

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего
профессионального образования

«Оренбургский государственный университет»

Кафедра системного анализа и управления

А.Л. Коннов, Ю.А. Ушаков

ВЫЧИСЛИТЕЛЬНЫЕ СЕТИ И КОМПЛЕКСЫ

Методические указания
к лабораторным работам. Часть 2

Рекомендовано к изданию Редакционно-издательским советом Федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Оренбургский государственный университет»

Оренбург
ОГУ
2012

УДК 004.7(07)
ББК 32.973.202я7
К 64

Рецензент – доцент, кандидат педагогических наук А.Е. Шухман

Коннов, А. Л.
К64 Вычислительные сети и комплексы: методические указания к лабораторным работам. Часть 2 / А. Л. Коннов, Ю. А. Ушаков; Оренбургский гос. ун-т. – Оренбург : ОГУ, 2012. – 65 с.

Методические указания содержат теоретический материал и задания к выполнению лабораторных работ по дисциплине «Вычислительные сети и комплексы».

Предназначены для бакалавров, обучающихся по направлению 220100.62 Системный анализ и управление при изучении дисциплины «Вычислительные сети и комплексы».

УДК 004.7(07)
ББК 32.973.202я7

© Коннов А. Л.,
Ушаков Ю. А., 2012
© ОГУ, 2012

Содержание

1 Лабораторная работа №1. Маршрутизация в сетях передачи данных. Основные понятия и определения	4
1.1 Основные теоретические положения	4
1.2 Рабочее задание	8
1.3 Контрольные вопросы	9
2 Лабораторная работа №2. Статическая маршрутизация	9
2.1 Основные теоретические положения	9
2.2 Рабочее задание	15
2.3 Контрольные вопросы	23
3 Лабораторная работа №3. Протоколы динамической маршрутизации	24
3.1 Основные теоретические положения	24
3.2 Рабочее задание	26
3.3 Контрольные вопросы	28
4 Лабораторная работа №4. Протоколы RIP, RIPv2	28
4.1 Основные теоретические положения	28
4.2 Рабочее задание	34
4.3 Контрольные вопросы	34
5 Лабораторная работа №5. Протоколы IGRP, EIGRP	34
5.1 Основные теоретические положения	35
5.2 Рабочее задание	41
5.3 Контрольные вопросы	42
6 Лабораторная работа №6. Протокол OSPF	43
6.1 Основные теоретические положения	43
6.2 Рабочее задание	55
6.3 Контрольные вопросы	57
7 Лабораторная работа №7. Протокол BGP	58
7.1 Основные теоретические положения	58
7.2 Рабочее задание	62
7.3 Контрольные вопросы	63
Список использованных источников	65

1 Лабораторная работа №1. Маршрутизация в сетях передачи данных. Основные понятия и определения

Цель работы. Изучить теоретические положения, связанные с маршрутизацией в сетях передачи данных. Выполнить задание в соответствии с вариантом.

1.1 Основные теоретические положения

В процессе организации межсетевого взаимодействия важное место занимает маршрутизация сообщений между отдельными подсетями [1]. При этом под маршрутизацией понимается процесс доставки сообщения из одной подсети в другую. Данная задача может решаться различными способами. При этом, чем сложнее рассматриваемая система, чем больше подсетей ее образуют, тем более нетривиальным является решение задачи доставки сообщений. Сетевой компонент, выполняющий маршрутизацию пакетов, называется маршрутизатором (router). Маршрутизатор может быть реализован на базе компьютера с несколькими сетевыми интерфейсами, на котором установлено специальное программное обеспечение. В этом случае говорят о программном маршрутизаторе. В другом случае маршрутизатор может быть выполнен в виде отдельного сетевого устройства. Разумеется, наиболее эффективным решением является использование специальных аппаратных маршрутизаторов. В настоящее время лидером на рынке корпоративных маршрутизаторов является компания Cisco, предлагающая высокопроизводительные и надежные устройства. В небольших сетях (таких как сеть небольшого офиса или домашняя сеть), использование аппаратного маршрутизатора может быть экономически невыгодно.

В межсетевой среде каждая подсеть может быть соединена с произвольным количеством других подсетей посредством маршрутизаторов. Суть процесса маршрутизации сводится к тому, что два хоста, разделенных друг с другом любым произвольным количеством маршрутизаторов (другими словами, находящиеся в

разных подсетях), могут взаимодействовать друг с другом. Всю организацию процесса доставки пакета от одного хоста другому берут на себя маршрутизаторы. Рассмотрим основные принципы, лежащие в основе процесса маршрутизации сообщений. Подавляющее большинство сетевых служб Windows функционирует на базе стека протоколов TCP/IP, получившего широкое распространение именно благодаря простоте организации межсетевого взаимодействия (как известно, самое большое объединение сетей — Интернет, тоже основывается на этом стеке протоколов). Тем не менее, заметим, что в своей основе принципы маршрутизации являются общими для большинства стеков протоколов.

В зависимости от количества вовлеченных получателей стек протоколов TCP/IP поддерживает два способа маршрутизации: одноадресная и многоадресная маршрутизация. Соответственно, мы рассмотрим принципы маршрутизации применительно к каждому из способов в отдельности.

Под одноадресной маршрутизацией понимается процесс передачи сообщений между подсетями, в котором сообщение адресовано только одному заданному получателю. Вся задача маршрутизации в этом случае сводится к доставке пакета получателю и выбору оптимального маршрута из множества возможных.

Отправителя и получателя может разделять произвольное количество маршрутизаторов [2]. При этом процесс передачи сообщения от одного маршрутизатора другому называется "прыжком" (hop). Каждый маршрутизатор обладает информацией о структуре сети на расстоянии одного прыжка. Другими словами, маршрутизатор не обладает информацией о точном местоположении требуемого хоста. В большой сети, да еще и с интенсивно меняющейся структурой (как, например, Интернет), это было бы невозможно. Вместо этого, маршрутизатор обладает информацией о соседних маршрутизаторах и о том, кому из них необходимо передать сообщение для последующей доставки в той или иной ситуации. Эта информация хранится в специальной таблице, которая носит название таблицы маршрутизации (routing table).

Таблицы маршрутизации используются для принятия решения о том, как именно будет доставлено то или иное сообщение. Наличие этих таблиц не является

исключительным свойством маршрутизатора. В сети TCP/IP любой хост (даже не являющийся маршрутизатором) может также располагать таблицей маршрутизации, которая используется с целью определения оптимального маршрута передачи сообщений. Так, скажем, если в подсети имеется три маршрутизатора, хост использует таблицу маршрутизации для того, чтобы выбрать из них наиболее оптимальный для доставки сообщения.

Записи в таблице маршрутизации называются маршрутами. При этом существует три типа маршрутов.

Маршрут к хосту, или узловой маршрут (Host Route). Этот тип маршрута определяет путь доставки пакета, адресованного хосту с конкретным сетевым адресом. Маршруты к хостам обычно используются для создания настраиваемых маршрутов к определенным компьютерам, а также для управления или оптимизации сетевого трафика.

Маршрут к сети, или сетевой маршрут (Network Route). Данный тип маршрута используется для определения способа доставки пакета в подсеть с определенным адресом. Большую часть содержимого таблицы маршрутизации представляют собой маршруты данного типа.

Маршрут по умолчанию (Default Route) используется, когда не найдены никакие другие маршруты в таблице маршрутизации [3]. Маршрут по умолчанию используется в ситуации, когда в таблице маршрутизации отсутствует соответствующий маршрут по идентификатору сети или маршрут к хосту по адресу получателя. Маршрут по умолчанию упрощает конфигурацию компьютеров. Вместо конфигурирования компьютера и настройки маршрутов для всех идентификаторов сетей в межсетевой среде используется одиночный маршрут по умолчанию для пересылки всех пакетов в сеть получателя или по адресу в межсетевой среде, который не был найден в таблице маршрутизации.

Рассмотрим структуру таблицы маршрутизации на следующем примере (рисунок 1).

```

C:\Documents and Settings\Admin>route print
=====
Список интерфейсов
0x1 ..... MS TCP Loopback interface
0x2 ...00 13 d4 54 9c a9 ..... Marvell Yukon 88E8053 PCI-E Gigabit Ethernet Con
troller - [шэшыяЕЕ яырэшЕют шър ярьхЕют
=====
Активные маршруты:
Сетевой адрес      Маска сети      Адрес шлюза      Интерфейс      Метрика
0.0.0.0            0.0.0.0         10.14.0.3        10.14.1.39     10
10.14.0.0          255.255.128.0   10.14.1.39       10.14.1.39     10
10.14.1.39         255.255.255.255 127.0.0.1        127.0.0.1      10
10.255.255.255     255.255.255.255 10.14.1.39       10.14.1.39     10
127.0.0.0          255.0.0.0       127.0.0.1        127.0.0.1      1
224.0.0.0          240.0.0.0       10.14.1.39       10.14.1.39     10
255.255.255.255    255.255.255.255 10.14.1.39       10.14.1.39     1
Основной шлюз:      10.14.0.3
=====
Постоянные маршруты:
Отсутствует

```

Рисунок 1 – Таблица маршрутов

Каждая запись в таблице маршрутизации (представляющая собой информацию о маршруте) состоит из информационных полей, перечисленных ниже.

Сеть назначения (Network Destination). Данное поле содержит сведения об адресе хоста-получателя пакета или сети, в которой этот хост располагается. Принимая решение о маршрутизации пакета, система просматривает именно это поле. Если в данном поле не будет найдено записи о конкретном адресе сети или хоста, маршрутизатором будет использован маршрут по умолчанию.

Маска подсети (Netmask). Это поле в сочетании с предыдущим полем используется для вычисления идентификатора IP-сети.

Шлюз (Gateway). В этом поле указывается адрес, по которому будет должен быть передан согласно данному маршруту. Адрес пересылки может быть аппаратным адресом или адресом в междоменной среде. В большинстве случаев в этом поле указывается следующий в цепочке маршрутизатор, который должен будет принять решение о дальнейшей маршрутизации сообщения [4].

Интерфейс (Interface). В этом поле указывается сетевой интерфейс, с которого будет осуществляться передача сообщения согласно данному маршруту. Данное поле необходимо в ситуации, когда маршрутизатор имеет множество сетевых интерфейсов, подключенных к разным подсетям. Фактически данное поле указывает, в какую именно подсеть необходимо передать сообщение.

Метрика (Metric). Стоимость маршрута, характеризующая меру его предпочтения. Из множества альтернативных маршрутов будет выбран тот, что обладает наименьшей стоимостью (т. е. меньшим значением метрики). Некоторые алгоритмы маршрутизации сохраняют только один маршрут для любого идентификатора сети в таблице маршрутизации, даже когда существует несколько маршрутов. В этом случае метрика используется маршрутизатором, чтобы определить какой именно маршрут необходимо сохранить в таблице маршрутизации.

1.2 Рабочее задание

Необходимо просмотреть таблицу маршрутизации локального компьютера при помощи утилиты `route` и выполнить задание в соответствии с вариантом указанным в таблице 1.1.

Таблица 1.1 – Варианты заданий

Номер варианта	Задание
1	Получить подробную информацию о маршрутах в таблице маршрутизации локального компьютера (ключ PRINT)
2	Добавить маршрут в таблицу маршрутизации (ключ ADD)
3	Добавить маршрут в таблицу маршрутизации (ключ ADD) таким образом, чтобы он остался в таблице после перезагрузки компьютера (ключ -p)
4	Удалить маршрут из таблицы маршрутизации (ключ DELETE)
5	Изменить уже существующий маршрут в таблице маршрутизации (ключ CHANGE)
6	Получить информацию только о конкретном маршруте из таблицы маршрутизации (ключ PRINT)
7	Очистить таблицу маршрутизации от записей для всех шлюзов (ключ -f)

1.3 Контрольные вопросы

1. Дайте понятие маршрутизации в сетях передачи данных.
2. Какое устройство выполняет функции маршрутизации в сетях передачи данных ?
3. Дайте понятие программного и аппаратного маршрутизатора.
4. Дайте понятие одноадресной маршрутизации.
5. Дайте понятие и опишите назначение таблицы маршрутизации.
6. Опишите три типа маршрутов (записей в таблице маршрутизации): маршрут к хосту, маршрут к сети, маршрут по умолчанию.
7. Назовите все поля и их назначения записи в таблице маршрутизации.

2 Лабораторная работа №2. Статическая маршрутизация

Цель работы. Изучить теоретические положения, связанные со статической маршрутизацией в сетях передачи данных. Выполнить задание в соответствии с вариантом.

2.1 Основные теоретические положения

В стеке TCP/IP принят так называемый одношаговый подход к оптимизации маршрута продвижения пакета (next-hop routing) - каждый маршрутизатор и конечный узел принимает участие в выборе только одного шага передачи пакета. Поэтому в каждой строке таблицы маршрутизации указывается не весь маршрут в виде последовательности IP-адресов маршрутизаторов, через которые должен пройти пакет, а только один IP-адрес - адрес следующего маршрутизатора, которому нужно передать пакет. Вместе с пакетом следующему маршрутизатору передается ответственность за выбор следующего шага маршрутизации. Одношаговый подход к маршрутизации означает распределенное решение задачи выбора маршрута. Это

снимает ограничение на максимальное количество транзитных маршрутизаторов на пути пакета[3].

Альтернативой одношаговому подходу является указание в пакете всей последовательности маршрутизаторов, которые пакет должен пройти на своем пути. Такой подход называется маршрутизацией от источника - Source Routing. В этом случае выбор маршрута производится конечным узлом или первым маршрутизатором на пути пакета, а все остальные маршрутизаторы только отрабатывают выбранный маршрут, осуществляя коммутацию пакетов, то есть передачу их с одного порта на другой. Алгоритм Source Routing применяется в сетях IP только для отладки, когда маршрут задается в поле Резерв (IP OPTIONS) пакета.

Для отправки пакета следующему маршрутизатору требуется знание его локального адреса, но в стеке TCP/IP в таблицах маршрутизации принято использование только IP-адресов для сохранения их универсального формата, не зависящего от типа сетей, входящих в интернет. Для нахождения локального адреса по известному IP-адресу необходимо воспользоваться протоколом ARP.

Конечный узел, как и маршрутизатор, имеет в своем распоряжении таблицу маршрутов унифицированного формата и на основании ее данных принимает решение, какому маршрутизатору нужно передавать пакет для сети N. Решение о том, что этот пакет нужно вообще маршрутизировать, компьютер принимает в том случае, когда он видит, что адрес сети назначения пакета отличается от адреса его собственной сети (каждому компьютеру при конфигурировании администратор присваивает его IP-адрес или несколько IP-адресов, если компьютер одновременно подключен к нескольким сетям). Когда компьютер выбрал следующий маршрутизатор, то он просматривает кэш-таблицу адресов своего протокола ARP и, может быть, находит там соответствие IP-адреса следующего маршрутизатора его MAC-адресу. Если же нет, то по локальной сети передается широковещательный ARP-запрос и локальный адрес извлекается из ARP-ответа [5].

После этого компьютер формирует кадр протокола, используемого на выбранном порту, например, кадр Ethernet, в который помещает MAC-адрес маршрутизатора. Маршрутизатор принимает кадр Ethernet, извлекает из него пакет

IP и просматривает свою таблицу маршрутизации для нахождения следующего маршрутизатора. При этом он выполняет те же действия, что и конечный узел.

Одношаговая маршрутизация обладает еще одним преимуществом - она позволяет сократить объем таблиц маршрутизации в конечных узлах и маршрутизаторах за счет использования в качестве номера сети назначения так называемого маршрута по умолчанию - default, который обычно занимает в таблице маршрутизации последнюю строку. Если в таблице маршрутизации есть такая запись, то все пакеты с номерами сетей, которые отсутствуют в таблице маршрутизации, передаются маршрутизатору, указанному в строке default. Поэтому маршрутизаторы часто хранят в своих таблицах ограниченную информацию о сетях интерсети, пересылая пакеты для остальных сетей в порт и маршрутизатор, используемые по умолчанию. Подразумевается, что маршрутизатор, используемый по умолчанию, передаст пакет на магистральную сеть, а маршрутизаторы, подключенные к магистрали, имеют полную информацию о составе интерсети.

Особенно часто приемом маршрутизации по умолчанию пользуются конечные узлы. Хотя они также в общем случае имеют в своем распоряжении таблицу маршрутизации, ее объем обычно незначителен, так как маршрутизация для компьютера - не основное занятие. Главная роль в маршрутизации пакетов в концепции протокола IP отводится, естественно, маршрутизаторам, которые должны обладать гораздо более полными таблицами маршрутизации, чем конечные узлы. Конечный узел часто вообще работает без таблицы маршрутизации, имея только сведения об IP-адресе маршрутизатора по умолчанию. При наличии одного маршрутизатора в локальной сети этот вариант - единственно возможный для всех конечных узлов. Но даже при наличии нескольких маршрутизаторов в локальной сети, когда проблема их выбора стоит перед конечным узлом, задание маршрута по умолчанию часто используется в компьютерах для сокращения объема их маршрутной таблицы [6].

Другим способом разгрузки компьютера от необходимости ведения больших таблиц маршрутизации является получение от маршрутизатора сведений о

рациональном маршруте для какой-нибудь конкретной сети с помощью протокола ICMP.

Кроме маршрута default, в таблице маршрутизации могут встретиться два типа специальных записей - запись о специфичном для узла маршруте и запись об адресах сетей, непосредственно подключенных к портам маршрутизатора.

Специфичный для узла маршрут содержит вместо номера сети полный IP-адрес, то есть адрес, имеющий ненулевую информацию не только в поле номера сети, но и в поле номера узла. Предполагается, что для такого конечного узла маршрут должен выбираться не так, как для всех остальных узлов сети, к которой он относится. В случае, когда в таблице есть разные записи о продвижении пакетов для всей сети N и ее отдельного узла, имеющего адрес N,D, при поступлении пакета, адресованного узлу N,D, маршрутизатор отдаст предпочтение записи для N,D.

Записи в таблице маршрутизации, относящиеся к сетям, непосредственно подключенным к маршрутизатору, в поле "Расстояние до сети назначения" содержат нули [7].

Еще одним отличием работы маршрутизатора и конечного узла при выборе маршрута является способ построения таблицы маршрутизации. Если маршрутизаторы обычно автоматически создают таблицы маршрутизации, обмениваясь служебной информацией, то для конечных узлов таблицы маршрутизации создаются, как правило, вручную администраторами, и хранятся в виде постоянных файлов на дисках.

Существуют различные алгоритмы построения таблиц для одношаговой маршрутизации. Их можно разделить на три класса:

- алгоритмы фиксированной маршрутизации (статическая),
- алгоритмы простой маршрутизации,
- алгоритмы адаптивной маршрутизации (динамическая).

Независимо от алгоритма, используемого для построения таблицы маршрутизации, результат их работы имеет единый формат. За счет этого в одной и той же сети различные узлы могут строить таблицы маршрутизации по своим алгоритмам, а затем обмениваться между собой недостающими данными, так как

форматы этих таблиц фиксированы. Поэтому маршрутизатор, работающий по алгоритму адаптивной маршрутизации, может снабдить конечный узел, применяющий алгоритм фиксированной маршрутизации, сведениями о пути к сети, о которой конечный узел ничего не знает.

Статическая маршрутизация характеризуется тем, что все маршруты прописываются и изменяются администратором системы вручную. Это самый простой способ организации маршрутизации. Однако он подходит только для небольших сетей, изменения в структуре которых происходят достаточно редко. Кроме того, данный способ маршрутизации не годится в случае, когда важно обеспечить высокую надежность межсетевого взаимодействия. Если один из маршрутов окажется по каким-либо причинам недоступен, администратору необходимо будет вручную изменить таблицу маршрутизации на всех маршрутизаторах в сети. До этого момента межсетевое взаимодействие на отдельных участках сети будет невозможно [5].

Статическая маршрутизируемая IP-сеть не использует протоколы маршрутизации, поскольку вся информация о маршрутизации хранится в статической таблице на каждом маршрутизаторе. Чтобы любые два произвольных хоста в сети могли взаимодействовать между собой, каждый маршрутизатор должен иметь такую таблицу маршрутов.

Статическая маршрутизируемая IP-среда лучше всего подходит для небольшой сети с редко изменяющейся структурой, в которой отсутствуют альтернативные маршруты. Статическая маршрутизируемая среда может применяться для:

- сети малого предприятия;
- сети домашнего офиса;
- филиала с одной сетью.

Вместо реализации протокола маршрутизации через узкополосный канал связи, одиночный маршрут по умолчанию на маршрутизаторе филиала гарантирует, что весь трафик, не предназначенный для компьютера в сети филиала, будет направлен в основной офис.

Недостатки статической маршрутизации заключаются в следующем [4].

Отсутствует отказоустойчивость, т.е. если в силу каких-либо причин один из маршрутизаторов выходит из строя или становится недоступным коммуникационный канал, статический маршрутизатор не сможет как-то отреагировать на неисправность. Более того, другие маршрутизаторы в сети не будут знать о неисправности и будут продолжать передавать данные по недоступному маршруту. В сетях малого офиса (например, с двумя маршрутизаторами и тремя сетями, соединенными в ЛВС) подобные ситуации могут решаться администратором оперативно. В крупных сетях более предпочтительным оказывается использование специальных протоколов маршрутизации.

Второй недостаток - это непроизводительные административные затраты. Если добавляется новая подсеть или удаляется из междоменной среды существующая, маршруты к ней должны быть вручную добавлены или удалены. Если добавляется новый маршрутизатор, то он должен быть правильно сконфигурирован для маршрутизации в междоменной среде.

Алгоритмы простой маршрутизации подразделяются на три подкласса:

- случайная маршрутизация - пакеты передаются в любом, случайном направлении, кроме исходного;
- лавинная маршрутизация - пакеты передаются во всех направлениях, кроме исходного (применяется в мостах для пакетов с неизвестным адресом доставки);
- маршрутизация по предыдущему опыту - таблицы маршрутов составляются на основании данных, содержащихся в проходящих через маршрутизатор пакетах. Именно так работают прозрачные мосты, собирая сведения об адресах узлов, входящих в сегменты сети. Такой способ маршрутизации обладает медленной адаптируемостью к изменениям топологии сети [7].

2.2 Рабочее задание

Необходимо научиться добавлять и удалять строки в таблицу маршрутизации и таким образом настроить статическую маршрутизацию на роутере в соответствии с вариантом указанным в таблице 2.1.

Для выполнения этого задания необходимо использовать бесплатную программу производителя сетевого оборудования компании CISCO – Cisco Packet Tracer 5.3.1.

Packet Tracer (PT) - эмулятор сетевой среды, выпускаемый фирмой Cisco, который:

- позволяет делать работоспособные модели сети, настраивать маршрутизаторы и коммутаторы, взаимодействовать между несколькими пользователями;
- включает в себя серии маршрутизаторов Cisco 1800, 2600, 2800 и коммутаторов 2950, 2960, 3650; серверы DHCP, HTTP, TFTP, FTP, TIME, рабочие станции, различные модули к компьютерам и маршрутизаторам, устройства WiFi, различные кабели;
- успешно позволяет создавать сложные макеты сетей. Внешний вид рабочего окна Packet Tracer показан на рисунке 2.1.

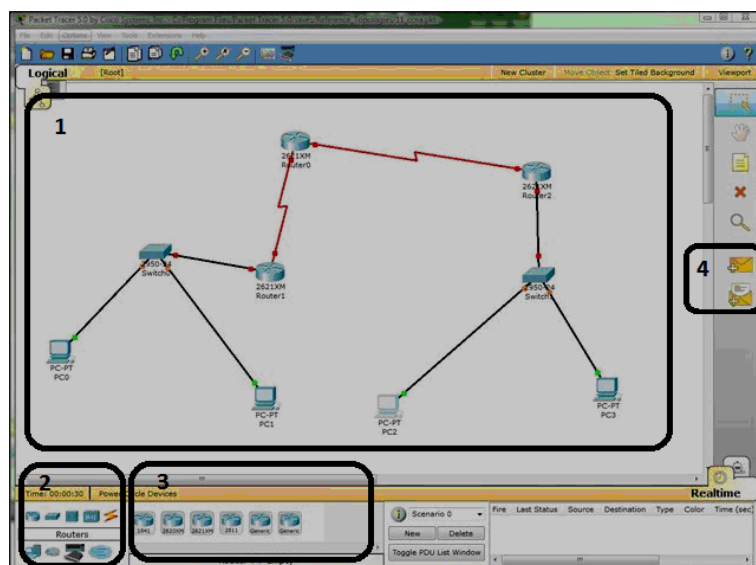


Рисунок 2.1 – Главное окно программы Packet Tracer

Основные области главного окна программы Packet Tracer следующие:

- 1 – рабочая область программы, в этой области можно собирать виртуальные сети, видеть трафик, запускать настройку устройств;
- 2 – область, используемая для выбора типа устройств, которые будут добавляться в рабочую область;
- 3 – область для выбора конкретного устройства для добавления;
- 4 – область, необходимая для визуального запуска сетевого пакета с одного устройства на другое.

В рабочей области отображается *логическая диаграмма сети*. Работа с объектами на логической диаграмме происходит мышью. Чтобы войти в режим настройки оборудования надо кликнуть на нужной картинке оборудования. Откроется окно настройки (рисунок 2.2).

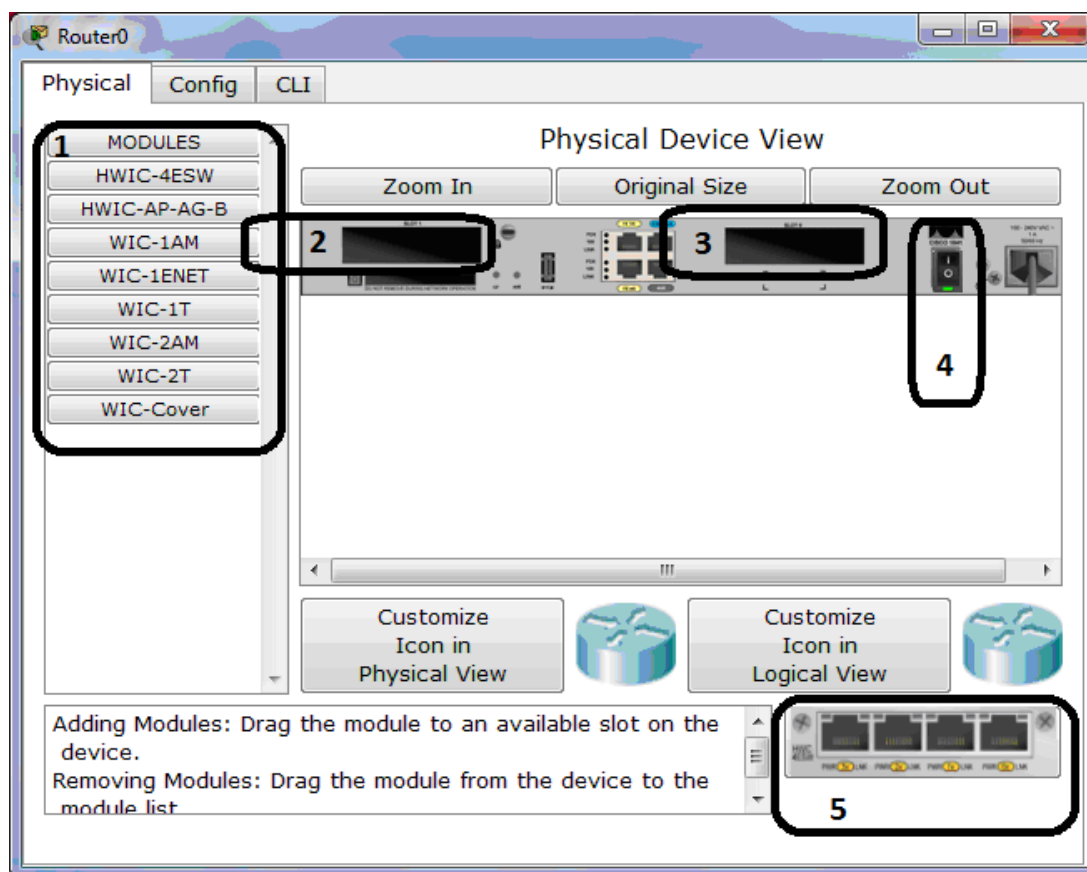


Рисунок 2.2 – Окно настройки

В первой вкладке окна настройки есть следующие элементы:

1. Модули, которые можно вставить в роутер. Чтобы вставить модуль, необходимо сначала выключить устройство (элемент 4), выбрать в списке нужный модуль, он появится в элементе 5. Перетащить мышью изображение модуля в пустой слот для модулей (элемент 2 или 3).

2. Слот для модуля 1.
3. Слот для модуля 2.
4. Кнопка выключения питания.
5. Изображение выбранного модуля.

В маршрутизаторах представлены следующие модули:

- HWIC-4ESW – модуль-коммутатор с 4 портами Ethernet;
- HWIC-AP-AG-B – модуль точки доступа 802.11B/G;
- WIC-1AM – 1 аналоговый порт модема V.90;
- WIC-1ENET – 1 маршрутизируемый порт Ethernet;
- WIC-2AM – 1 аналоговых порта модема V.90;
- WIC-2T – 2 последовательных порта serial;
- WIC-Cover – заглушка.

В каждом маршрутизаторе есть, как минимум, 2 порта Ethernet – как правило, для модульных маршрутизаторов они называются FastEthernet 0/0 и FastEthernet 0/1. Для немодульных устройств это будет FastEthernet0 и FastEthernet1.

Если в пустой слот вставлена карта расширения, например WIC-1ENET с 1 портом Ethernet в слоте №1, порт в маршрутизаторе будет обозначаться Ethernet0/0/0, где первая цифра 1 – это номер слота. Если карта будет вставлена в слот №2, то порт будет обозначаться Ethernet0/1/0. Последовательные (serial) порты обозначаются в маршрутизаторе аналогично, например, Serial0/0/0. Лучший способ проверить названия интерфейсов – зайти на вкладку «Config» окна настройки (рисунок 2.3).

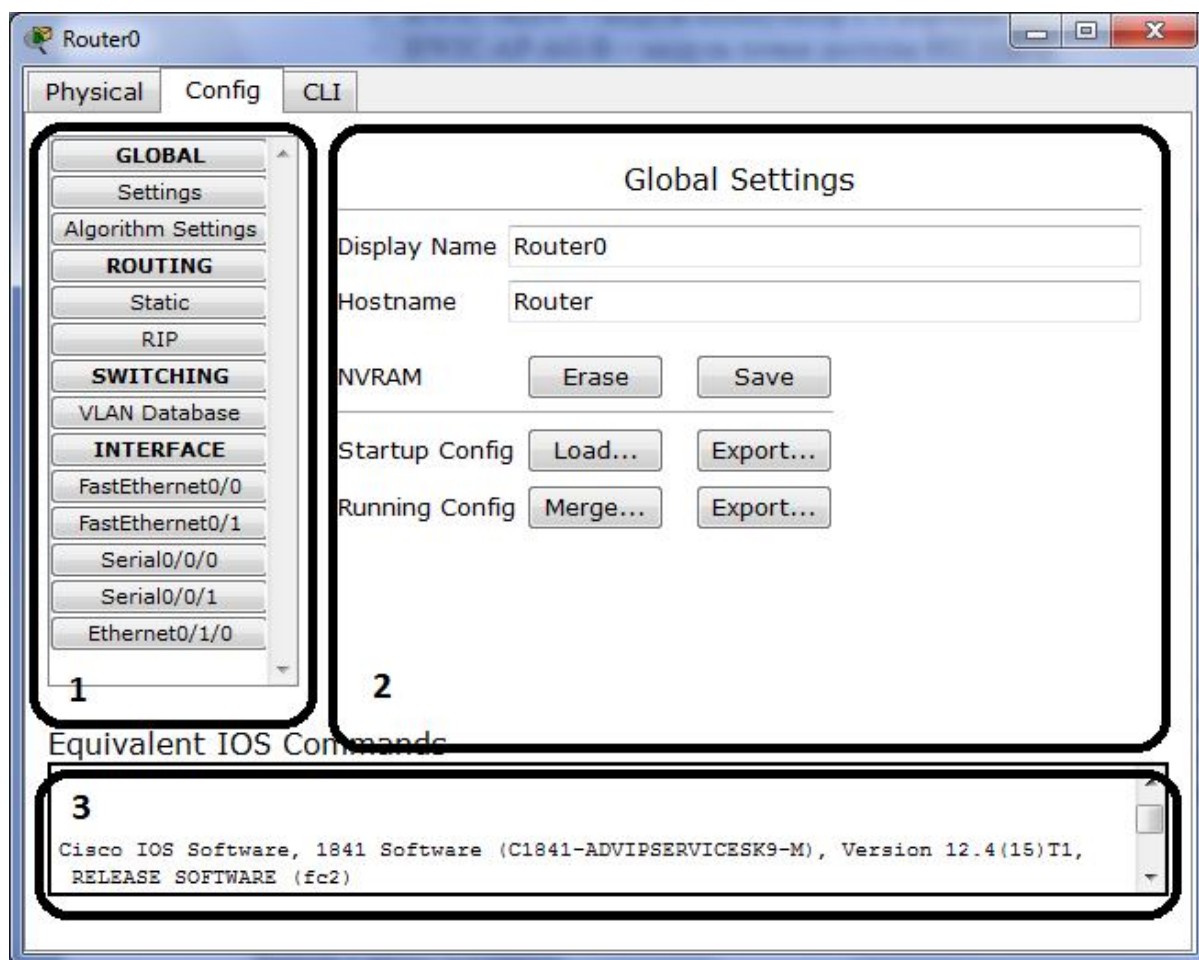


Рисунок 2.3 – Вкладка «Config» окна настройки

В окне настройки маршрутизатора есть следующие элементы:

1. Выбор типа настройки, имеет четыре вкладки, выделенные жирным шрифтом:

- GLOBAL - для общих настроек (рисунок 3.4).
- ROUTING - для статической и динамической маршрутизации.
- SWITCHING – для внутренней коммутации между виртуальными подсетями VLAN.
- INTERFACE – настройка конкретных интерфейсов.

2. Область «2» предназначена для задания настроек.

3. В области «3» показываются эквиваленты команд для настройки маршрутизатора через командную строку (CLI, command line interface). На рисунке 2.4 показана настройка интерфейса.

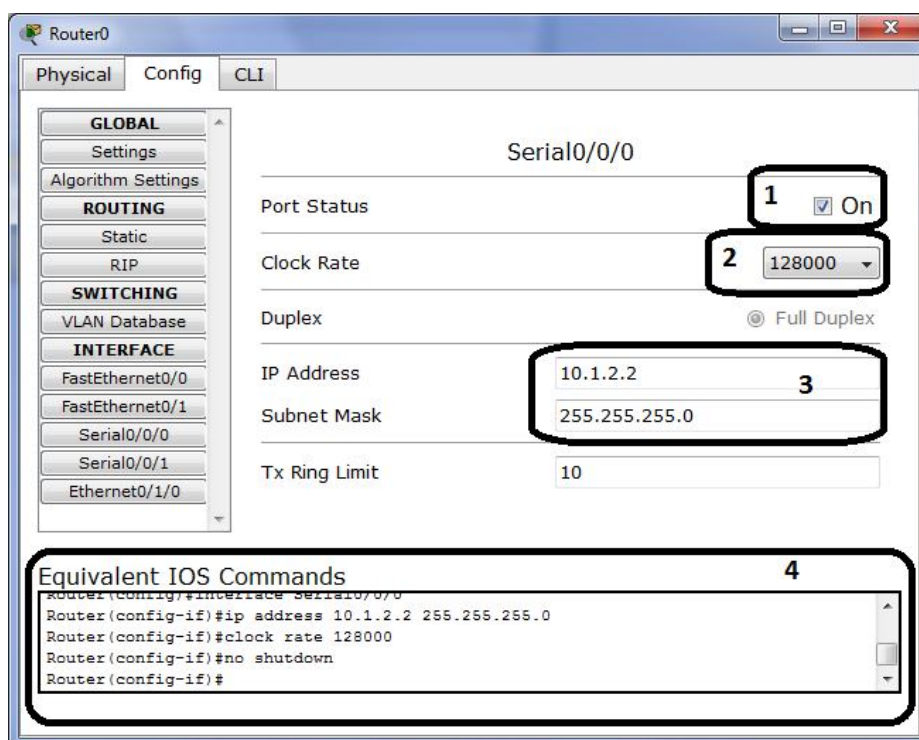


Рисунок 2.4 – Настройка интерфейса

Первое, что необходимо сделать – включить интерфейс (элемент 1). Затем можно задать IP адрес и маску (элемент 3). Для Serial интерфейсов необходимо заполнить еще скорость передачи данных Clock rate (элемент 2). В нижней части окна (элемент 4) будет показано, как сделать то же самое, только без использования графических инструментов, в командной строке.

Для конечных устройств, таких как компьютер, ноутбук, сервер, используется третья вкладка “Desktop”, которая выглядит, как показано на рисунке 2.5.

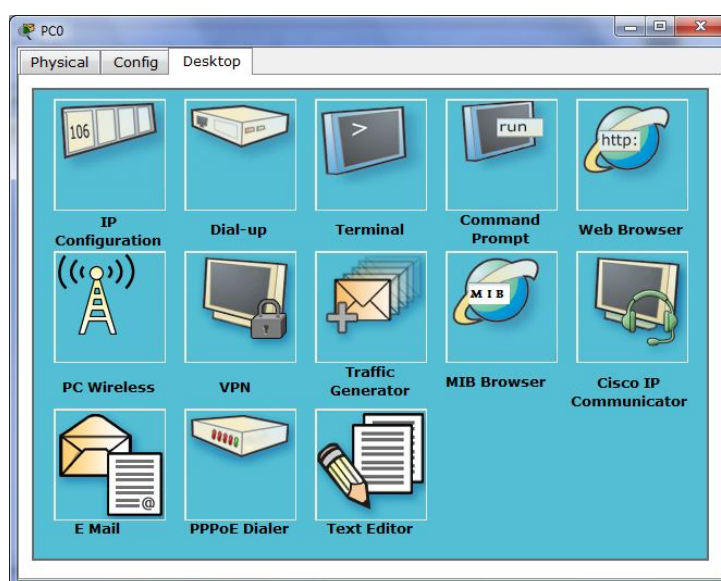


Рисунок 2.5 – Вкладка “Desktop” компьютера

Для настройки IP адреса, маски, шлюза по умолчанию и DNS лучше всего воспользоваться пунктом IP Configuration (рисунок 2.6).

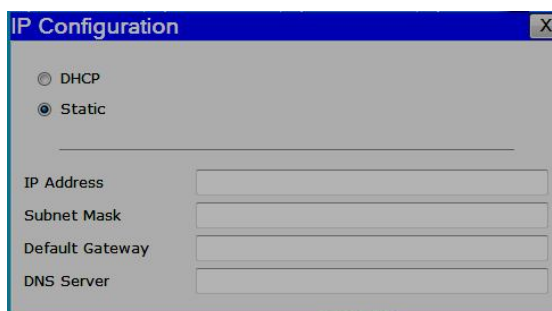


Рисунок 2.6 – Настройка IP параметров компьютера и сервера

Также часто используется пункт Command Prompt (рисунок 2.7). Командная строка поддерживает основные команды для тестирования сети – ping, tracer, arp, telnet.

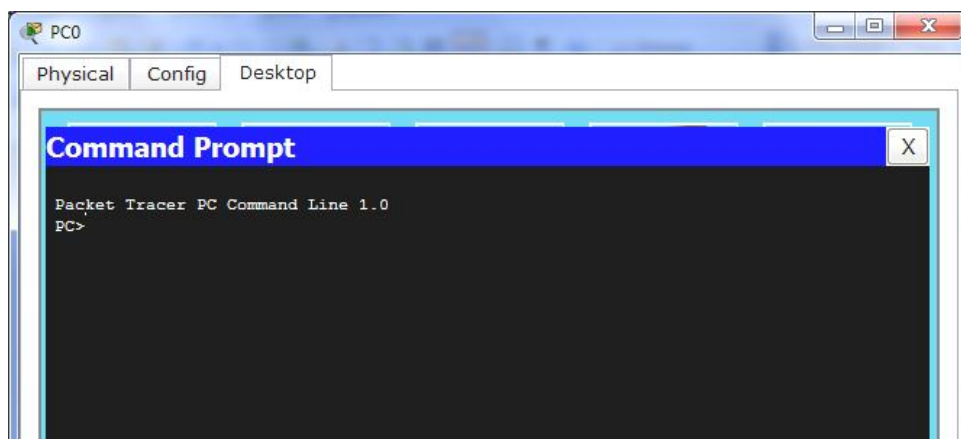


Рисунок 2.7 – Командная строка компьютера

В Packet Tracer дополнительно есть множество различных устройств. Символическое изображение показано на рисунке 2.8.

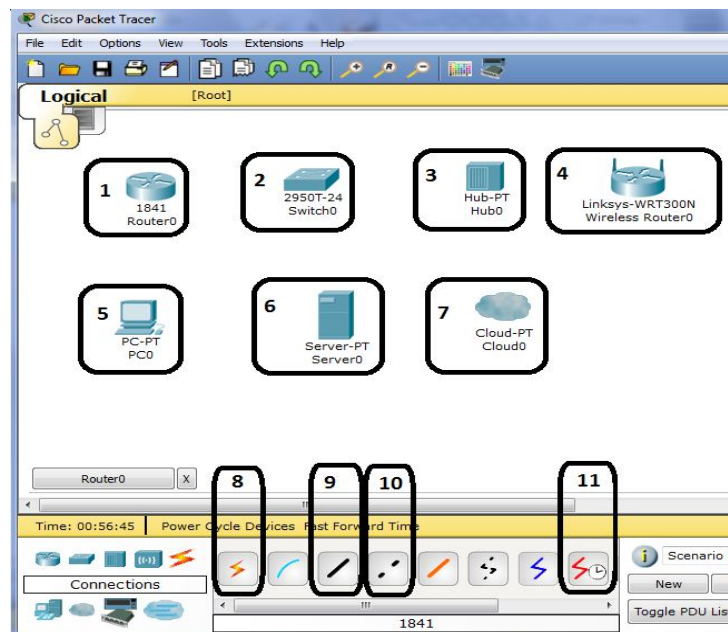


Рисунок 2.8 – Устройства и связи в Packet Tracer

Устройства обозначаются следующим образом:

- 1 – маршрутизатор, он же «роутер». Используется для передачи данных между сетями;
- 2 – коммутатор, он же «свич». Используется для объединения компьютеров в одну сеть;
- 3 – концентратор, он же «хаб». Используется с той же целью, что и коммутатор, но менее интеллектуален, поэтому уже несколько лет не выпускается;
- 4 – беспроводной маршрутизатор. Обычный маршрутизатор, оснащенный беспроводным модулем. Изображенный на рисунке маршрутизатор относится к серии домашних, поэтому имеет только Веб-интерфейс для настройки;
- 5 – персональный компьютер;
- 6 – сервер;
- 7 – облако, изображает провайдера Интернет;

Кроме устройств сеть состоит еще из соединительных носителей, например, из кабелей. На рисунке они обозначены как:

- 8 – автоматический определитель типа кабеля. Используется для быстрого соединения устройств;
- 9 – прямой кабель, он же «патч-корд». Используется для соединения разных классов устройств, например компьютер-коммутатор, коммутатор-маршрутизатор;

- 10 – обратный кабель, он же «кроссовер». Используется для соединения одинакового класса устройств, например компьютер-компьютер, коммутатор-коммутатор, компьютер-маршрутизатор;

- 11 – последовательный кабель, он же «серийный». Используется исключительно для соединения портов типа Serial между маршрутизаторами.

Порядок действий по выполнению лабораторной работы следующий:

- добавить в рабочую область два маршрутизатора cisco 1841;
- в каждый из этих маршрутизаторов добавить по модулю VIC-2T для соединения их серийной линией связи;
- соединить маршрутизаторы серийной линией связи;
- настроить серийные интерфейсы маршрутизаторов, задав частоту синхронизации и IP-адреса (выбираются произвольно из одной подсети);
- подключить к интерфейсам FastEthernet роутеров коммутаторы, к каждому коммутатору подключить по одному компьютеру;
- настроить адреса FastEthernet интерфейсов роутера, компьютеров задав им адреса из сетей, отличных от сети серийных интерфейсов роутеров, в качестве шлюза у компьютеров прописать адрес соответствующего интерфейса ближайшего роутера.

Далее необходимо выполнить настройку статической маршрутизации. При правильных настройках компьютеры смогут отправлять пакеты друг другу через сеть. Добиться этого можно следующим образом:

- прописать на каждом маршрутизаторе маршрут по умолчанию;
- добавить в таблицы маршрутизации каждого роутера строку, содержащую путь к локальным сетям, в которых находятся наши компьютеры (рисунок 2.9).



Рисунок 2.9 – Схема сети

В таблице 2.1 приведены варианты заданий.

Таблица 2.1 – Варианты заданий

Номер варианта	Задание
1	Сеть компьютера PC0: 192.168.10.0/24 Сеть между маршрутизаторами: 10.10.10.0/30 Сеть компьютера PC1: 192.168.11.0/24
2	Сеть компьютера PC0: 172.16.0.0/16 Сеть между маршрутизаторами: 10.10.20.0/30 Сеть компьютера PC1: 172.17.0.0/16
3	Сеть компьютера PC0: 192.168.20.0/24 Сеть между маршрутизаторами: 10.20.10.0/30 Сеть компьютера PC1: 192.168.21.0/24
4	Сеть компьютера PC0: 172.18.0.0/16 Сеть между маршрутизаторами: 10.20.10.0/30 Сеть компьютера PC1: 172.19.0.0/16
5	Сеть компьютера PC0: 192.168.40.0/24 Сеть между маршрутизаторами: 10.30.10.0/30 Сеть компьютера PC1: 192.168.41.0/24
6	Сеть компьютера PC0: 192.168.50.0/24 Сеть между маршрутизаторами: 10.11.10.0/30 Сеть компьютера PC1: 192.168.51.0/24
7	Сеть компьютера PC0: 172.20.0.0/16 Сеть между маршрутизаторами: 11.10.10.0/30 Сеть компьютера PC1: 172.21.0.0/16

2.3 Контрольные вопросы

1. Дайте понятие одношагового подхода к оптимизации маршрута продвижения пакета.
2. Дайте понятие маршрутизации от источника.
3. В чем заключается преимущество одношаговой маршрутизации ?
4. В чем заключается маршрутизация по умолчанию ?
5. Дайте понятие специфичного для узла маршрута.
6. Какие существуют алгоритмы построения таблиц для одношаговой маршрутизации?
7. Дайте понятие и опишите недостатки статической маршрутизации.

3 Лабораторная работа №3. Протоколы динамической маршрутизации

Цель работы. Изучить теоретические положения, связанные с динамической маршрутизацией в сетях передачи данных. Выполнить задание в соответствии с вариантом.

3.1 Основные теоретические положения

Адаптивная маршрутизация - это основной вид алгоритмов маршрутизации, применяющихся маршрутизаторами в современных сетях со сложной топологией. Адаптивная маршрутизация основана на том, что маршрутизаторы периодически обмениваются специальной топологической информацией об имеющихся в интернет-сетях, а также о связях между маршрутизаторами. Обычно учитывается не только топология связей, но и их пропускная способность и состояние [1].

Адаптивные протоколы позволяют всем маршрутизаторам собирать информацию о топологии связей в сети, оперативно отрабатывая все изменения конфигурации связей. Эти протоколы имеют распределенный характер, который выражается в том, что в сети отсутствуют какие-либо выделенные маршрутизаторы, которые бы собирали и обобщали топологическую информацию: эта работа распределена между всеми маршрутизаторами.

Построение таблицы маршрутизации осуществляется посредством специальных протоколов маршрутизации. Участие администратора в этом процессе минимально и сводится к изначальной конфигурации маршрутизаторов. Наиболее распространенные протоколы IP-маршрутизации - RIP (Routing Information Protocol), OSPF (Open Shortest Path First), IGRP (Interior Gateway Routing Protocol), EIGRP (Enhanced Interior Gateway Routing Protocol), BGP (Border Gateway Protocol). П посредством указанных протоколов маршрутизаторы способны информировать друг друга об изменениях в структуре сети. В случае недоступности одного из

маршрутов, маршрутизаторы автоматически перестроят свои таблицы маршрутизации и, при возможности, выберут другой маршрут доставки сообщений.

Канальные (link state) и векторные (distance vector) — два основных семейства алгоритмов маршрутизации. Принудительная маршрутизация (policy routing) — подвид векторной [2].

В первой схеме, которую еще называют маршрутизация по состоянию канала, маршрутизатор широковещательно рассылает список узлов, к которым подключен. Этот список называется состояние канала (link state). При такой схеме маршрутизаторы отправляют маленькие объемы информации множеству узлов. Данные передаются по мере надобности (при изменении состояния канала). Алгоритмы канальной маршрутизации требуют больше вычислений, нежели при векторной маршрутизации. Но при этом гораздо реже возникают циклические маршруты. К канальной маршрутизации относятся следующие алгоритмы:

- ISO Intermediate System to Intermediate System (IS-IS);
- Netware Link Services Protocol;
- Open Shortest Path First (OSPF).

Маршрутизатор, использующий векторный алгоритм, рассылает полную таблицу маршрутизации, но только своим соседям; то есть много информации ограниченному числу узлов. Суть векторной маршрутизации в минимизации числа узлов, проходимых пакетом. Ее стоит применять в маленьких сетях с небольшим числом надежных каналов. Она проще и требует меньше памяти, чем канальная маршрутизация. При настройке векторного маршрутизатора необходимо указать всех его соседей и “стоимость” каналов к каждому из них (в терминах времени и ресурсов).

Векторные алгоритмы, также называемые алгоритмами Беллмана-Форда (Bellman-Ford) или Форда-Фалкерсона (Ford-Fulkerson), сходятся медленнее, чем протоколы канальной маршрутизации. В данном контексте термин “сходиться” означает приведение таблиц маршрутизации всех узлов к единому согласованному виду, полностью отражающему реальное состояние сети. Крайний пример

медленной сходимости известен как “проблема ухода в бесконечность” (count-to-infinity problem) [8].

К векторным протоколам маршрутизации относятся:

- Routing Information Protocol (RIP);
- AppleTalk Routing Table Management Protocol (RTMP);
- Interior Gateway Routing Protocol (IGRP).

Протоколы принудительной маршрутизации не что иное, как модификации векторных. Эти алгоритмы при выборе маршрута помимо физических факторов, например числа переходов и стоимости, учитывают и политические, например деловые соглашения с другими компаниями. Такие алгоритмы используются достаточно часто [9].

3.2 Рабочее задание

Необходимо собрать схему сети, представленную на рисунке 3.1, настроить IP адреса устройств в соответствии с вариантом указанным в таблице 3.1. Адресом компьютера является последний возможный адрес из выделенной подсети, адрес роутера первый возможный адрес из соответствующей подсети.

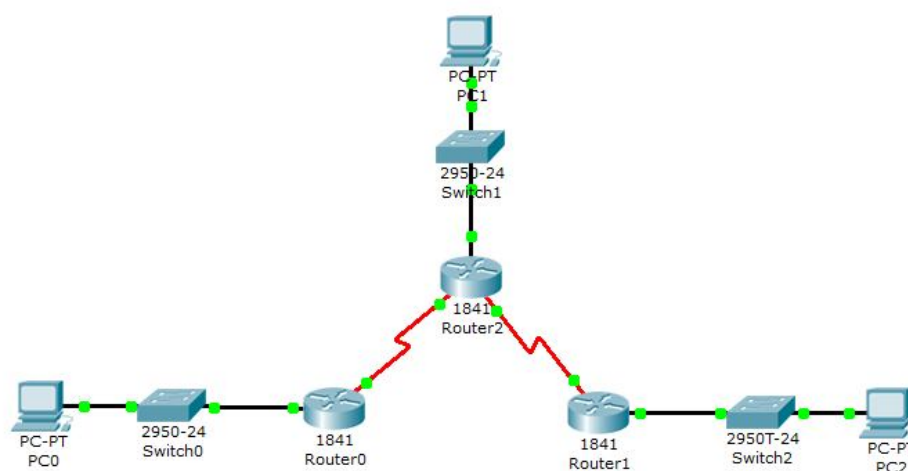


Рисунок 3.1 – Схема сети

Таблица 3.1 – Варианты заданий

Номер варианта	Задание
1	Сеть компьютера PC0: 192.168.10.0/24 Сеть компьютера PC1: 192.168.11.0/24 Сеть компьютера PC1: 192.168.12.0/24 Сеть между маршрутизаторами Router0-Router2: 10.10.10.0/30 Сеть между маршрутизаторами Router1-Router2: 10.10.11.0/30
2	Сеть компьютера PC0: 172.16.0.0/16 Сеть компьютера PC1: 172.17.0.0/16 Сеть компьютера PC1: 172.18.0.0/16 Сеть между маршрутизаторами Router0-Router2: 10.0.0.16/30 Сеть между маршрутизаторами Router1-Router2: 10.0.1.20/30
3	Сеть компьютера PC0: 192.168.20.0/24 Сеть компьютера PC1: 192.168.21.0/24 Сеть компьютера PC1: 192.168.22.0/24 Сеть между маршрутизаторами Router0-Router2: 10.10.0.0/30 Сеть между маршрутизаторами Router1-Router2: 10.10.1.0/30
4	Сеть компьютера PC0: 172.19.0.0/16 Сеть компьютера PC1: 172.20.0.0/16 Сеть компьютера PC1: 172.21.0.0/16 Сеть между маршрутизаторами Router0-Router2: 10.0.10.8/30 Сеть между маршрутизаторами Router1-Router2: 10.0.11.12/30
5	Сеть компьютера PC0: 192.168.30.0/24 Сеть компьютера PC1: 192.168.31.0/24 Сеть компьютера PC1: 192.168.32.0/24 Сеть между маршрутизаторами Router0-Router2: 10.10.15.0/30 Сеть между маршрутизаторами Router1-Router2: 10.10.16.0/30
6	Сеть компьютера PC0: 172.22.0.0/16 Сеть компьютера PC1: 172.23.0.0/16 Сеть компьютера PC1: 172.24.0.0/16 Сеть между маршрутизаторами Router0-Router2: 10.10.17.0/30 Сеть между маршрутизаторами Router1-Router2: 10.10.18.0/30
7	Сеть компьютера PC0: 192.168.10.0/24 Сеть компьютера PC1: 192.168.11.0/24 Сеть компьютера PC1: 192.168.12.0/24 Сеть между маршрутизаторами Router0-Router2: 10.10.10.4/30 Сеть между маршрутизаторами Router1-Router2: 10.10.11.8/30

3.3 Контрольные вопросы

1. Дайте понятие адаптивной маршрутизации.
2. Какое преимущество имеют адаптивные протоколы маршрутизации перед статической маршрутизацией ?
3. Назовите два основных семейства алгоритмов маршрутизации.
4. Дайте понятие маршрутизации по состоянию канала (канальной маршрутизации).
5. Назовите протоколы канальной маршрутизации.
6. Дайте понятие векторных алгоритмов маршрутизации.
7. Назовите векторные протоколы маршрутизации.
8. Дайте понятие протоколов принудительной маршрутизации.

4 Лабораторная работа №4. Протоколы RIP, RIPv2

Цель работы. Научиться настраивать динамическую маршрутизацию на основе протокола RIP. Выполнить задание в соответствии с вариантом.

4.1 Основные теоретические положения

Протокол маршрутизации RIP (Routing Information Protocol) является динамическим, внутридоменным, распределенным, одноуровневым, однопутевым и векторным [1]. Разработанный компанией Херох, он был одобрен другими производителями — 3Com, Apple, Banyan, Novell и Ungermann Bass. Этот протокол идеально подходит для малых и средних сетей, но не для крупных, поскольку максимальное число переходов ограничено числом 16. Протокол RIP не может оперативно учитывать изменения свойств сети (например, время задержки или загруженность каналов). Предполагается, что каждый маршрутизатор является отправной точкой нескольких маршрутов до сетей, с которыми он связан.

Если сеть однородна, то есть все каналы имеют равную пропускную способность и примерно равную загрузку, что типично для небольших локальных сетей, то число шагов до цели является разумной оценкой пути (метрикой).

Описания этих маршрутов хранятся в специальной таблице, называемой маршрутной. Таблица маршрутизации RIP содержит по записи на каждый маршрут. Запись должна включать в себя:

- IP-адрес места назначения;
- метрика маршрута (от 1 до 15; число шагов до места назначения);
- IP-адрес ближайшего маршрутизатора (gateway) по пути к месту назначения;
- таймеры маршрута.

Первым двум полям записи мы обязаны появлению термина вектор расстояния (место назначения - направление; метрика - модуль вектора). Периодически (раз в 30 сек) каждый маршрутизатор посылает широковещательно копию своей маршрутной таблицы всем соседям-маршрутизаторам, с которыми связан непосредственно. Маршрутизатор-получатель просматривает таблицу. Если в таблице присутствует новый путь или сообщение о более коротком маршруте, или произошли изменения длин пути, эти изменения фиксируются получателем в своей маршрутной таблице. Протокол RIP должен быть способен обрабатывать три типа ошибок [2].

1. Циклические маршруты. Так как в протоколе нет механизмов выявления замкнутых маршрутов, необходимо либо слепо верить партнерам, либо принимать меры для блокировки такой возможности.

2. Для подавления нестабильностей RIP должен использовать малое значение максимально возможного числа шагов (<16).

3. Медленное распространение маршрутной информации по сети создает проблемы при динамичном изменении маршрутной ситуации (система не поспевает за изменениями). Малое предельное значение метрики улучшает сходимость, но не устраняет проблему.

Несоответствие маршрутной таблицы реальной ситуации типично не только для RIP, но характерно для всех протоколов, базирующихся на векторе расстояния,

где информационные сообщения актуализации несут в себе только пары кодов - адрес места назначения и расстояние до него.

В RIP сообщения инкапсулируются в udp-дейтограммы, при этом передача осуществляется через порт 520. В качестве метрики RIP использует число шагов до цели. Если между отправителем и приемником расположено три маршрутизатора (gateway), считается, что между ними 4 шага. Такой вид метрики не учитывает различий в пропускной способности или загруженности отдельных сегментов сети. Применение вектора расстояния не может гарантировать оптимальность выбора маршрута, ведь, например, два шага по сегментам сети ethernet обеспечат большую пропускную способность, чем один шаг через последовательный канал на основе интерфейса RS-232.

Маршрут по умолчанию имеет адрес 0.0.0.0 (это верно и для других протоколов маршрутизации). Каждому маршруту ставится в соответствие таймер тайм-аута и "сборщика мусора". Тайм-аут-таймер сбрасывается каждый раз, когда маршрут инициализируется или корректируется. Если со времени последней коррекции прошло 3 минуты или получено сообщение о том, что вектор расстояния равен 16, маршрут считается закрытым. Но запись о нем не стирается, пока не истечет время "уборки мусора" (2мин). При появлении эквивалентного маршрута переключения на него не происходит, таким образом, блокируется возможность осцилляции между двумя или более равноценными маршрутами. Формат сообщения протокола RIP имеет вид, показанный на рисунке 4.1 [9].



Рисунок 4.1 - Формат сообщения RIP

Поле версия для RIP равно 1 (для RIP-2 двум). Поле набор протоколов сети i определяет набор протоколов, которые используются в соответствующей сети (для Интернет это поле имеет значение 2). Поле расстояние до сети i содержит целое число шагов (от 1 до 15) до данной сети. В одном сообщении может присутствовать информация о 25 маршрутах. При реализации RIP можно выделить следующие режимы.

1. Инициализация, определение всех "живых" интерфейсов путем отправки запросов, получение таблиц маршрутизации от других маршрутизаторов. Часто используются широковещательные запросы.

2. Получен запрос. В зависимости от типа запроса высылаются адресату полная таблица маршрутизации, или проводится индивидуальная обработка.

3. Получен отклик. Проводится коррекция таблицы маршрутизации (удаление, исправление, добавление).

4. Регулярные коррекции. Каждые 30 секунд вся или часть таблицы маршрутизации посылается всем соседним маршрутизаторам. Могут посылаться и специальные запросы при локальном изменении таблицы.

RIP достаточно простой протокол, но, к сожалению не лишенный следующих недостатков [1].

1. RIP не работает с адресами субсетей. Если нормальный 16-бит идентификатор ЭВМ класса В не равен 0, RIP не может определить является ли нулевая часть субсетевым ID, или полным IP-адресом.

2. RIP требует много времени для восстановления связи после сбоя в маршрутизаторе (минуты). В процессе установления режима возможны циклы.

3. Число шагов важный, но не единственный параметр маршрута, да и 15 шагов не предел для современных сетей.

4. Непосредственно подключенным соседним маршрутизаторам периодически рассылаются полные копии всей таблицы маршрутизации – в крупных сетях каждое обновление может сопровождаться значительным всплеском трафика.

Протокол RIP-2 (RFC-1388, 1993 год) является новой версией RIP, которая в дополнение к широковещательному режиму поддерживает мультикастинг; позволяет работать с масками субсетей, т.е. поддерживает бесклассовую маршрутизацию за счет включения маски подсети в обновления маршрутов.

На рисунке 4.2 представлен формат сообщения для протокола RIP-2 [9]. Поле маршрутный демон является идентификатором резидентной программы-маршрутизатора. Поле метка маршрута используется для поддержки внешних протоколов маршрутизации, сюда записываются коды автономных систем. При необходимости управления доступом можно использовать первые 20 байт с кодом набора протоколов сети 0xFFFF и меткой маршрута =2. Тогда в остальные 16 байт можно записать пароль.

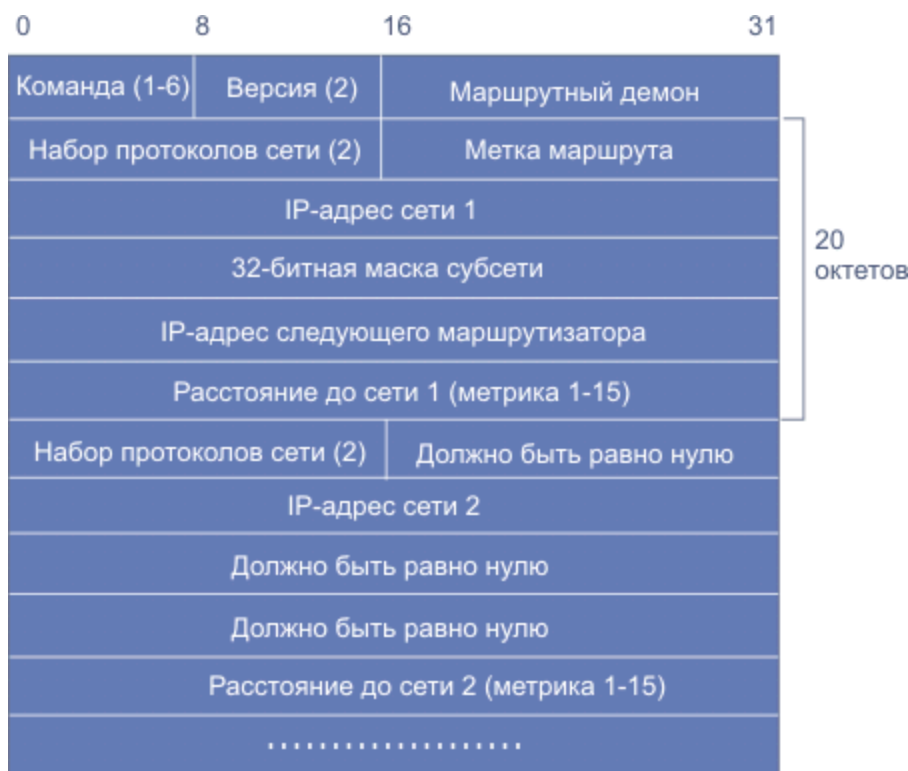


Рисунок 4.2 - Формат сообщений протокола RIP-2

Перед настройкой протокола RIP на маршрутизаторах необходимо присвоить IP-адреса и активировать все физические интерфейсы, которые будут участвовать в маршрутизации. На последовательных каналах необходимо установить тактовую

частоту главного маршрутизатора. Эти действия были сделаны в рамках третьей лабораторной работы.

Настройка RIP в самом общем случае заключается в выполнении трех команд:

- Router(config)#router rip;
- Router (config-router)#version 2;
- Router(config-router)#network [номер-сети].

Первая команда используется для включения протокола RIP на маршрутизаторе. Эту команду необходимо ввести в глобальном режиме настройки. В режиме настройки протокола маршрутизации RIP введите команду network, чтобы указать маршрутизатору состав сетей, участвующих в процессе маршрутизации RIP. Процесс маршрутизации связывает конкретные интерфейсы с номерами сетей и начинает отправку и прием обновлений RIP на этих интерфейсах.

По завершении настройки необходимо сравнить рабочую конфигурацию с точной схемой топологии для сверки номеров сетей и IP-адресов интерфейсов для обнаружения возможных механических ошибок, допущенных при вводе IP-адресов.

Проверить функционирование протокола RIP в сети можно несколькими способами.

Если конфигурация верна, то для проверки работоспособности маршрутизации можно отправить эхо-запросы командой ping на устройства в удаленных сетях. Успешное выполнение команды ping будет свидетельством работоспособности маршрутизации.

Выполните команды для проверки IP-маршрутизации show ip protocols и show ip route в приглашении командной строки.

Команда show ip protocols позволяет убедиться в верности настройки маршрутизации RIP, использовании соответствующих интерфейсов для отправки и приема обновлений RIP, а также правильном составе сетей в оповещениях.

Команда show ip route выводит таблицу маршрутизации, по которой можно проверить присутствие маршрутов, полученных соседними маршрутизаторами.

4.2 Рабочее задание

Необходимо настроить динамическую маршрутизацию на основе протокола RIP в соответствии с вариантом указанным в таблице 3.1 лабораторной работы №3. При правильной настройке маршрутизации все компьютеры должны иметь возможность успешно отправлять icmp запросы друг другу.

4.3 Контрольные вопросы

1. Охарактеризуйте протокол динамической маршрутизации RIP.
2. Дайте понятие маршрутной таблицы протокола RIP.
3. Назовите три типа ошибок, которые протокол RIP способен обрабатывать.
4. Какую характеристику RIP использует в качестве метрики?
5. В какой случае маршрут считается закрытым ?
6. Опишите формат сообщения протокола RIP первой версии.
7. Какие режимы можно выделить при реализации протокола RIP ?
8. Перечислите недостатки протокола RIP первой версии.
9. В чем разница протоколов RIP первой и второй версии ?
10. Опишите формат сообщения протокола RIPv2.
11. Опишите настройку протокола RIP в самом общем случае.
12. Какие команды используются для проверки работы протокола RIP ?

5 Лабораторная работа №5. Протоколы IGRP, EIGRP

Цель работы. Научиться настраивать динамическую маршрутизацию на основе протокола EIGRP. Выполнить задание в соответствии с вариантом.

5.1 Основные теоретические положения

Протокол маршрутизации IGRP (Interior Gateway Routing Protocol) является динамическим, внутрисетевым, распределенным, одноуровневым, многопутевым и векторным [1]. Он разработан компанией Cisco Systems для применения в сложных сетях в пределах автономной системы. При выборе маршрутов учитывается множество факторов, например пропускная способность сети, ее надежность и загруженность, а также размеры сообщений. Администратор сети назначает вес каждого параметра для принятия решения, либо протокол работает с параметрами по умолчанию.

IGRP является протоколом внутренних роутеров (IGP) с вектором расстояния. Для выбора маршрута в IGRP используется комбинация показателей, таких как задержка сети, полоса пропускания, надежность и загруженность сети. Весовой коэффициент этих показателей может выбираться автоматически или задаваться администратором сети. Для надежности и загруженности сети это значения от 1 до 255, полоса пропускания — от 1200 бит/сек до 10 Гбит/сек, задержка может принимать значение до 24-го порядка.

Основные достоинства протокола [2]:

- стабильность маршрутов даже в очень больших и сложных сетях;
- быстрый отклик на изменения топологии сети;
- минимальная избыточность. Поэтому IGRP не требует дополнительной пропускной способности каналов для своей работы;
- разделение потока данных между несколькими параллельными маршрутами, примерно равного достоинства;
- учет частоты ошибок и уровня загрузки каналов;
- возможность реализовать различные виды сервиса для одного и того же набора информации.

Для повышения стабильности работы IGRP предусматривает такие механизмы, как удержание изменений, расщепленный горизонт (split-horizon) и корректировка отмены.

Удержание изменений имеется ввиду когда в сеть поступает информация об изменениях маршрутов (например, об обрыве связи) от одного из роутеров, то изменения в таблицы маршрутизации поступают не мгновенно, а в течение некоторого времени. В этот период роутер, ещё не получивший информацию об изменениях, может продолжать распространять информацию об уже несуществующем маршруте. При этом возможна ситуация, когда устройство, уже внесшее изменения в свою таблицу маршрутизации, после получения этих данных внесёт повторную корректировку в таблицу. Временное удержание изменений — это механизм, по которому удерживаются все изменения, которые могут повлиять на маршруты в течение некоторого времени. Время удержания должно быть больше времени, необходимого для того, чтобы информация об измененных маршрутах распространилась по всем роутерам системы [6].

Суть механизма расщепленного горизонта (split-horizon) состоит в том, для предотвращения заикливания маршрутов между соседними роутерами, информация об изменении маршрута не должна распространяться в направлении того роутера, от которого она пришла.

Корректировка отмены маршрута (route-poisoning) — это принудительное удаление маршрута и перевод в состояние удержания, применяется для борьбы с маршрутными петлями.

Таймер корректировки определяет, как часто должны отправляться сообщения о корректировке маршрутов. Таймер недействующих маршрутов определяет, сколько времени должен ожидать роутер при отсутствии сообщений о корректировке какого-нибудь конкретного маршрута, прежде чем объявить этот маршрут недействующим. Время по умолчанию IGRP для этой переменной в три раза превышает период корректировки. Переменная величина времени удерживания определяет промежуток времени удерживания. Время по умолчанию IGRP для этой переменной в три раза больше периода таймера корректировки, плюс 10 сек. И наконец, таймер отключения указывает, сколько времени должно пройти прежде, чем какой-нибудь роутер должен быть исключен из маршрутной таблицы. Время по

умолчанию IGRP для этой величины в семь раз превышает период корректировки маршрутизации.

Метрика, используемая в IGRP, учитывает:

- время задержки;
- пропускную способность самого слабого сегмента пути (в битах в сек);
- загруженность канала (относительную);
- надежность канала (определяется долей пакетов, достигших места назначения неповрежденными).

Время задержки предполагается равным времени, необходимому для достижения места назначения при нулевой загрузке сети. Дополнительные задержки, связанные с загрузкой учитываются отдельно.

Среди параметров, которые контролируются, но не учитываются метрикой, находятся число шагов до цели и MTU (maximum transfer unit - размер пакета пересылаемого без фрагментации). Расчет метрики производится для каждого сегмента пути [3].

Время от времени каждый маршрутизатор широковещательно рассылает свою маршрутную информацию всем соседним маршрутизаторам. Получатель сравнивает эти данные с уже имеющимися и вносит, если требуется, необходимые коррекции. На основании вновь полученной информации могут быть приняты решения об изменении маршрутов. Эта процедура типична для многих маршрутизаторов и этот алгоритм носит имя Белмана-Форда. (см. также описание протокола RIP, RFC-1058). Наилучший путь выбирается с использованием комбинированной метрики.

Путь, имеющий наименьшую комбинированную метрику, считается лучшим. В такой схеме появляется возможность, используя весовые коэффициенты, адаптировать выбор маршрутов к задачам конечного пользователя.

Одним из преимуществ IGRP является простота реконфигурации. В IGRP маршрут по умолчанию не назначается, а выбирается из числа кандидатов.

Когда маршрутизатор включается, его маршрутные таблицы инициализируются оператором вручную или с использованием специальных файлов.

Сообщения об изменении маршрута, направленные какому-то маршрутизатору, не должны содержать данных об объектах, непосредственно с ним связанных [4]. Сообщения об изменении маршрутов должны содержать:

- адреса сетей, с которыми маршрутизатор связан непосредственно;
- пропускную способность каждой из сетей;
- топологическую задержку каждой из сетей;
- надежность передачи пакетов для каждой сети;
- загруженность канала для каждой сети;
- MTU для каждой сети.

Следует еще раз обратить ваше внимание, что в IGRP не используется измерение задержек, измеряется только надежность и коэффициент загрузки канала. Надежность определяется на основе сообщений интерфейсов о числе ошибок.

Существует 4 временные константы, управляющие процессом распространения маршрутной информации (эти константы определяются оператором сети) [5]:

- период широковещательных сообщений об изменении маршрутов (это время по умолчанию равно 90 сек);

- время существования - если за это время не поступило никаких сообщений о данном маршруте, он считается нерабочим. Это время в несколько раз больше периода сообщений об изменениях (по умолчанию в 3 раза);

- время удержания - когда какой-то адресат становится недостижим, он переходит в режим выдержки. В этом режиме никакие новые маршруты, ведущие к нему, не воспринимаются. Длительность этого режима и называется временем удержания. Обычно это время в три раза дольше периода сообщений об изменениях маршрутов;

- время удаления - если в течение данного времени не поступило сообщений о доступе к данному адресату, производится удаление записи о нем из маршрутной базы данных (по умолчанию это время в 7 раз больше периода сообщений об изменениях маршрутов).

В начале 90-х годов разработана новая версия протокола IGRP - EIGRP с улучшенным алгоритмом оптимизации маршрутов, сокращенным временем установления и масками субсетей переменной длины.

В частности, по отношению к протоколу IGRP обеспечиваются следующие дополнительные возможности [1]:

- поддержка внеклассовых IP сетей;
- передача частичных обновлений таблицы маршрутов;
- поддержка различных протоколов сетевого уровня.

Формально протокол EIGRP относится к алгоритмам маршрутизации типа distant – vector, однако этот протокол сочетает в себе лучшие качества протокола типа link- state и поэтому может быть отнесен к особому типу протоколов маршрутизации – к гибридным протоколам.

EIGRP поддерживает многие протоколы сетевого уровня. Рассылка маршрутной информации здесь производится лишь при изменении маршрутной ситуации. Протокол периодически рассылает соседним маршрутизаторам короткие сообщения Hello. Получение отклика означает, что сосед функционален и можно осуществлять обмен маршрутной информацией. Протокол EIGRP использует таблицы соседей (адрес и интерфейс), топологические таблицы (адрес места назначения и список соседей, объявляющих о доступности этого адреса), состояния и метки маршрутов. Для каждого протокольного модуля создается своя таблица соседей. Протоколом используется сообщения типа hello (мультикастная адресация), подтверждении (acknowledgment), актуализация (update), запрос (query; всегда мультикастный) и отклик (reply; посылается отправителю запроса). Маршруты здесь делятся на внутренние и внешние - полученные от других протоколов или записанные в статических таблицах. Маршруты помечаются идентификаторами их начала. Внешние маршруты помечаются следующей информацией:

- идентификатор маршрутизатора EIGRP, который осуществляет рассылку информации о маршруте;
- номер AS, где расположен адресат маршрута;
- метка администратора;

- идентификатор протокола;
- метрика внешнего маршрута;
- битовые флаги маршрута по умолчанию.

Протокол EIGRP полностью совместим с IGRP, он обеспечивает работу в сетях IP, Apple Talk и Novell.

В отличие от RIP, EIGRP не ограничивается использованием содержимого таблицы маршрутизации маршрутизатора. Для EIGRP создаются две дополнительные таблицы базы данных: таблица соседних маршрутизаторов и таблица топологии [2].

В таблице соседних маршрутизаторов хранятся данные о соседних маршрутизаторах в локальных сетях, подключенных напрямую. Эта таблица содержит такую информацию, как IP-адрес, тип и полоса пропускания интерфейса.

EIGRP формирует таблицу топологии на основе извещений от соседних маршрутизаторов. Таблица топологии содержит все маршруты, объявленные соседними маршрутизаторами. Для расчета кратчайшего пути по сети к месту назначения в протоколе EIGRP применяется алгоритм диффузионного обновления (DUAL). Рассчитанный путь помещается в таблицу маршрутизации. Таблица топологии позволяет маршрутизатору, на котором используется протокол EIGRP, определять оптимальный альтернативный маршрут при изменениях в сети. Если в таблице маршрутизации отсутствуют альтернативные маршруты, EIGRP опрашивает соседние маршрутизаторы для нахождения нового маршрута к месту назначения.

В отличие от протокола RIP, предназначенного для небольших сетей, в которых число участков между маршрутизаторами не превышает 15, протокол EIGRP наилучшим образом подходит для крупных более сложных сетей, объединяющих до 224 участков и требующих быстрого схождения.

5.2 Рабочее задание

Необходимо настроить динамическую маршрутизацию на основе протокола EIGRP в соответствии с вариантом указанным в таблице 3.1 лабораторной работы №3. При правильной настройке маршрутизации все компьютеры должны иметь возможность успешно отправлять icmp запросы друг другу.

Перед настройкой протокола EIGRP на маршрутизаторах необходимо присвоить IP-адреса и активировать все физические интерфейсы, которые будут участвовать в маршрутизации. На последовательных каналах необходимо установить тактовую частоту главного маршрутизатора. Эти действия были сделаны в рамках третьей лабораторной работы.

Настройка EIGRP заключается в выполнении следующих команд:

- Router(config)#router eigrp [номер автономной системы];
- Router(config-router)#network [номер сети].

Первая команда используется для включения протокола EIGRP на маршрутизаторе. Эту команду необходимо ввести в глобальном режиме настройки.

Также для включения процесса EIGRP необходим параметр автономной системы. Этому параметру AS можно назначить любое 16-разрядное значение, и он означает все маршрутизаторы одной компании или организации. Несмотря на то, что EIGRP рассматривает параметр как номер автономной системы, он фактически выступает в роли идентификатора процесса. Этот номер AS имеет только локальное значение и отличен от номера автономной системы, выдаваемого и контролируемого Комитетом по цифровым адресам в Интернете (IANA).

Номер AS в команде должен совпадать для всех маршрутизаторов, участвующих в процессе маршрутизации EIGRP.

В режиме настройки протокола маршрутизации EIGRP введите команду network, чтобы указать маршрутизатору состав сетей, участвующих в процессе маршрутизации EIGRP. Процесс маршрутизации связывает конкретные интерфейсы с номерами сетей и начинает отправку и прием обновлений RIP на этих интерфейсах.

По завершении настройки необходимо сравнить рабочую конфигурацию с точной схемой топологии для сверки номеров сетей и IP-адресов интерфейсов для обнаружения возможных механических ошибок, допущенных при вводе IP-адресов.

Проверить функционирование протокола EIGRP в сети можно несколькими способами.

Если конфигурация верна, то для проверки работоспособности маршрутизации можно отправить эхо-запросы командой `ping` на устройства в удаленных сетях. Успешное выполнение команды `ping` будет свидетельством работоспособности маршрутизации.

Выполните команды для проверки IP-маршрутизации `show ip protocols` и `show ip route` в приглашении командной строки.

Команда `show ip protocols` позволяет убедиться в верности настройки маршрутизации EIGRP, использовании соответствующих интерфейсов для отправки и приема обновлений EIGRP, а также правильном составе сетей в оповещениях.

Команда `show ip route` выводит таблицу маршрутизации, по которой можно проверить присутствие маршрутов, полученных соседними маршрутизаторами.

5.3 Контрольные вопросы

1. Дайте понятие протокола маршрутизации IGRP.
2. Какие показатели протокол IGRP использует для выбора маршрута ?
3. Перечислите основные достоинства протокола IGRP.
4. Какие механизмы протокол IGRP использует для повышения стабильности своей работы ?
5. Опишите удержание изменений, как механизм повышения стабильности работы протокола IGRP.
6. Опишите расщепленный горизонт (split-horizon), как механизм повышения стабильности работы протокола IGRP.
7. Опишите корректировку отмены маршрута (route-poisoning), как механизм повышения стабильности работы протокола IGRP.

8. Дайте понятие таймера недействующих маршрутов.
9. Какие параметры учитывает метрика, используемая в IGRP ?
10. Что должны содержать сообщения об изменении маршрутов ?
11. Какие существуют временные константы, управляющие процессом распространения маршрутной информации ?
12. Какие дополнительные возможности по отношению к протоколу IGRP обеспечиваются при использовании протокола EIGRP ?
13. Какой информацией помечаются внешние маршруты ?
14. Какие две дополнительные таблицы, помимо таблицы маршрутов, создаются протоколом EIGRP ?
15. Какое количество транзитных переходов обеспечивает протокол EIGRP ?

6 Лабораторная работа №6. Протокол OSPF

Цель работы. Научиться настраивать динамическую маршрутизацию на основе протокола OSPF. Выполнить задание в соответствии с вариантом.

6.1 Основные теоретические положения

Протокол маршрутизации OSPF (Open Shortest Path First) является динамическим, внутрисетевым, распределенным, иерархическим, многопутевым и канальным [1]. При изменении таблицы состояния канала OSPF-маршрутизаторы обмениваются обновлениями. Для выявления сбоев маршрутизатор рассылает сообщения “еще жив”. Протокол OSPF поддерживает запросы QoS (quality of service), когда приложение сообщает о срочности некоторых данных. В этом случае OSPF может по своему усмотрению использовать имеющиеся каналы, чтобы как можно быстрее отправить данные.

Протокол OSPF представляет собой протокол внутреннего шлюза (Interior Gateway Protocol — IGP). Протокол OSPF распространяет информацию о доступных маршрутах между маршрутизаторами одной автономной системы.

OSPF имеет следующие преимущества [2]:

- отсутствие ограничений на размер сети;
- передачу обновлений маршрутов с использованием адресов типа multicast;
- высокая скорость сходимости по сравнению с дистанционно-векторными протоколами маршрутизации;
- поддержка сетевых масок переменной длины (VLSM);
- оптимальное использование пропускной способности;
- использование алгоритма SPF для расчета пути к месту назначения с наименьшей стоимостью;
- рассылка обновлений маршрутов только при изменении топологии;
- периодическая рассылка полной таблицы маршрутизации не производится;
- аутентификация маршрутов.

В сетях с поддержкой OSPF маршрутизаторы обмениваются извещениями о состоянии каналов связи, информируя друг друга о таких изменениях, как:

- добавление нового соседнего маршрутизатора;
- выход из строя канала;
- восстановление канала.

При изменении топологии сети, например, при выходе из строя одного из каналов или при добавлении нового маршрутизатора, все маршрутизаторы, на которых влияет данное изменение, рассылают остальным маршрутизаторам сети извещения LSA для обновления маршрутов. Все маршрутизаторы вносят соответствующие изменения в базы данных топологий, перестраивают деревья SPF для поиска кратчайшего пути к каждой сети и обновляют маршруты в своих таблицах маршрутизации.

Протокол OSPF является альтернативой RIP в качестве внутреннего протокола маршрутизации. OSPF представляет собой протокол состояния маршрута (в качестве метрики используется - коэффициент качества обслуживания). Каждый маршрутизатор обладает полной информацией о состоянии всех интерфейсов всех маршрутизаторов (переключателей) автономной системы. Протокол OSPF

реализован в демоне маршрутизации gated, который поддерживает также RIP и внешний протокол маршрутизации BGP [1].

Автономная система может быть разделена на несколько областей, куда могут входить как отдельные ЭВМ, так и целые сети. В этом случае внутренние маршрутизаторы области могут и не иметь информации о топологии остальной части AS. Сеть обычно имеет выделенный (designated) маршрутизатор, который является источником маршрутной информации для остальных маршрутизаторов AS. Каждый маршрутизатор самостоятельно решает задачу оптимизации маршрутов. Если к месту назначения ведут два или более эквивалентных маршрута, информационный поток будет поделен между ними поровну. Переходные процессы в OSPF завершаются быстрее, чем в RIP. В процессе выбора оптимального маршрута анализируется ориентированный граф сети.

Распределение нагрузки между параллельными каналами (Load balancing) заключается в следующем. При использовании протокола маршрутизации OSPF допускается существование нескольких маршрутов в направлении некоторого узла сети. В том случае, если эти маршруты обеспечивают одинаковое качество передачи данных, информационный поток в адрес данного узла может быть направлен по всем этим каналам одновременно, что обеспечит существенное увеличение скорости передачи данных.

Использование процедуры установления подлинности целесообразно в тех информационных системах, в которых большое внимание уделяется информационной безопасности. В таких системах маршрутизаторы, которые участвуют в процессе определения маршрута, должны выполнить совокупность действий, которая необходима для установления приемником подлинности источника передаваемых данных (authentication procedure). Только в том случае, если источник передаваемых данных успешно выполнил процедуру аутентификации, те данные о маршрутах, которые были от него получены, принимаются для обработки.

Существуют следующие способы организации обмена информацией о маршрутах [2].

1. Использование адресов типа multicast для информационного обмена между маршрутизаторами в процессе определения маршрута. Использование таких адресов позволяет отказаться от использования адресов типа broadcast, что в свою очередь приводит к повышению эффективности использования вычислительных ресурсов сети.

2. Использование аппарата «назначенных» (designated) маршрутизаторов. Использование этой возможности позволяет существенно сократить объем служебного трафика в том случае, когда несколько маршрутизаторов подключены к одной сети.

В отличие от протокола маршрутизации RIP, который для сравнения маршрутов может использовать только их длину, выраженную в числе переходов, протокол маршрутизации OSPF использует для этой – же цели специальный критерий, который называется метрика. Метрика маршрута в протоколе OSPF формируется по специальному алгоритму и учитывает следующие параметры:

- пропускная способность канала;
- величина задержки распространения сигнала в канале;
- надежность канала;
- загруженность канала;
- размер максимального блока данных, который может быть передан через данный канал.

Использование такой метрики позволяет более объективно оценивать маршруты и, при наличии выбора, принимать эффективное и целесообразное решение.

Для обеспечения формирования и обслуживания этих баз данных маршрутизаторы OSPF должны обмениваться специальными сообщениями. В частности такие сообщения формируются в том случае, если в сети появился новый маршрутизатор или изменилось состояние канала передачи данных. При получении сообщения об изменениях в структуре сети, каждый маршрутизатор вносит соответствующие изменения в свою копию базы данных. Таким образом, в каждый момент времени все базы данных маршрутизаторов, которые находятся внутри

одной автономной системы, являются идентичными и адекватно отображают структуру информационного взаимодействия внутри автономной системы. Для того, чтобы определить маршрут по которому должен быть передана дейтаграмма, каждый маршрутизатор, на основании своей копии базы данных, строит дерево кратчайших путей. В вершине своего дерева каждый из маршрутизаторов размещает себя самого.

При описании алгоритма OSPF используются несколько следующих специальных терминов и понятий [1].

1. Autonomous System (AS), автономной системой называется группа маршрутизаторов, которая для обеспечения взаимного обмена информацией о маршрутах использует единый протокол маршрутизации.

2. Neighboring Routers - маршрутизаторы, которые подключены к одной и той же сети называются соседними маршрутизаторами.

3. Adjacency - два маршрутизатора из числа соседних могут быть выбраны для установления близких отношений, которые предполагают обмен информацией о маршрутах. Близкие отношения устанавливаются не в каждой паре соседствующих маршрутизаторов.

4. Link State Advertisement (LSA) - блок данных, который содержит информацию о состоянии маршрутизатора или сети называется объявлением о состоянии канала. В том случае, если данное объявление представляет состояние маршрутизатора, оно должно содержать информацию о статусе его интерфейсов и близких ему маршрутизаторов. Каждое такое объявление распространяется по всей автономной системе. Совокупность таких LSA формирует базу данных маршрутизации в каждом из маршрутизаторов.

5. Flooding - процесс распространения LSA в пределах автономной системы называется затоплением.

Одним из компонентов протокола OSPF является Hello протокол, с помощью которого маршрутизаторы устанавливают и обслуживают соседские отношения. С помощью этого протокола, в частности производится выбор назначенного маршрутизатора для некоторых сетей.

Возможно возникновение ситуации, когда к одной сети типа broadcast окажутся подключенными несколько входящих в один домен маршрутизации OSPF маршрутизаторов. Для того, чтобы избежать дублирования представления сети типа broadcast несколькими маршрутизаторами в протоколе OSPF используется специальный алгоритм, с помощью которого выбирается Designated Router (назначенный маршрутизатор, DR). В этом случае только один маршрутизатор обеспечивает передачу информации о маршрутах в сегменте сети.

В сетях со множественным доступом отношения соседства устанавливаются между всеми маршрутизаторами. Если бы все маршрутизаторы в состоянии соседства обменивались топологической информацией, это привело бы к рассылке большого количества копий LSA. Если, к примеру, количество маршрутизаторов в сети со множественным доступом равно n , то будет установлено $n(n-1)/2$ отношений соседства. Каждый маршрутизатор будет рассылать $n-1$ LSA своим соседям, плюс одно LSA для сети, в результате сеть сгенерирует n^2 LSA [8].

Для предотвращения проблемы рассылки копий LSA в сетях со множественным доступом выбираются выделенный маршрутизатор (DR) и запасной выделенный маршрутизатор (BDR).

Выделенный маршрутизатор управляет процессом рассылки LSA в сети. Каждый маршрутизатор сети устанавливает отношения смежности с DR. Информация об изменениях в сети отправляется DR маршрутизатором, обнаружившим это изменение, а DR отвечает за то, чтобы эта информация была отправлена остальным маршрутизаторам сети.

Недостатком в схеме работы с DR маршрутизатором является то, что при выходе его из строя должен быть выбран новый DR. Новые отношения соседства должны быть сформированы и, пока базы данных маршрутизаторов не синхронизируются с базой данных нового DR, сеть будет недоступна для пересылки пакетов. Для устранения этого недостатка выбирается BDR.

Существует также резервный выделенный маршрутизатор (backup designated router, BDR). Каждый маршрутизатор сети устанавливает отношения соседства не только с DR, но и BDR. DR и BDR также устанавливают отношения соседства и

между собой. При выходе из строя DR, BDR становится DR и выполняет все его функции. Так как маршрутизаторы сети установили отношения соседства с BDR, время недоступности сети минимизируется.

Маршрутизатор, выбранный DR или BDR в одной присоединённой к нему сети со множественным доступом, может не быть DR (BDR) в другой присоединённой сети. Роль DR (BDR) является свойством интерфейса, а не свойством всего маршрутизатора.

Протокол OSPF относится к протоколам, которые обеспечивают иерархическую маршрутизацию. При использовании протоколов данного типа информационная система разбивается на независимые области по функциональному принципу. Как уже было выше отмечено, область №0 играет роль backbone и используется для обеспечения информационного взаимодействия между остальными областями.

В зависимости от того, к какой области принадлежит маршрутизатор, и какие информационные потоки через него проходят, различают четыре типа маршрутизаторов OSPF [10]:

- Internal Router – IR;
- Area Border Router – ABR;
- Backbone Router – BR;
- AS Boundary Router – ASBR.

Маршрутизаторы типа Internal Router – внутренний маршрутизатор – размещаются внутри автономной системы и не имеют интерфейсов, которые выходят за пределы этой автономной системы. На приведенном рисунке маршрутизаторы этого типа обозначены буквами IR.

К маршрутизаторам Backbone Router относятся все маршрутизаторы, которые имеют интерфейсы в нулевую область.

Маршрутизаторы типа Area Border Router (пограничный маршрутизатор области) – размещаются на границе между несколькими областями в пределах автономной системы. Такие маршрутизаторы имеют интерфейсы, которые связывают их с маршрутизаторами, находящимися в других областях.

Маршрутизаторы данного типа обозначены на рисунке ABR и предназначены для того, чтобы передавать информацию о маршрутах между различными областями.

Маршрутизаторы типа AS Boundary Router (пограничный маршрутизатор автономной системы) обеспечивают информационный обмен с маршрутизаторами, которые расположены в других автономных системах.

База данных Link-State Database отображает текущую структуру информационных связей в рассматриваемой области маршрутизации. Эти базы данных должны быть идентичными у всех маршрутизаторов, которые расположены в пределах одной области. Базы данных состоят из сообщений, которые называются Link – State Advertisement и формируются всеми активными маршрутизаторами данной области. Активным в данном случае считается маршрутизатор, который имеет хотя бы один подключенный канал в данной области.

Сообщения, в которых содержатся LSA, формируются при каждом изменении состояния канала и передаются всеми маршрутизаторами данной области методом затопления. Для формирования базы данных используются различные типы LSA [9]:

- LSA типа 1 - router link advertisement;
- LSA типа 2 - network link advertisement;
- LSA типа 3, 4 - summary link advertisement;
- LSA типа 5 - external link advertisement;
- LSA типа 6 - multicast OSPF LSA;
- LSA типа 7 - AS external LSA for NSSA;
- LSA типа 8 - link LSA.

Сообщения типа 1 - router link advertisement (состояния каналов маршрутизатора) формируются каждым маршрутизатором для каждой области, в которой он имеет активные интерфейсы. Сообщения LSA типа 1 содержат объединенную информацию о состоянии каналов, которые имеет маршрутизатор в данной области. Сообщения этого типа распространяются только в пределах одной области.

Сообщения LSA типа 2 - network link advertisement (состояние сети) формируется только в сетях, которые могут быть отнесены к классу broadcast

(Ethernet) или NBMA (Non Broadcast Multi Access). В сообщении LSA типа 2 указываются идентификаторы всех маршрутизаторов, подключенных к данной сети. Формирование сообщений данного типа выполняется маршрутизатором, который называется Designated Router. Выбор этого маршрутизатора выполняется по специальному алгоритму среди всех маршрутизаторов, которые подключены к данной сети.

Сообщения LSA типа 3, 4 – summary link advertisement формируются Area Border Router – маршрутизаторами и направляются за пределы области, в которой они сформированы. Каждое сообщение данного типа содержит маршрут, который может быть использован для информационного обмена между различными областями в пределах одной автономной системы. В частности, LSA типа 3 описывают маршруты к сетям, LSA типа 4 описывают маршруты к AS Boundary Router – маршрутизаторам.

Сообщения LSA типа 5 - external link advertisement формируются AS Boundary Router- маршрутизаторами и содержат информацию о маршрутах, которые являются внешними по отношению к данной автономной системе. Сообщения данного типа распространяются по всем областям автономной системы за исключением отдельных специально сконфигурированных областей, которые называются stub-areas.

Сообщения LSA типа 6 — Multicast OSPF LSA, специализированный LSA, который используют мультикаст OSPF приложения .

Сообщения LSA типа 7Type - AS external LSA for NSSA это объявления о состоянии внешних каналов автономной системы в NSSA зоне. Оно может передаваться только в NSSA зоне. На границе зоны пограничный маршрутизатор преобразует type 7 LSA в type 5 LSA.

Сообщения LSA типа 8 - link LSA, анонсирует link-local адрес и префикс(ы) маршрутизатора всем маршрутизаторам разделяющим канал (link). Отправляется только если на канале присутствует более чем один маршрутизатор. Распространяются только в пределах канала (link).

Помимо установления партнерских отношений данный протокол используется для регулярного подтверждения наличия двустороннего обмена между маршрутизаторами. Для этого пакеты Hello периодически отправляются через все интерфейсы маршрутизатора. В пакете Hello маршрутизатор размещает IP адреса соседей, от которых он получил сообщения Hello. Двусторонний характер обмена заключается в том, что маршрутизатор должен обнаружить в принятом от партнера пакете Hello свой собственный идентификатор.

В broadcast и NBMA сетях данный протокол используется для выбора назначенного маршрутизатора. Процедуры, которые маршрутизатор выполняет в рамках протокола Hello, являются различными в сетях различного типа.

В broadcast сетях маршрутизатор периодически заявляет о себе путем передачи пакетов адресованных в адрес типа multicast. В данном случае эти пакеты Hello содержат представления данного маршрутизатора по поводу кандидатуры назначенного маршрутизатора, а также, список маршрутизаторов, от которых были получены пакеты Hello в течение установленного интервала времени.

При разделении автономной системы на зоны, маршрутизаторам принадлежащим к одной зоне не известна информация о детальной топологии других зон [4].

Разделение на зоны позволяет:

- снизить нагрузку на ЦП маршрутизаторов за счёт уменьшения количества перерасчётов по алгоритму OSPF;
- уменьшить размер таблиц маршрутизации;
- уменьшить количество пакетов обновлений состояния канала.

Каждой зоне присваивается идентификатор зоны (area ID). Идентификатор может быть указан в десятичном формате или в формате записи IP-адреса. Однако идентификаторы зон не являются IP-адресами и могут совпадать с любым назначенным IP-адресом.

Существует несколько типов зон приведенных далее [2].

1. Магистральная зона или backbone area (известная также как нулевая зона или зона 0.0.0.0) формирует ядро сети OSPF. Все остальные зоны соединены с ней, и

межзональная маршрутизация происходит через маршрутизатор соединенный с магистральной зоной. Магистральная зона ответственна за распространение маршрутизирующей информации между немагистральными зонами. Магистральная зона должна быть смежной с другими зонами, но она не обязательно должна быть физически смежной; соединение с магистральной зоной может быть установлено и с помощью виртуальных каналов.

2. Стандартная зона (standard area) - обычная зона, которая создается по умолчанию. Эта зона принимает обновления каналов, суммарные маршруты и внешние маршруты.

3. Тупиковая зона (stub area) не принимает информацию о внешних маршрутах для автономной системы, но принимает маршруты из других зон. Если маршрутизаторам из тупиковой зоны необходимо передавать информацию за границу автономной системы, то они используют маршрут по умолчанию. В тупиковой зоне не может находиться ASBR. Исключение из этого правила — ABR может быть и ASBR.

Totally stubby area не принимает информацию о внешних маршрутах для автономной системы и маршруты из других зон. Если маршрутизаторам необходимо передавать информацию за пределы зоны, то они используют маршрут по умолчанию.

Not-so-stubby area (NSSA) определяет дополнительный тип LSA — LSA type 7. В NSSA зоне может находиться ASBR.

Сообщения об изменениях маршрутов могут быть вызваны следующими причинами:

- возраст маршрута достиг предельного значения (lsrefreshtime);
- изменилось состояние интерфейса;
- произошли изменения в маршрутизаторе сети;
- произошло изменение состояния одного из соседних маршрутизаторов;
- изменилось состояние одного из внутренних маршрутов (появление нового, исчезновение старого и т.д.);
- произошло изменение состояния межзонного маршрута.

- появление нового маршрутизатора, подключенного к сети.
- вариация виртуального маршрута одним из маршрутизаторов.
- возникли изменения одного из внешних маршрутов;
- маршрутизатор перестал быть пограничным для данной аs (например, перезагрузился).

Маршрутная таблица OSPF содержит в себе:

- IP-адрес места назначения и маску;
- тип места назначения (сеть, граничный маршрутизатор и т.д.);
- тип функции (возможен набор маршрутизаторов для каждой из функций TOS);
- область (описывает область, связь с которой ведет к цели, возможно несколько записей данного типа, если области действия граничных маршрутизаторов перекрываются);
- тип пути (характеризует путь как внутренний, межобластной или внешний, ведущий к AS);
- цена маршрута до цели;
- очередной маршрутизатор, куда следует послать дейтограмму;
- объявляющий маршрутизатор (используется для межобластных обменов и для связей автономных систем друг с другом).

Преимущества OSPF приведены далее.

1. Для каждого адреса может быть несколько маршрутных таблиц, по одной на каждый вид IP-операции (TOS).
2. Каждому интерфейсу присваивается безразмерная цена, учитывающая пропускную способность, время транспортировки сообщения. Для каждой IP-операции может быть присвоена своя цена (коэффициент качества).
3. При существовании эквивалентных маршрутов OSPF распределяет поток равномерно по этим маршрутам.
4. Поддерживается адресация субсетей (разные маски для разных маршрутов).
5. При связи точка-точка не требуется IP-адрес для каждого из концов, что экономит адресов.

6. Применение мультикастинга вместо широковещательных сообщений снижает загрузку не вовлеченных сегментов.

К недостаткам OSPF относят:

- трудности в получении информации о предпочтительности каналов для узлов, поддерживающих другие протоколы, или со статической маршрутизацией;
- OSPF является лишь внутренним протоколом.

6.2 Рабочее задание

Необходимо настроить динамическую маршрутизацию на основе протокола OSPF в соответствии с вариантом указанным в таблице 3.1 лабораторной работы №3. При правильной настройке маршрутизации все компьютеры должны иметь возможность успешно отправлять icmp запросы друг другу.

Перед настройкой протокола OSPF на маршрутизаторах необходимо присвоить IP-адреса и активировать все физические интерфейсы, которые будут участвовать в маршрутизации. На последовательных каналах необходимо установить тактовую частоту главного маршрутизатора. Эти действия были сделаны в рамках третьей лабораторной работы.

Настройка базового протокола OSPF не является сложной задачей и состоит только из двух шагов. Первый шаг - включение процесса маршрутизации OSPF. Второй шаг - определение сетей, которые должны быть объявлены:

- Router(config)#router ospf [id процесса];
- Router(config-router)#network [адрес сети] [групповая маска] область [id области].

Первая команда используется для включения протокола OSPF на маршрутизаторе. Эту команду необходимо ввести в глобальном режиме настройки.

Также для включения протокола OSPF необходимо указать идентификатор процесса, который выбирается администратором, он может представлять собой любое число в диапазоне от 1 до 65535. Идентификатор процесса имеет только локальное значение и необязательно должен совпадать с идентификатором других маршрутизаторов OSPF.

Команда `network` имеет такую же функцию, как в других протоколах маршрутизации IGP. Этой командой определяются интерфейсы, которые могут посылать и принимать пакеты OSPF. Данная инструкция определяет сети, включаемые в обновления маршрутизации OSPF.

В команде `OSPF network` используется сочетание сетевого адреса и групповой маски. Сетевой адрес, наряду с групповой маской, указывает адрес интерфейса, или диапазон адресов, который будет включен для OSPF.

Идентификатор области определяет область OSPF, которой принадлежит сеть. Даже если никакие области не указаны, должна присутствовать какая-либо область 0. В окружении OSPF с одной областью область всегда имеет идентификатор 0. По завершении настройки необходимо сравнить рабочую конфигурацию с точной схемой топологии для сверки номеров сетей и IP-адресов интерфейсов для обнаружения возможных механических ошибок, допущенных при вводе IP-адресов.

Проверить функционирование протокола OSPF в сети можно несколькими способами.

Если конфигурация верна, то для проверки работоспособности маршрутизации можно отправить эхо-запросы командой `ping` на устройства в удаленных сетях. Успешное выполнение команды `ping` будет свидетельством работоспособности маршрутизации.

Выполните команды для проверки IP-маршрутизации `show ip protocols` и `show ip route` в приглашении командной строки.

Команда `show ip protocols` позволяет убедиться в верности настройки маршрутизации OSPF, использовании соответствующих интерфейсов для отправки и приема обновлений OSPF, а также правильном составе сетей в оповещениях.

Команда `show ip route` выводит таблицу маршрутизации, по которой можно проверить присутствие маршрутов, полученных соседними маршрутизаторами.

6.3 Контрольные вопросы

1. Дайте понятие протокола маршрутизации OSPF.
2. Назовите основные преимущества протокола OSPF.
3. О каких изменениях в состоянии каналов маршрутизаторы обмениваются извещениями ?
4. Дайте понятие выделенного (designated) маршрутизатора.
5. Дайте понятие распределения нагрузки между параллельными каналами.
6. В каких информационных системах целесообразно использование процедуры установления подлинности ?
7. Перечислите способы организации обмена информацией о маршрутах.
8. Какие параметры учитывает метрика маршрута в протоколе OSPF ?
9. Дайте понятие автономной системы (Autonomous System).
10. Какие маршрутизаторы называются соседними ?
11. Какие маршрутизаторы называются смежными ?
12. Дайте понятие объявления о состоянии канала (Link State Advertisement).
13. Как называется процесс распространения LSA в пределах автономной системы ?
14. Дайте понятие выделенного маршрутизатора (DR) и запасного выделенного маршрутизатора (BDR).
15. С какой целью в сетях со множественным доступом выбираются выделенный маршрутизатор (DR) и запасной выделенный маршрутизатор (BDR) ?
16. Назовите и опишите типы маршрутизаторов OSPF ?
17. Какие типы LSA используются для формирования базы данных ?
18. Какие преимущества дает разделение автономной системы на зоны ?
19. Какие типов зон существуют в автономных системах ?
20. Какие причины вызывают сообщения об изменениях маршрутов ?
21. Какие данные содержит в себе маршрутная таблица OSPF ?
22. Перечислите преимущества и недостатки протокола OSPF.

7 Лабораторная работа №7. Протокол BGP

Цель работы. Научиться настраивать динамическую маршрутизацию на основе протокола BGP. Выполнить задание в соответствии с вариантом.

7.1 Основные теоретические положения

Протокол маршрутизации BGP (Border Gateway Protocol) является динамическим, междоменным, распределенным, одноуровневым, многопутевым и управляется маршрутизатором [1]. Он разработан с целью устранить недостатки протокола EGP (Exterior Gateway Protocol), считается его приемником и уже скоро полностью вытеснит его с просторов Интернета.

Изначально маршрутизаторы, использующие протокол BGP, обмениваются полными таблицами маршрутизации. Далее, по мере их изменения, рассылаются обновления — последовательные и отражающие только изменения. В таблицах протокола BGP возможно несколько маршрутов к одному месту назначения, но другим маршрутизаторам сообщаются только оптимальные. Естественно, для выбора таких маршрутов необходима какая-то метрика. В BGP она предусмотрена и представляет собой просто число, которое назначено администратором сети. При этом администратор должен сам учитывать такие факторы, как число переходов, скорость канала и его стабильность.

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 [2].

Обновления таблиц BGP рассылаются при помощи протокола TCP. Они содержат информацию о том, какие домены достижимы с конкретного узла. Существует способ выявить сбои в работе узлов и маршрутизаторов посредством

сообщений “еще жив” (keep-alive), которые генерируются примерно каждые 30 секунд. Также BGP называют протоколом, поддерживающим бесклассовую междоменную маршрутизацию (Classless Interdomain Routing, CIDR). Это означает, что в таблицах маршрутизации используются 32-разрядные IP-адреса и маски подсетей, значения которых при выборе маршрутов трактуются как “сплошные”.

Протокол BGP использует суммирование маршрутов для уменьшения таблиц маршрутизации.

Сейчас используется новая версия протокола BGP — BGP-4. Помимо других возможностей, в ней можно применять маски подсетей произвольной длины.

Протокол BGP используется для передачи информации о внутренних маршрутах между автономными системами. Протокол BGP может быть использован для определения различных типов маршрутов [1]:

- Inter-autonomous system routing маршруты которые соединяют данную автономную систему с одной или несколькими другими автономными системами;
- Intra-autonomous system routing - протокол может быть использован для определения маршрута внутри автономной системы, в том случае, когда несколько маршрутизаторов участвуют в процессе определения маршрута BGP;
- Pass-through autonomous system - протокол может быть использован для определения маршрутов, которые проходят через автономную систему, которая не участвует в процессе BGP.

Пара BGP-соседей устанавливает между собой соединение по протоколу TCP, порт 179. Соседи, принадлежащие разным АС, должны быть доступны друг другу непосредственно; для соседей из одной АС такого ограничения нет, поскольку протокол внутренней маршрутизации обеспечит наличие всех необходимых маршрутов между узлами одной автономной системы.

Поток информации, которым обмениваются BGP-соседи по протоколу TCP, состоит из последовательности BGP-сообщений. Максимальная длина сообщения 4096 октетов, минимальная – 19. Имеется 4 типа сообщений [10].

1. OPEN – посылается после установления TCP-соединения. Ответом на OPEN является сообщение KEEPALIVE, если вторая сторона согласна стать BGP-соседом;

иначе посылается сообщение NOTIFICATION с кодом, поясняющим причину отказа, и соединение разрывается.

2. KEEPALIVE – сообщение предназначено для подтверждения согласия установить соседские отношения, а также для мониторинга активности открытого соединения: для этого BGP-соседи обмениваются KEEPALIVE-сообщениями через определенные интервалы времени.

3. UPDATE – сообщение предназначено для анонсирования и отзыва маршрутов. После установления соединения с помощью сообщений UPDATE пересылаются все маршруты, которые маршрутизатор хочет объявить соседу (full update), после чего пересылаются только данные о добавленных или удаленных маршрутах по мере их появления (partial update).

4. NOTIFICATION – сообщение этого типа используется для информирования соседа о причине закрытия соединения. После отправления этого сообщения BGP-соединение закрывается.

Вся маршрутная информация хранится в специальной базе данных RIB (routing information base). Маршрутная база данных BGP состоит из трех частей.

1. ADJ-RIBS-IN: Запоминает маршрутную информацию, которая получена из update-сообщений. Это список маршрутов, из которого можно выбирать. (policy information base - PIB).

2. LOC-RIB: Содержит локальную маршрутную информацию, которую BGP-маршрутизатор отобрал, руководствуясь маршрутной политикой, из ADJ-RIBS-IN.

3. ADJ-RIBS-OUT: Содержит информацию, которую локальный BGP-маршрутизатор отобрал для рассылки соседям с помощью UPDATE-сообщений.

Так как разные BGP-партнеры могут иметь разную политику маршрутизации, возможны колебания маршрутов. Для исключения этого необходимо выполнять следующее правило: если используемый маршрут объявлен не рабочим (в процессе корректировки получено сообщение с соответствующим атрибутом), до переключения на новый маршрут необходимо ретранслировать сообщение о недоступности старого всем соседним узлам.

Протокол BGP позволяет реализовать маршрутную политику, определяемую администратором AS. Политика отражается в конфигурационных файлах BGP. Маршрутная политика это не часть протокола, она определяет решения, когда место назначения достижимо несколькими путями, политика отражает соображения безопасности, экономические интересы и пр. Количество сетей в пределах одной AS не лимитировано. Один маршрутизатор на много сетей позволяет минимизировать таблицу маршрутов [2].

BGP использует три таймера:

- connectretry (сбрасывается при инициализации и коррекции; 120 сек);
- holdtime (запускается при получении команд Update или Keepalive; 90сек);
- keepalive (запускается при посылке сообщения Keepalive; 30сек).

BGP отличается от RIP и OSPF тем, что использует TCP в качестве транспортного протокола. Две системы, использующие BGP, связываются друг с другом и пересылают посредством TCP полные таблицы маршрутизации. В дальнейшем обмен идет только в случае каких-то изменений. ЭВМ, использующая BGP, не обязательно является маршрутизатором. Сообщения обрабатываются только после того, как они полностью получены.

В BGP в качестве метрики используется число шагов до цели, и время распространения маршрутной информации велико, у разных маршрутизаторов может быть прописана разная маршрутная политика. Допустим, какой-то маршрутизатор на основании анализа ситуации принял решение об изменении маршрута с варианта 1 на вариант 2 и сразу реализовал это решение. Эти данные дойдут до соседей спустя несколько минут. Они на основе новых данных могут также принять определенные решения, уведомив об этом своих соседей. Может так получиться, что, после того как наш маршрутизатор получит данные от своих соседей, метрика для варианта маршрута 1 окажется меньше метрики маршрута 2 и придется вернуться к пути, от которого он только что отказался. Чтобы такого не происходило, нужно сначала уведомлять соседние маршрутизаторы о принятом решении, но на новый маршрут не переключаться, пока от соседей не придут данные об их намерениях. (Для этого нужно задать соответствующие таймерные

переменные). Может так случиться, что переключение на новый маршрут придется отменить, так как это ведет к осцилляции маршрута. Кто-то может сказать, что ему все равно, по какому маршруту доставляется пакет (по пути 1 или 2), и пусть себе маршруты осциллируют. Эта точка зрения ошибочна, так как при осцилляции маршрутов их установление происходит в маршрутизаторах не одновременно и заметное число пакетов не будет доставлено адресату вообще.

Важным свойством протокола является возможность декларации резервного (backup) маршрута. Так, если основной маршрут автономной системы стал недоступен, маршрутизатор переключит поток на этот резервный канал. При этом пользователи сети не должны ожидать момента, когда администратор сети вернется из отпуска, проснется или вернется из кафетерия и сам внесет необходимые коррективы [2].

7.2 Рабочее задание

Необходимо настроить динамическую маршрутизацию на основе протокола BGP в соответствии с вариантом указанным в таблице 3.1 лабораторной работы №3. При правильной настройке маршрутизации все компьютеры должны иметь возможность успешно отправлять icmp запросы друг другу.

Перед настройкой протокола BGP на маршрутизаторах необходимо присвоить IP-адреса и активировать все физические интерфейсы, которые будут участвовать в маршрутизации. На последовательных каналах необходимо установить тактовую частоту главного маршрутизатора. Эти действия были сделаны в рамках третьей лабораторной работы.

Когда Интернет-провайдер размещает граничный маршрутизатор на объекте клиента, в качестве маршрута по умолчанию обычно настраивается статический маршрут к Интернет-провайдеру. Однако иногда Интернет-провайдеру требуется включить маршрутизатор в свою автономную систему и сделать его участником BGP. В этих случаях необходимо настроить маршрутизатор в помещении клиента, введя необходимые команды для активации BGP.

Первый шаг в активации BGP на маршрутизаторе состоит в настройке номера автономной системы. Это делается с помощью следующей команды:

```
router bgp [номер AS].
```

Следующий шаг – идентификация маршрутизатора провайдера, который будет выступать соседним узлом BGP для обмена информацией с маршрутизатором в помещении клиента (CPE). Соседний маршрутизатор идентифицируется следующей командой:

```
neighbor [IP-адрес] remote-as [номер AS].
```

Клиентам Интернет-провайдера, имеющим собственные зарегистрированные блоки IP-адресов, может быть необходима возможность объявления маршрутов к своим внутренним сетям в Интернете. Объявление внутренних маршрутов посредством BGP осуществляется по команде "network". Формат команды "network":

```
network [адрес сети]
```

После установки оборудования в помещениях клиента и настройки протоколов маршрутизации клиент получает работающую локальную сеть и подключение к Интернету. Клиент становится полноправным участником других сервисов, предлагаемых провайдером.

Для BGP обычно используются зарегистрированные IP-адреса, которые могут использоваться в маршрутизации и однозначно идентифицируют организацию. В очень крупных организациях для процессов BGP могут применяться частные адреса, как показано на рисунке. В Интернете запрещается применять BGP для объявления адресов частных сетей.

7.3 Контрольные вопросы

1. Дайте понятие протокола маршрутизации BGP.
2. Назовите основные особенности протокола BGP.
3. Для определения каких типов маршрутов может быть использован протокол BGP ?

4. Какие типы сообщений содержит поток информации, которым обмениваются BGP-соседи по протоколу TCP ?
5. Какие таймеры использует BGP ?
6. В чем заключается отличие BGP от RIP и OSPF ?
7. Опишите важное свойство протокола BGP - возможность декларации резервного (backup) маршрута.

Список использованных источников

- 1 Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы / В. Г. Олифер, Н. А. Олифер. - СПб.: Питер, 2002. - 643 с.
- 2 Локальные вычислительные сети: справочник / Под ред. С. В. Назарова. - М.: Финансы и статистика, 1994. - 430 с.
- 3 Заргер, К. Компьютерные сети. Модернизация поиск неисправностей / К. Заргер. - Л., 2001. - 218 с.
- 4 Блэк, Ю. Сети ЭВМ: протоколы, стандарты, интерфейсы / Ю. Блэк. - М., 1990. - 206 с.
- 5 Кулаков, Ю. А. Компьютерные сети. Выбор, установка, использование, администрирование / Ю. А. Кулаков. - М., 1999. - 194 с.
- 6 Нанс, Б. Компьютерные сети / Б. Нанс. – М.: БИНОМ, 1996. - 262 с.
- 7 Таненбаум, Э. Компьютерные сети / Э. Таненбаум. - СПб.: BHV-СПб, 1998. – 345 с.
8. Электронный ресурс: <http://book.itep.ru/4/44/bgp44114.htm>
9. Электронный ресурс: <http://maximano.h1.ru/net.htm>
10. Электронный ресурс: http://abc.vvsu.ru/Books/ebooks_iskt/bgp.html