналам.

Спецификация LMI по мимо основных функций вкдючает и дополнителные:

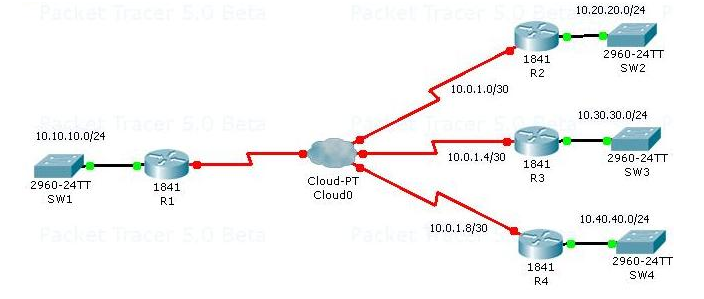
1. **Многоадресатная передача** (дополнительная функция) позволяет отправителю передать один фрейм нескольким адресатам в сети. Многоадресатная передача поддерживает эффективную транспортировку сообщений протокола маршрутизации и работу процедур разрешения адресов, в процессе которой обычно необходимо одновременно рассылать сообщения во многие места назначения.
2. **Глобальная адресация** (дополнительная функция) придает идентификаторам соединений глобальную значимость, что позволяет им идентифицировать конкретный интерфейс сети Frame Relay. Глобальная адресация придает сети Frame Relay сходство с адресацией в локальной сети (т.е. LAN). В результате протоколы разрешения адресов работают в сети Frame Relay точно так же, как и в сети LAN.
3. **Простое управление потоками** (дополнительная функция) обеспечивает работу механизма контроля потока сообщений XON/XOFF, который взаимодействует со всем интерфейсом Frame Relay33. Этот механизм предназначен для устройств, высшие уровни которых не могут использовать биты уведомления о возникновении перегрузки, и поэтому им нужен определенный уровень управления потоком.

Для LMI используются определенные DLCI адреса: “0” или “1023” в зависимости от стандарта.

# Практическое выполнение Конфигурирование корпоративной сети с помощью эмулятора Packet Tracer.

## Исходные данные и указания

Четыре маршрутизатора должны быть связаны в виде звездообразной Frame Relay архитектуры (in a hub-and-spoke Frame Relay configuration), в которой R1 должен быть центром (hub- звезды), а маршрутизаторы R2, R3, и R4 – ее лучами (spoke routers) (англ. spoke -спица). Frame Relay соединения должны устанавливаться с применением соединения типа point-to-point от подынтерфейсов R1 до каждого spoke маршрутизатора. Маршрутизация будет строиться с использованием статических маршрутов на hub маршрутизаторе и маршрутов по умолчанию на всех spoke маршрутизаторах. Frame Relay коммутатор(ы) конфигурируются в пределах облака (cloud). Далее к каждому маршрутизатору подключается коммутатор –swith для конкретной подсети. На Рис. 14.5.указаны IP адреса для примера. **При выполнении, IP адреса и DLCI выбираются согласно варианта.** На заключительном этапе необходимо к каждому коммутатору подключить оконечное оборудование – рабочую станцию. На коммутаторе SW1 помимо рабочей станции подключается сервер DNS и сервер Web.

Рис. 14.5. Схема включения сетевого оборудования корпоративной сети.

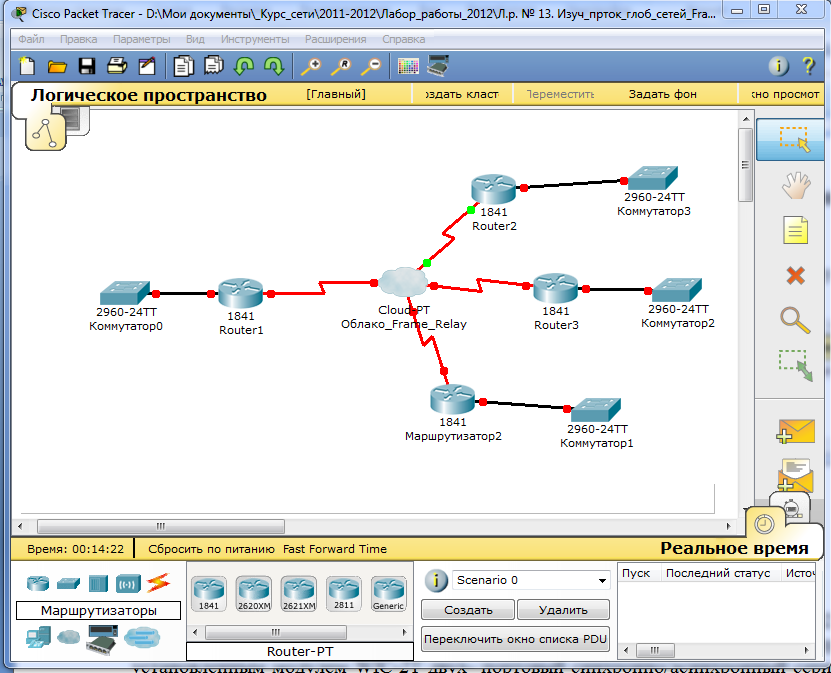


Рис. 14.6. Рабочее окно программного эмулятора Cisco Packet Tracer

## Задача 1: Создание схемы корпоративной сети с использованием Packet Tracer согласно исходным данным.

Шаг 1. ***Создание «облака Frame Relay»***

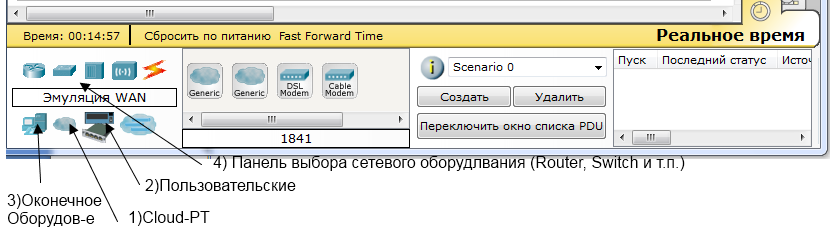
На панели оборудования Packet Tracer (в левом нижнем углу) выбираем «Эмуляцию WAN - Cloud-PT» и перетаскиваем в окно «Логическое пространство». Рис 14.7 «1)»

Рис 14.7. Панели выбора и отображения типа оборудования CISCO.

Шаг 2 ***Установка магистральных маршрутизаторов***.

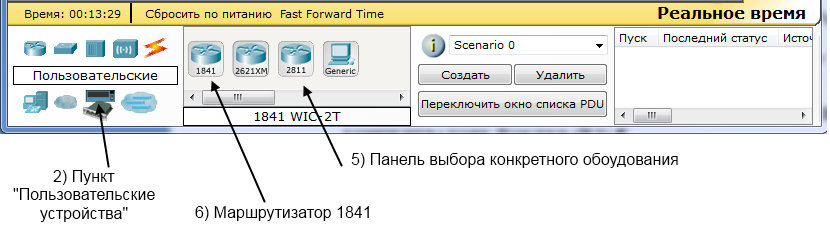
 На той же панели выбираем «Пользовательское устройство» -Рис 14.8 -«2)». На панели выбора конкретного типа оборудования -«5)» выбираем маршрутизатор 1841 с предварительно установленным модулем WIC-2T двух- портовый синхронно/асинхронный серийный модуль. Данное оборудование можно выбрать и на панели выбора сетевого оборудования Рис 14.7 «4)», но без установленных модулей.

Рис 14.8. Панели выбора и отображения конкретного оборудования CISCO.

Перетаскиваем в окно «Логическое пространство».

Шаг 3. Аналогично устанавливаем в окне «Логическое пространство» ещё три маршрутизатора 1841 согласно схеме Рис 14.6.

***Шаг 4.*** ***Соединение магистрального сетевого оборудования***.

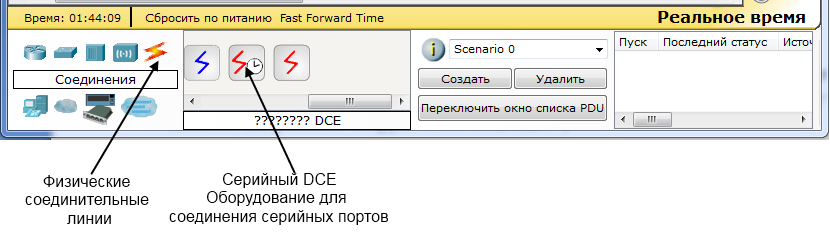
Установленное на «Логическом пространстве» сетевое оборудование необходимо соединить физическими линиями (каналами). Для данного выбранного оборудования подходит «Серийный DCE».

Рис 14.9. Выбор физических соединительных линий и коммутационных устройств.

Выбрав «Серийный DCE», щелкаем левой клавишей мыши по объекту «Cloud-PT» и в появившимся списке свободных портов выбираем Serial (например для router R1- Serial0). Далее соединяем объект «Cloud-PT» c «R1» и аналогично выбираем порт R1 типа Serial – Serial0/0/0.

Таким же образом соединяем роутеры R2, R3, R4 с Cloud-PT.

***Шаг 5. Установка коммутаторов CISCO 2960***

Мы должны соединить три независимых локальных сети LAN#n с LAN#1 С этой целью на панели «тип оборудования» Рис 3.7 «4)» выбираем коммутаторы (switch) и далее на панели «конкретное сетевое оборудование» выбираем коммутатор 2960 и устанавливаем напротив роутера- R1. Повторяем эти действия для каждого оставшегося роутера, собирая схему, приведенную на Рис. 14.5.

## Задача 2. Конфигурирование оборудования

***Шаг 1.*** Конфигурация Frame Relay на объекте «Cloud-PT»

Откроем окно конфигурации объекта «Cloud-PT», щелкнув по нему левой клавишей мышки.

Окно имеет две вкладки «Физическое пространство», где отображаются модули оборудования для дополнительных портов, и вкладка «Конфигурация» Рис.14.10.

Открыв вкладку «Физическое пространство», можно выбрать и установить модуль дополнительных портов типа Serial или Ethernet.

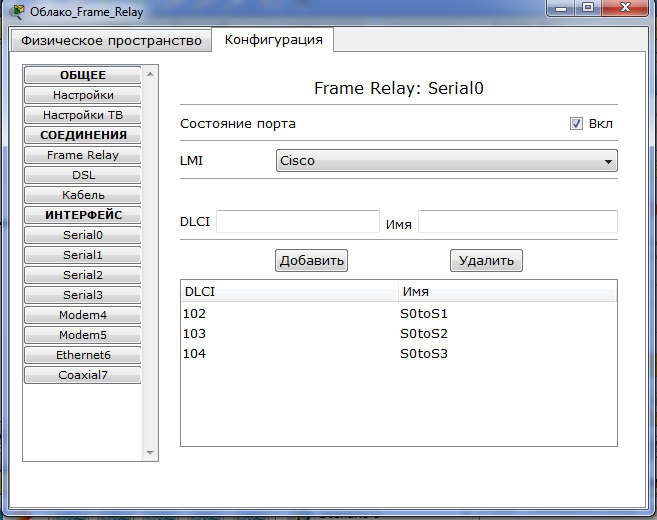


Рис 14.10. Окно конфигурации объекта «Could-PT»

В данном случае, нам нужна вкладка «Конфигурация».

1. Становимся на **интерфей*с Serial0***. Так как маршрутизатор R1, подключенный к этому порту, должен иметь соединения (логические каналы PVC) с остальными тремя маршрутизаторами R2, R3 и R4, назначаем (добавляем) этому порту три идентификатора DLCI, соответствующих трем направлениям потоков данных (трем каналам PVC). Для канала PVC с порта Serial0 на порт Serial1 выбираем DLCI 102 с именем S0toS1, для второго назначаем DLCI 103- имя S0toS2, для третьего 104 соответственно S0toS3. (При выполнении задания, значения DLCI выбираем из таблицы ниже, согласно варианта.) Для обратных каналов с портов S1(2,3) на S0, инициализируем по очереди порты и в каждом случае назначаем DLCI 101, а имя соответственно S1(2,3)toS0.
2. Нумерация DLCI абонентских каналов PVC и SVC используются в диапазоне 16-991; Далее, выбираем «***Соединения***» - «***Frame Relay***» и строим таблицу коммутации Рис 14.11, выбирая с помощью кнопок и ниспадающих списков необходимые значения.

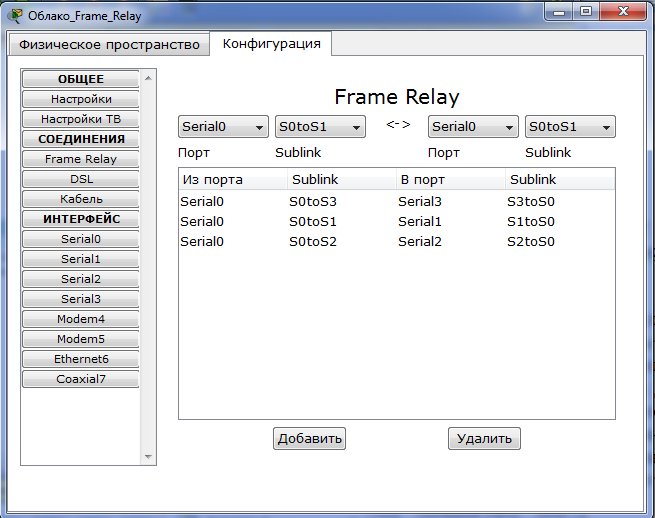


Рис 14.11. Таблица коммутации Frame Relay

***Шаг 2.***Конфигурирование **Frame Relay** и статических маршрутов на маршрутизаторе **Router (R1).**

Конфигурирование маршрутизаторов R1-R4 производится с помощью консоли CLI, т.е. с командной строки в ручную вводятся необходимые команды конфигурации.

Инициализируем R1, открываем окно консоли CLI, нажимаем «Enter», появляется приглашение **R1>.**

Входим в «привилегированный режим» - для этого вводим:

**R1> enable** – «привилегированный режим»

- далее переходим в глобальный режим;

**R1# configure terminal –**переходим в глобальный режим;

**R1(config)# -**приглашение глобального режима.

Вводим следующие команды R1 для разрешения Frame Relay на физическом интерфейсе.

R1(config)# **interface serial0/0/0**

R1(config-if)# **encapsulation frame-relay**

R1(config-if)# **no shutdown**

Последней командой мы поднимаем интерфейс (порт) Serial0/0/0

***Шаг 3***. **Конфигурирование подынтерфейсов на R1.**

Физический интерфейс можно разбить на ряд логических подынтерфейсов для создания виртуальных каналов PVC Frame Relay.

Frame Relay подынтерфейсы можно сконфигурировать использованием двухточечной (point-to-point) связи. Сконфигурируйте point-to-point соединения к трем spoke маршрутизаторам через подынтерфейсы и назначьте соответствующие значения DLCI для каждого frame relay подключения согласно таблице 14.3 (конкретные значения выбирайте из таблицы 14.4 согласно варианта):

Таблица 14.

|  |  |  |
| --- | --- | --- |
| S0/0/0.102 | IP: 10.0.1.1  SM: 255.255.255.252 | DLCI: 102 |
| S0/0/0.103 | IP: 10.0.1.5  SM: 255.255.255.252 | DLCI: 103 |
| S0/0/0.104 | IP: 10.0.1.9  SM: 255.255.255.252 | DLCI: 104 |

1. Создайте и сконфигурируйте подынтерфейс s0/0/0.102. Из режима глобального конфигурирования выполните следующие команды:

***1)***Создаем подынтерфейс s0/0/0**.**102 в режиме point-to-point.

**R1(config)# interface Serial0/0/0.102 point-to-point**

***2)***Присеваем ***IP***  адрес подынтерфейсу s0/0/0.102.

**R1(config-subif)# ip address 10.0.1.1 255.255.255.252**

***3)***устанавливаем протокол подынтерфейса s0/0/0.102. и назначаем ему DLCI 102

**R1(config-subif)# frame-relay interface-dlci 102**

***4)***Выходим из режима конфигурации подынтерфейса s0/0/0.102.

**R1(config-subif)# exit**

1. Повторите данные команды для создания и конфигурирования под интерфейсов s0/0/0.103 и s0/0/0.104.

При назначении IP-адресов учитывать следующее: между маршрутизаторами выделяется сеть с адресным пространством на 256 адресов, которое разбивается на три подсети с маской **255.255.255.252**, например: имеем глобальную сеть 10.0.1.0/24, разбиваем её на три подсети 1) 10.0.1.0/30 с маской **255.255.255.252; 2) 10.0.1.4/30 (255.255.255.252); 3) 10.0.1.8/30 (255.255.255.252); значения для конкретного варианта выбираем из таблицы 14.4.**

1. R1(config)# **interface Serial0/0/0.103 point-to-point**

R1(config-subif)# **ip address 10.0.1.5 255.255.255.252**

R1(config-subif)# **frame-relay interface-dlci 103**

R1(config-subif)# **exit**

R1(config)# **interface Serial0/0/0.104 point-to-point**

R1(config-subif)# **ip address 10.0.1.9 255.255.255.252**

R1(config-subif)# **frame-relay interface-dlci 104**

R1(config-subif)# **exit**

**Создадим таблицу статической маршрутизации R1** в режиме глобального конфигурирования к сетям с компьютерами PC1- PC3, подключенным к маршрутизаторам R2-R4. Например: R1(config)# **ip route 10.20.20.0 255.255.255.0 10.0.1.2 для сети с PC1 маршрутизатор R2, (см.** Рис. 14.5**), аналогично и для остальных сетей. (IP-адреса сетей с компьютерами выбираем согласно вариантам таблица** 14. 4**)**

## Задача 3: Конфигурирование Frame Relay и маршрута по умолчанию на spoke маршрутизаторах.

**Шаг 1. Конфигурирование физического Frame Relay интерфейса на spoke маршрутизаторах.**

Frame Relay конфигурируется на spoke роутерах также как и на hub маршрутизаторе.

1. Перейдите на роутер R2. Откройте консоль CLI, дождитесь загрузки и нажмите «Enter»; после появления приглашения R2> наберите enable и войдите в привилегированный режим.
2. На R2 из привилегированного режима перейдите в режим глобального конфигурирования R2# configure terminal/

Сконфигурируйте основной физический интерфейс для Frame Relay соединения. Введите следующие команды на R2.

R2(config)# **interface serial0/0/0**

R2(config-if)# **encapsulation frame-relay**

R2(config-if)# **no shutdown**

**Шаг 2. Конфигурирование подынтерфейса на R2.**

Из режима глобального конфигурирования введите следующие команды для создания и конфигурирования подынтерфейса. Назначьте DLCI номер 101 для данного соединения.

R2(config)# **interface Serial0/0/0.101 point-to-point**

R2(config-subif)# **ip address 10.0.1.2 255.255.255.252**

R2(config-subif)# **frame-relay interface-dlci 101**

R2(config-subif)# **exit**

**Шаг 3. Конфигурирование маршрута по умолчанию на R2.**

Из режима глобального конфигурирования введите следующий статический маршрут.

R2(config)# **ip route 0.0.0.0 0.0.0.0 10.0.1.1**

**Шаг 4. Повторите шаги 1 – 3 на R3 и R4.**

1. На роутере R3 выполните следующие команды, назначая DLCI 101 frame relay соединению.

R3(config)# **interface serial0/0/0**

R3(config-if)# **encapsulation frame-relay**

R3(config-if)# **no shutdown**

R3(config-if)# **exit**

R3(config)# **interface Serial0/0/0.101 point-to-point**

R3(config-subif)# **ip address 10.0.1.6 255.255.255.252**

R3(config-subif)# **frame-relay interface-dlci 101**

R3(config-subif)# **exit**

R3(config)# **ip route 0.0.0.0 0.0.0.0 10.0.1.5**

На роутере R4 выполните следующие команды. Дайте DCLI 101 frame relay соединению.

R4(config)# **interface serial0/0/0**

R4(config-if)# **encapsulation frame-relay**

R4(config-if)# **no shutdown**

R4(config-if)# **exit**

R4(config)# **interface Serial0/0/0.101 point-to-point**

R4(config-subif)# **ip address 10.0.1.10 255.255.255.252**

R4(config-subif)# **frame-relay interface-dlci 101**

R4(config-subif)# **exit**

R4(config)# **ip route 0.0.0.0 0.0.0.0 10.0.1.9**

**Задача 4: Проверка соединения.**

**Шаг 1. Проверка Frame Relay сети.**

После конфигурирования Frame Relay на всех роутерах проверьте Frame Relay конфигурацию на R1.

1. Командой **show frame-relay map** проверьте соединение от R1 до spoke маршрутизаторов.

R1# **show frame-relay map**

Serial0/0/0.102 (up): point-to-point dlci, dlci 102, broadcast, status defined, active

Serial0/0/0.103 (up): point-to-point dlci, dlci 103, broadcast, status defined, active

Serial0/0/0.104 (up): point-to-point dlci, dlci 104, broadcast, status defined, active

Затем выполните команду **show frame-relay lmi** на R1.

**LM**I (Local Management Interface — LMI) - локальный интерфейс управления (расширение стандарта Frame Relay).

1. LMI –позволяет контролировать и управлять виртуальными каналами FR, например, контроль состояния активности интерфейса сети, изменения DLCI канала.
2. В случае коммутируемого канала (SVC) DLCI автоматически меняется при каждом установлении соединения. С помощью LMI соседние маршрутизаторы Cisco получают новый идентификатор в передаваемом Frame Relay обновлении LMI.

R1# **show frame-relay lmi**

LMI Statistics for interface Serial0/0/0 (Frame Relay DTE) LMI TYPE = CISCO

Invalid Unnumbered info 0 Invalid Prot Disc 0

Invalid dummy Call Ref 0 Invalid Msg Type 0

Invalid Status Message 0 Invalid Lock Shift 0

Invalid Information ID 0 Invalid Report IE Len 0

Invalid Report Request 0 Invalid Keep IE Len 0

Num Status Enq. Sent 26 Num Status msgs Rcvd 26

Num Update Status Rcvd 0 Num Status Timeouts 16

LMI Statistics for interface Serial0/0/0.102 (Frame Relay DTE) LMI TYPE = CISCO

Invalid Unnumbered info 0 Invalid Prot Disc 0

Invalid dummy Call Ref 0 Invalid Msg Type 0

Invalid Status Message 0 Invalid Lock Shift 0

Invalid Information ID 0 Invalid Report IE Len 0

Invalid Report Request 0 Invalid Keep IE Len 0

Num Status Enq. Sent 0 Num Status msgs Rcvd 0

Num Update Status Rcvd 0 Num Status Timeouts 16

LMI Statistics for interface Serial0/0/0.103 (Frame Relay DTE) LMI TYPE = CISCO

Invalid Unnumbered info 0 Invalid Prot Disc 0

Invalid dummy Call Ref 0 Invalid Msg Type 0

Invalid Status Message 0 Invalid Lock Shift 0

Invalid Information ID 0 Invalid Report IE Len 0

Invalid Report Request 0 Invalid Keep IE Len 0

Num Status Enq. Sent 0 Num Status msgs Rcvd 0

Num Update Status Rcvd 0 Num Status Timeouts 16

LMI Statistics for interface Serial0/0/0.104 (Frame Relay DTE) LMI TYPE = CISCO

Invalid Unnumbered info 0 Invalid Prot Disc 0

Invalid dummy Call Ref 0 Invalid Msg Type 0

Invalid Status Message 0 Invalid Lock Shift 0

Invalid Information ID 0 Invalid Report IE Len 0

Invalid Report Request 0 Invalid Keep IE Len 0

Num Status Enq. Sent 0 Num Status msgs Rcvd 0

Num Update Status Rcvd 0 Num Status Timeouts 16

Последней командой является **show frame-relay pvc**.

R1# **show frame-relay pvc (выполнить для каждого маршрутизатора)**

PVC Statistics for interface Serial0/0/0 (Frame Relay DTE)

DLCI = 102, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0/0/0.102

input pkts 14055 output pkts 32795 in bytes 1096228

out bytes 6216155 dropped pkts 0 in FECN pkts 0

in BECN pkts 0 out FECN pkts 0 out BECN pkts 0

in DE pkts 0 out DE pkts 0

out bcast pkts 32795 out bcast bytes 6216155

DLCI = 103, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0/0/0.103

input pkts 14055 output pkts 32795 in bytes 1096228

out bytes 6216155 dropped pkts 0 in FECN pkts 0

in BECN pkts 0 out FECN pkts 0 out BECN pkts 0

in DE pkts 0 out DE pkts 0

out bcast pkts 32795 out bcast bytes 6216155

DLCI = 104, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0/0/0.104

input pkts 14055 output pkts 32795 in bytes 1096228

out bytes 6216155 dropped pkts 0 in FECN pkts 0

in BECN pkts 0 out FECN pkts 0 out BECN pkts 0

in DE pkts 0 out DE pkts 0

out bcast pkts 32795 out bcast bytes 6216155

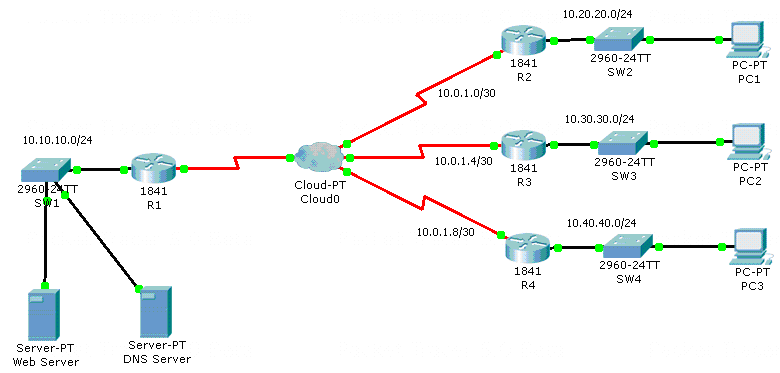
**Шаг 2. Проверка соединения с spoke сетями.**

С роутера R1 с CLI пошлите команду ping в сторону интерфейсов роутеров R2, R3 и R4.

Ваш процент завершения должен составить 100 %. В противном случае необходимо выяснить, какие компоненты задания не выполнены или выполнены с ошибками.

**Задача 5. Проверка функционирования сети с хостами и web сервиса.**

**Шаг 1. Добавление хостов к подсетям.**

**Рис 14.1****2.** Полная схема сети с транспортной сетью Frame Relay.

Добавьте в подсеть 10.10.10.0/24 два сервера, в остальные подсети - по одной рабочей станции как показано на рисунке. Назначьте им IP адреса, учитывая, что один адрес в каждой подсети должен быть назначен интерфейсу соответствующего роутера. Назначьте серверам имена “Web Server” и “DNS Server”. На хостах PC1 – PC3 укажите IP адрес DNS сервера. На всех хостах укажите IP адрес шлюза по умолчанию. На DNS сервере заполните таблицу с DNS записями указ в каждой имя компьютера и его IP- адрес. Командой **ipconfig** проверьте конфигурации на всех хостах. На Web сервере измените содержимое html-страницы, добавив приветствие произвольного содержания. На DNS сервере укажите доменное имя Web сервера (произвольное, например, **www.mycom.edu**) и его IP адрес.

**Шаг 2. Проверка соединения.**

Между добавленными хостами должны проходить успешные piong’s. В противном случае удостоверьтесь, что Вы правильно ввели все команды предыдущего раздела.

**Шаг 3. Проверка маршрутов.**

С хоста PC1 выполните команду **tracert**, указав IP адрес хоста PC2. Объясните полученные результаты.

**Шаг 4. Проверка web сервиса.**

С одного из хостов PC1 –PC3 в адресной строке браузера наберите адрес Web сервера (например, **www.mycom.edu**).

Контрольные вопросы***:***

1. Что представляют собой постоянный и коммутируемый виртуальные каналы и как обозначаются?
2. Какие байты служат для разграничения кадров Frame Relay (FR)?
3. На основе какой технологии разработан протокол FR и чем отличается от неё? Поясните работу этой технологии на основании Рис. 14-1. И Рис. 14-2
4. Чем отличается FR от IP протокола (см. [2]), в чем преимущества и недостатки?
5. Какие организации занимаются стандартизацией технологии Frame Relay?
6. Назовите два слоя протоколов Frame Relay! На основании Рис. 14.3 перечислите протоколы FR и расскажите назначение каждого!
7. Назначение особенности и два типа (версии) протокола LAP-F?
8. Подробно описать структуру кадров Frame Relay, на чем основана, перечислить все поля рассказать назначение каждого!?
9. Что такое DLCI? Какие значения DLCI можно применять при конфигурировании виртуальных каналов (устройств, интерфейсов, подинтерфейсов)? Применяются ли в протоколе FR адреса хостов (см.также [1,2]) и в каких случаях?
10. Как осуществляется поддержка качества каналов FR? Какие параметры и алгоритмы применяются для этого?
11. Для чего нужен LMI, какие функции им выполняются? [см.также 3,4]
12. Что представляет собой interface на маршрутизаторе CISCO, какие бывают интерфейсы и sub-interface.
13. Что такое IOS, CLI? Какие режимы поддерживаются в CLI? Какие основные команды Вы знаете? [3,4].
14. Практически показать смоделированную сеть и подробно рассказать о конфигурации любого узла сети.
15. ***Номер варианта согласовать с преподавателем.***

# Варианты для выполнения практического задания

Таблица 14. 4

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № вар-та | DLCI | | | | IP сети Между  R1,2,3,4 | **IP – адреса сетей с PC компьютерами.** | | | |
| S0toS1 | S0toS2 | S0toS3 | S1(2,3) | R1 | R2 | R3 | R4 |
| 1 | 111+gp | 112+gp | 113+gp | 100+gp | 10. gp.1.0 | 10. gp+1.1.0 | 10. gp+1.2.0 | 10. gp+1.3.0 | 10. gp+1.4.0 |
| 2 | 21+gp | 22+gp | 23+gp | 20+gp | 10. gp.2.0 | 10. gp+2.1.0 | 10. gp+2.2.0 | 10. gp+2.3.0 | 10. gp+2.4.0 |
| 3 | 31+gp | 32+gp | 33+gp | 30+gp | 10. gp.3.0 | 10. gp+3.1.0 | 10. gp+3.2.0 | 10. gp+3.3.0 | 10. gp+3.4.0 |
| 4 | 41+gp | 42+gp | 43+gp | 40+gp | 10. gp.4.0 | 10. gp+4.1.0 | 10. gp+4.2.0 | 10. gp+4.3.0 | 10. gp+4.4.0 |
| 5 | 51+gp | 52+gp | 53+gp | 50+gp | 10. gp.5.0 | 10. gp+5.1.0 | 10. gp+5.2.0 | 10. gp+5.3.0 | 10. gp+5.4.0 |
| 6 | 61+gp | 62+gp | 63+gp | 60+gp | 10. gp.6.0 | 10. gp+6.1.0 | 10. gp+6.2.0 | 10. gp+6.3.0 | 10. gp+6.4.0 |
| 7 | 201+gp | 202+gp | 203+gp | 200+gp | 10. gp.7.0 | 10. gp+7.1.0 | 10. gp+7.2.0 | 10. gp+7.3.0 | 10. gp+7.4.0 |
| 8 | 301+gp | 302+gp | 303+gp | 300+gp | 10. gp.8.0 | 10. gp+8.1.0 | 10. gp+8.2.0 | 10. gp+8.3.0 | 10. gp+8.4.0 |
| 9 | 401+gp | 402+gp | 403+gp | 400+gp | 10. gp.9.0 | 10. gp+9.1.0 | 10. gp+9.2.0 | 10. gp+9.3.0 | 10. gp+9.4.0 |
| 10 | 501+gp | 502+gp | 503+gp | 500+gp | 10. gp.10.0 | 10. gp+10.1.0 | 10. gp+10.2.0 | 10. gp+10.3.0 | 10. gp+10.4.0 |
| 11 | 601+gp | 602+gp | 603+gp | 600+gp | 10. gp.11.0 | 10. gp+11.1.0 | 10. gp+11.2.0 | 10. gp+11.3.0 | 10. gp+11.4.0 |
| 12 | 701+gp | 702+gp | 703+gp | 700+gp | 10. gp.12.0 | 10. gp+12.1.0 | 10. gp+12.2.0 | 10. gp+12.3.0 | 10. gp+12.4.0 |
| 13 | 801+gp | 802+gp | 803+gp | 800+gp | 10. gp.13.0 | 10. gp+13.1.0 | 10. gp+13.2.0 | 10. gp+13.3.0 | 10. gp+13.4.0 |
| 14 | 901+gp | 902+gp | 903+gp | 900+gp | 10. gp.14.0 | 10. gp+14.1.0 | 10. gp+14.2.0 | 10. gp+14.3.0 | 10. gp+14.4.0 |
| 15 | 911+gp | 912+gp | 913+gp | 910+gp | 10. gp.15.0 | 10. gp+15.1.0 | 10. gp+15.2.0 | 10. gp+15.3.0 | 10. gp+15.4.0 |

**!!! gp**- значение: **g** –**номер группы**, **p**- **номер подгруппы**, например **gp=21**- вторая группа, первая подгруппа. Для интерфейсов, соединяющих R1 с другими маршрутизаторами применять IP адреса, например вариант 1, для R1-R2: R1- 10.11.1.1 и R2-10.11.1.2 с маской /30; для R1-R3 соответственно R1- 10.11.1.5 и R2-10.11.1.6 с маской /30 и т.д. …

***Дополнительные материалы:***

1. В.Г. Олифер, Н.А. Олифер Компьютерные сети, 3-е издание, 2009г.
2. Тема 34 Технология виртуальных каналов. Сети Frame Relay.
3. Димарцио Д. Ф. Маршрутизаторы Cisco. Пособие для самостоятельного изучения. - Пер. с англ. СПб: Символ-Плюс, 2003. - 512 с, ил. ISBN 5-93286-048-0
4. Дж. Бони Руководство по Cisco IOS. — СПб.: Питер, М.: Издательство «Русская Редакция», 2003г.