

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
**«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ НАЦИОНАЛЬНЫЙ
ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ»**
(Н И У « Б е л Г У »)

ИНСТИТУТ ИНЖЕНЕРНЫХ ТЕХНОЛОГИЙ И ЕСТЕСТВЕННЫХ НАУК

Кафедра информационно-телекоммуникационных систем и технологий

**ИССЛЕДОВАНИЕ ПРОИЗВОДИТЕЛЬНОСТИ ПРОТОКОЛОВ
МАРШРУТИЗАЦИИ В IP СЕТЯХ ДЛЯ ТРАФИКА РЕАЛЬНОГО ВРЕМЕНИ**

**Магистерская диссертация
Укот Исраэл Акпаника**

**очного отделения
направления подготовки 11.04.02 Инфокоммуникационные технологии и
системы связи
2 года обучения группы 07001432**

Научный руководитель
канд. техн. наук, старший преподаватель кафедры
Информационно-телекоммуникационных
систем и технологий НИУ «БелГУ»
Ушаков Д.И.

Рецензент
канд. техн. наук, старший преподаватель кафедры
Информационных систем НИУ «БелГУ»
Жихарев А. Г.

БЕЛГОРОД 2016

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	3
1 ОСНОВНЫЕ ПРИНЦИПЫ МАРШРУТИЗАЦИИ В СЕТЯХ.....	5
1.1 Компьютерная сеть	5
1.2 Маршрутизация	18
2 ОБЗОР ПРОТОКОЛОВ МАРШРУТИЗАЦИИ	35
2.1 Протокол маршрутизации на базе вектора расстояний	35
2.2 Протокол маршрутизации на основе состояния канала.....	39
2.3 Усовершенствованный протокол маршрутизации на базе вектора расстояний.....	44
2.4 Сравнительная характеристика внутренних протоколов маршрутизации	48
3 МОДЕЛИРОВАНИЕ В СРЕДЕ RIVERBED MODELER	51
3.1 Технология Riverbed Modeler.....	51
3.2 Топология сети	53
3.3 Результаты исследований и анализ симуляции.....	59
ЗАКЛЮЧЕНИЕ.....	67
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ	68

ВВЕДЕНИЕ

На сегодняшний день количество телекоммуникационных сетей с коммутацией пакетов непрерывно растет. Современные информационные системы все в большей степени ориентируются на предоставлении телематических и медийных услуг в виде передачи потокового видео и голоса абонентам с высоким качеством, что накладывает свои особенности при управлении и функционирования сетей такого класса. Вместе с тем большое количество узлов и промежуточных элементов вызывает необходимость в маршрутизации передаваемого в сети трафика, т.е. в выборе оптимального маршрута следования пакетов с точки зрения времени доставки пакета или надежности передачи. Как правило проблему выбора оптимального по заданному критерию пути следования пакетов в сети, решают алгоритмы маршрутизации [1].

Современные сетевые технологии передачи и коммутации пакетов в IP сетях в значительной мере определяются стэком протоколов маршрутизации, которые в основном классифицируются на внешние (BGP, IDRP, IS-IS level 3) и внутренние (RIP, OSPF, IGRP, EIGRP) протоколы [2]. Однако от работы данных протоколов зависит производительность сети под которой понимается совокупность таких параметров как время конвергенции, потери пакетов, задержка голосового/видео трафика, задержка в очереди, использование канала связи и время отклика страницы HTTP.

Таким образом, работа в которой проводится оценка производительности внутренних протоколов маршрутизации по определенным критериям с помощью средств имитационного моделирования представляется актуальной.

Целью данной работы является оценка производительности внутренних протоколов маршрутизации при использовании сетевого симулятора Riverbed Modeler.

Поставленная цель достигается решением следующих задач:

1. Выбор среды моделирования сетей связи при различных параметрах;
2. Анализ внутренних протоколов маршрутизации;
3. Моделирование сети при использовании сетевого симулятора Riverbed Modeler.

Магистерская диссертация состоит из введения, трех глав, заключения, списка использованных источников. Текст магистерской диссертации изложен на 74 листах машинописного текста, включающий 21 рисунок и списка литературы из 60 названий.

1 ОСНОВНЫЕ ПРИНЦИПЫ МАРШРУТИЗАЦИИ В СЕТЯХ

1.1 Компьютерная сеть

Компьютерная сеть – совокупность оборудования (компьютеры, серверы, средств коммутации и др.), соединенная каналами или линиями связи, представляющая единую систему для обмена информацией.

Сеть можно представить в виде графа, в котором узлы играют роль сетевого оборудования, а ребра которые соединяют узлы – каналы связи. Узлы могут быть конечными, промежуточными или смежными. Оборудование может быть соединено друг с другом различными способами [2].

Топологией является соединение всех компонентов сети. Существует множество способов соединения оборудования. Наиболее распространенных топологий включается :

Шина. Все устройства соединяются с помощью общего (одного) кабеля, на концах находятся терминаторы, которые предотвращают отражение сигнала (рисунок 1.1). Сообщение, отосланное с одной машины, пересылается всем, и только та, которой оно адресовано, будет его обрабатывать. Такое построение сети отличается дешевизной и простой настройкой. Минус в том, что при выходе из строя общего кабеля или терминатора система откажет в работе. Так же тяжело найти неисправность на сети;

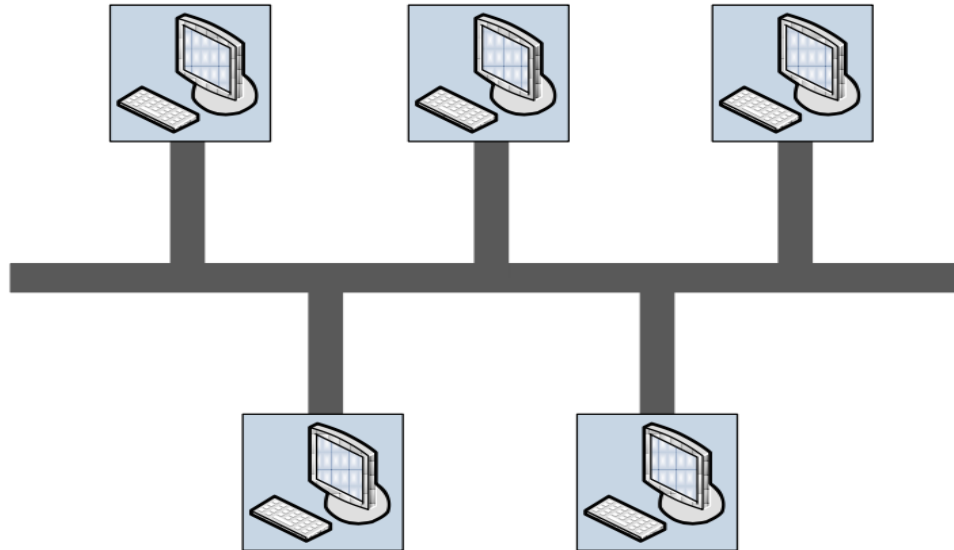


Рисунок. 1.1 – Топология типа «Шина»

Кольцо. Оборудование подключается только к двум своим соседям. Данные передаются от устройства к устройству в одном направлении, вследствие чего не возникает коллизий пакетов данных (рисунок 1.2). Каждое устройство ждет своей очереди для передачи данных. При отказе любого оборудования вся система выходит из строя, и найти неисправность сложно;

Звезда. К центральному узлу подключаются все рабочие станции, при их отказе система не выйдет из строя. Но в случае отказа центрального узла вся сеть становится не работоспособной (рисунок 1.3). Тем не менее, этот вид топологии отличается высокой производительностью, при правильном проектировании сети, и легкостью поиска неисправностей;

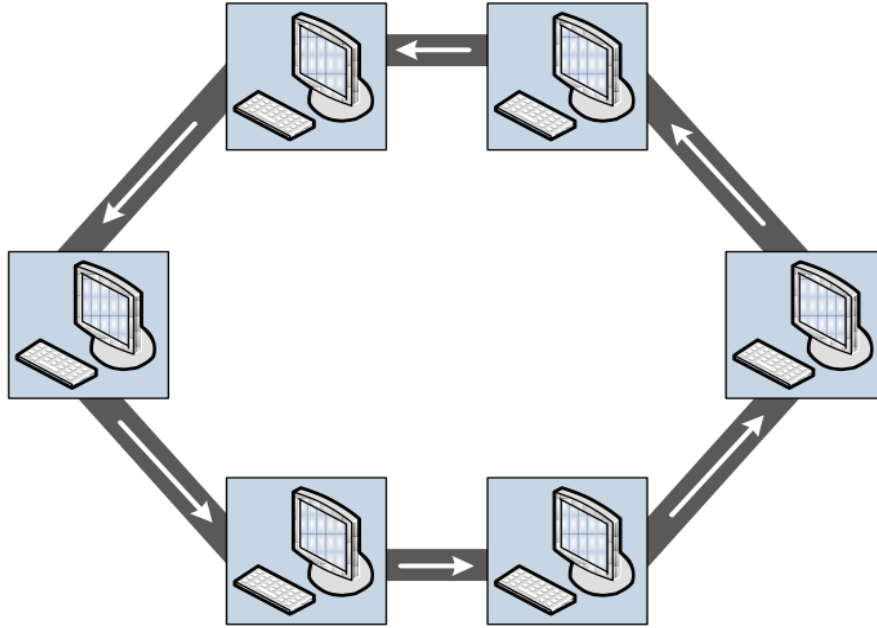


Рисунок 1.2 – Топология типа «Кольцо»

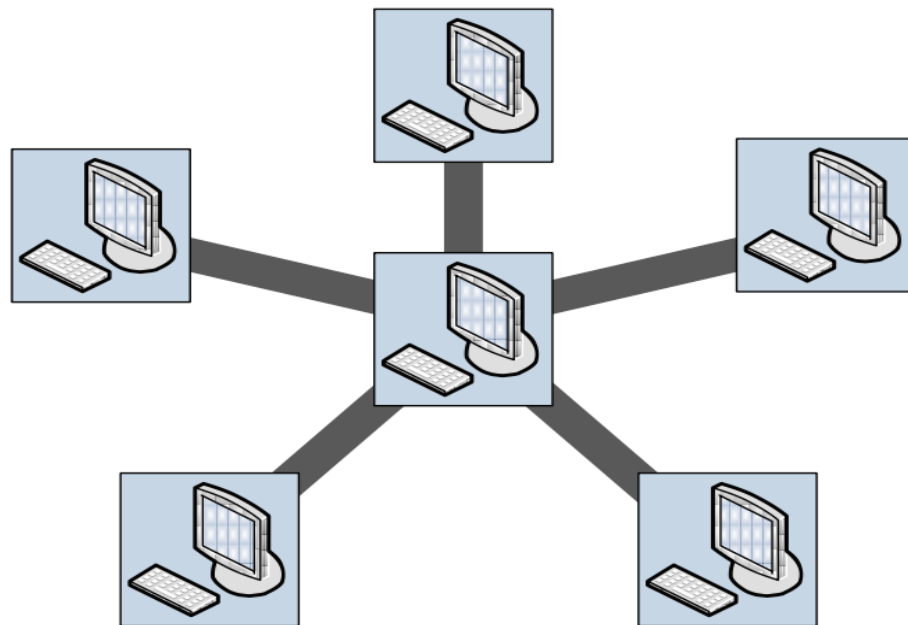


Рисунок 1.3 – Топология типа «Звезда»

Двойное кольцо. при этом , кольцевой топологии создается второе кольцо для передачи данных в обоих направлениях. Система становится более отказоустойчивой (рисунок 1.4).

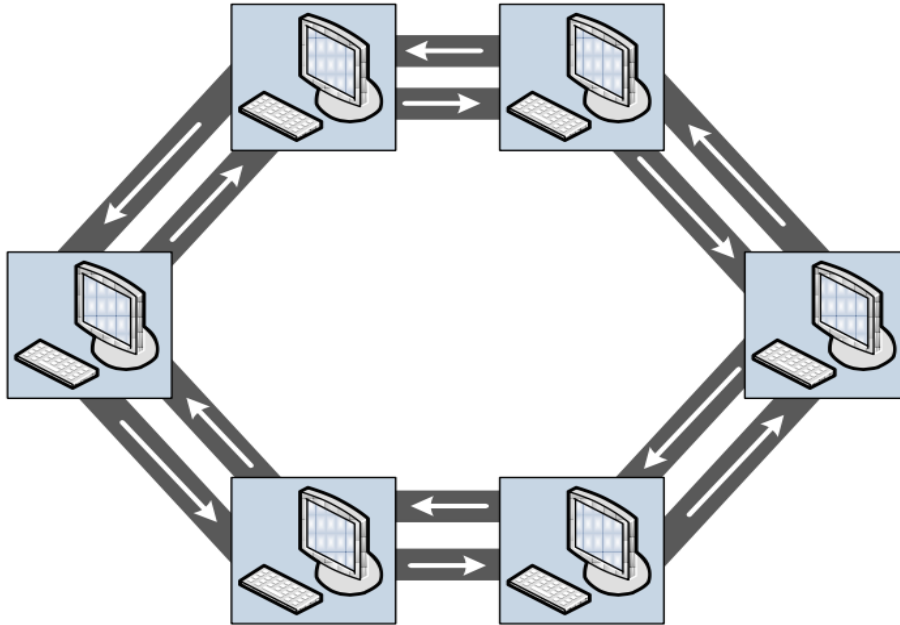


Рисунок 1.4 – Топология типа «Двойное кольцо»

Древовидная топология. Разновидность топологии звезда. Отличия только в том, что схема более сложная и соблюдается иерархичность сетевых узлов (рисунок 1.5).

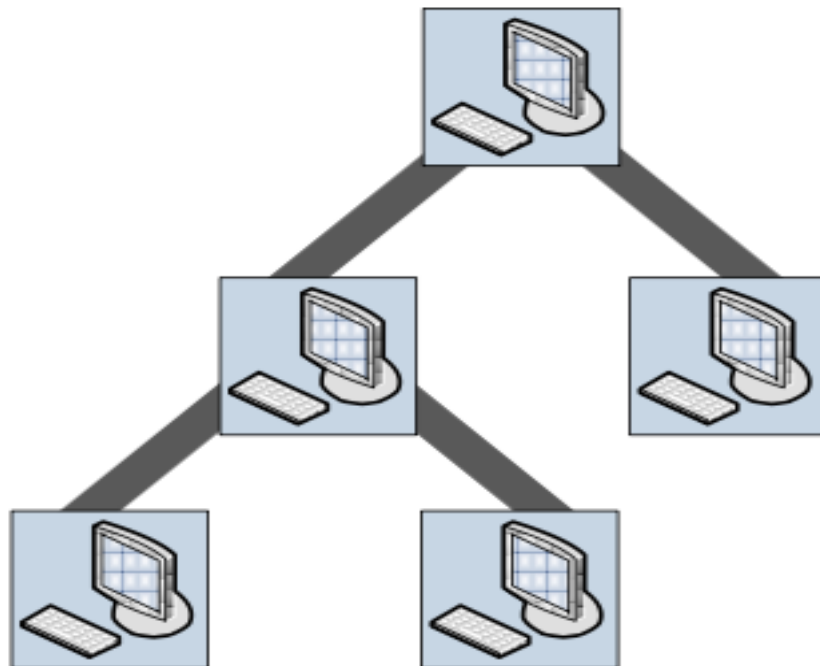


Рисунок 1.5 – Топология типа «Дерево»

Полносвязная. Все узлы при этом соединяются друг с другом, поэтому система отказоустойчивая (рисунок 1.6). Однако такая топология очень дорогая и сложная, поэтому лучше создавать частично связанную топологию [1-2].

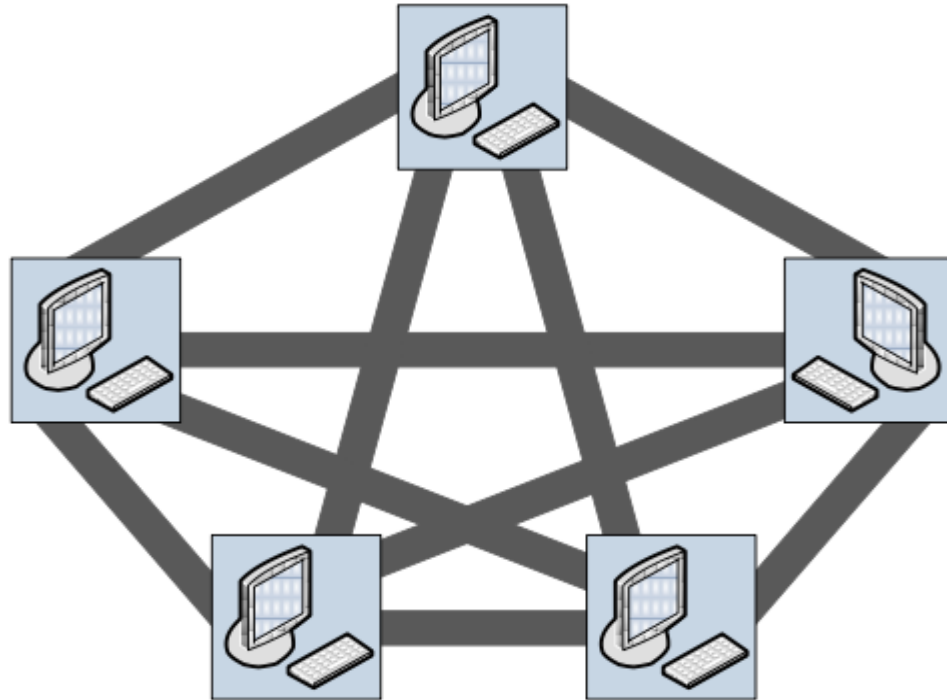


Рисунок 1.6 – Топология типа «Полносвязная»

Для организации обмена или передачи данных между узлами используют специализированные наборы правил взаимодействия аппаратуры, называемые протоколами.

Международная организация по стандартам ISO разработала модель OSI (включающая в себя семь уровней), которая определяет функции уровней взаимодействующих систем. В сети Интернет используется стек протоколов TCP/IP включающий в себя четыре уровня [2]. На рисунке 1.7 представлены иерархии уровней модели OSI и стека TCP/IP



Рисунок 1.7 – Модель OSI/ISO и стек протоколов TCP/IP

Прикладной уровень – уровень доступа приложений к сети который отвечает за обмен данных между приложениями на устройстве пользователя и сетью. (например: HTTP, SMTP, SNMP, Telnet, POP3, FTP).

Представительный уровень – отвечает за то, что данные, передаваемые на прикладном уровне, будут прочитаны и защищены.

Сеансовый уровень - управление сеансами связи, т.е. непрерывного обмена информацией в виде нескольких передач назад и вперед между двумя узлами. Основной элемент передачи – Protocol Data Unit (PDU)

Транспортный уровень – надежная передача сегментов данных между точками в сети, в том числе сегментации, подтверждение и мультиплексирования. Основным элементом передачи является Сегмент. (Примеры протоколов: TCP, UDP).

Сетевой уровень – подключение и выбор пути между двумя точками для передачи данных. Основной элемент передачи – Пакет. (Пример протокола: IP)

Канальный уровень - надежная передача кадров данных между двумя узлами, соединенными физического уровня.

Физический уровень - отвечает за физическое соединение между оборудованием. При передаче данных информация «упаковывается» в пакет, начиная с прикладного уровня до физического уровня, этот процесс называется Инкапсуляция. После этого пакет отправляется в сеть. При получении пакета происходит «распаковывание» от нижнего уровня (физический) к верхнему (прикладной), и этот процесс называется Деинкапсуляция [1-2].

Для связи между сетевым оборудованием в локальных и глобальных сетях обычно используется протокол сетевого уровня – IP (Internet Protocol). В настоящее время существует две версии этого протокола IPv4 и IPv6. Рассмотрим их подробнее:

IPv4 - это четвертая версия протокола IP (Internet Protocol), которая на сегодняшний день является основной и обслуживает большую часть сети Интернет. Протокол IPv4 устанавливает правила для функционирования компьютерных сетей на основе обмена пакетами. Это низкоуровневый протокол, который отвечает за установление соединения между узлами сети на основе IP-адреса. Адреса узлов в сети, согласно протоколу IPv4 имеют длину 32 бит (4 байта – 4 октета), что дает в совокупности $2^{32} = 4\ 294\ 967\ 296$ возможных адресов. Но не все адреса используются для глобального пространства (Интернет), часть адресов выделяется для специальных целей, например, для организации локальных сетей, виртуальных сетевых интерфейсов, используются для целей тестирования, являются специальными адресами и так далее. IPv4 адреса как правило записываются в виде четырех десятичных чисел от 0 до 255 разделенных символом "." (точка), например, минимальный возможный адрес - 0.0.0.0, максимальный - 255.255.255.255. Число от 0 до 255, как правило, в компьютерных системах требует для хранения

1 байт или 8 бит информации, таким образом $8 * 4 = 32$ бита или 4 байта, что соответствует заявленной длине адреса.

Бесклассовая адресация (CIDR)

Изначально адресация в IP-сетях была проведена по классовому принципу (существовали классы, которые делили адресное пространство на большие блоки). Тем не менее данная схема оказалась непрактичной и сегодня в Интернет используется бесклассовая адресация, которая известно как Classless Inter-Domain Routing, или сокращенно CIDR.

В целом, CIDR позволяет описывать блоки IP-адресов для Интернет-подсетей. Так, стандартной считается запись CIDR в виде IP-адреса, следующего за ним символа "/" и число, обозначающее битовую маску подсети, например, 15.16.17.0/24.

Число 24 в данном случае означает количество старших битов в маске подсети. Так как IP-адрес состоит из 32 бит, но маской являются старшие 24, это значит, что для всех возможных адресов в сети остается $32 - 24 = 8$ бит. То есть $2^8 = 256$ возможных. Или, если наша маска была бы 23 бита а не 24, то для адресов осталось бы 9 бит $= 2^9 = 512$ возможных, и напротив, если маска будет 25 бит, то для адресов останется $2^{32-25} = 2^7 = 128$ возможных. Таким образом, мы можем описывать сети, состоящие из различного количества доступных адресов. Кроме того, одна большая сеть может быть внутри опять раздроблена на несколько более мелких подсетей, те в свою очередь могут быть также разбиты на подсети и т.д.

Следует отметить, что количество возможных узлов (хостов) в подсети всегда минимум на 2 меньше количества всех возможных адресов. Это связано с тем, что первый адрес резервируется, как идентификатор сети, а последний является широковещательным.

Специальные IPv4 адреса

В соответствии с требованиями, определенных разных стандартах, относящимися к протоколу IPv4, существуют такие специальные адреса:

Таблица 1 – описание специальных адресов протокола IPv4

Сеть (адрес)	Описание	Стандарт
0.0.0.0/8	Источник адресов текущей сети	RFC 5735
10.0.0.0/8	Для организации частных сетей	RFC 1918
100.64.0.0/10	Для использования в сети провайдера	RFC 6598
127.0.0.0/8	Интерфейс коммутации внутри хоста	RFC 5735
169.254.0.0/16	Для автоматического конфигурирования (например, при отсутствии DHCP)	RFC 3927
172.16.0.0/12	Для организации частных сетей	RFC 1918
192.0.0.0/24	Для специального назначения (зарезервировано IETF)	RFC 5735
192.0.2.0/24	Тестовая сеть 1, для использования в качестве примеров в документации	RFC 5735
192.88.99.0/24	Для трансляций из IPv6 в IPv4	RFC 3068
192.168.0.0/16	Для организации частных сетей	RFC 1918
198.18.0.0/15	Для тестирования производительности	RFC 2544
198.51.100.0/24	Тестовая сеть 2, для использования в качестве примеров в документации	RFC 5737
203.0.113.0/24	Тестовая сеть 3, для использования в качестве примеров в документации	RFC 5737
224.0.0.0/4	Для многоадресной рассылки	RFC 5771
240.0.0.0/4	Зарезервировано для возможных потребностей в будущем	RFC 1700
255.255.255.255	Широковещательный адрес	RFC 919

Формат IP-адреса (протокол IPv4) представляет собой 32-х битное двоичное число, для простоты это число разбивают на октеты по 8 бит каждый и разделяют точкой. Двоичные числа в каждом октете преобразуют в десятичные от 0 до 255.

13 15 49 96
00001101.00001111.00110001.01100000

В локальных сетях используются частные адреса (протокол IPv4), эти адреса являются особыми IP адреса, которые не используются в глобальной сети:

- 10.0.0.0 - 10.255.255.255;
- 172.16.0.0 - 172.31.255.255;
- 192.168.0.0 - 192.168.255.255.

Необходимость в таких адресах возникла из-за того, что не ожидала такого большого роста в использовании сети. Сейчас проблему увеличения количества IP-адресов Конечно решает протокол IPv6, но на данный момент этот протокол еще широко не используется.

IPv6 - новая (шестая) версия протокола IP (Internet Protocol), которая пришла на смену четвертой версии IPv4. На данный момент IPv6 постепенно внедряется в работу. Многие устройства и узлы в Интернет уже поддерживают адресацию по протоколу IPv6. IPv6 адреса имеют длину 128 бит, что дает в общей сложности $2^{128} \approx 3.4 \times 10^{38}$ возможных адресов в адресном пространстве. Это в ≈ 79 септиллионов раз больше, чем все адресное пространство, определенное протоколом IPv4. Если сравнить это число с количеством видимых звезд в нашей Вселенной (которое оценивается примерно в 10^{24} звезд), то на каждую звезду можно выделить примерно чуть более 340 триллионов

адресов. Это настолько большое число, что можно говорить о том, что IPv6 раз и навсегда решает проблему нехватки Интернет-адресов. Можно Другими словами сказать что адресное пространство IPv6 теоретически способно удовлетворить потребности в IP-адресах для всей нашей Вселенной.

В действительности же при распределении IPv6 адресов, принято решение выдавать конечному пользователю вместо одного адреса целые подсети с длиной префикса 64 бит. Что это на практике означает, то что каждому из жителей Земли будет выдаваться огромное количество адресов, что позволит подключать несметное количество различных устройств, каждое из которых будет "выходить" в Интернет со своим "белым" и честным IP-адресом, и, естественно, при этом, может быть адресовано в сети напрямую! Это все позволит в теории значительно упростить маршрутизацию и инфраструктуру сети.

Представление адресов в IPv6

IPv6 адреса в стандартном виде решено записывать в виде восьми блоков шестнадцатеричных чисел от 0x0000 до 0xFFFF, разделенных двоеточием. Например:

```
2001:0db8:0000:0000:0000:0000:0000:1
```

Лидирующие нули в группах могут быть опущены:

```
2001:db8:0:0:0:0:0:1
```

При этом если блоки содержат нули, они могут быть упрощены и заменены двойным двоеточием, при этом сделано это может быть лишь в одном месте (чтобы не возникало неоднозначностей). Например, приведенный выше адрес может быть сокращен до вида:

2001:db8::1

Если есть две группы нулей, например:

2001:0:0:aa:0:0:0:1

То сокращают наиболее длинную группу:

2001:0:0:aa::1

Если же группы равны:

2001:db8:0:0:aa:0:0:1

То сокращают ту, которая находится левее:

2001:db8::aa:0:0:1

Например, адрес локального хоста 0000:0000:0000:0000:0000:0000:0000:0001 в IPv6 представлении можно записать как ::1, а адрес текущей сети (известный как unspecified address) 0000:0000:0000:0000:0000:0000:0000:0000, может быть сокращен до :: соответственно.

Также при записи IPv6 адресов отдают предпочтение прописным буквам шестнадцатеричных чисел перед заглавными. То есть предпочтительнее записать:

2001:db8:dead::beef

Чем: 2001:DB8:DEAD::BEEF

Таблица 1.2 – Специальные IPv6 адреса

Сеть (адрес)	Описание	Зарезервировано протоколом
::/128	Источник адресов текущей сети	да
::1/128	Интерфейс коммутации внутри хоста	да
64:ff9b::/96	Трансляция IPv4-IPv6	нет
::ffff:0:0/96	Адрес IPv4 отображенный на IPv6	да
100::/64	Блок адресов отказа	нет
2001::/23	Зарезервировано IETF для нужд протокола	нет
2001::/32	TEREDO - псевдо-интерфейс туннелей	нет
2001:2::/48	Для тестирования производительности	нет
2001:db8::/32	Для использования в примерах документации	нет
2001:10::/28	ORCHID - Слой маршрутизируемых криптографических хэш-идентификаторов	нет
2002::/16	6to4 - для трансляции IPv6 поверх IPv4	нет
fc00::/7	Unique-Local	нет
fe80::/10	Linked-Scoped Unicast	да

Главные изменения по сравнению с IPv4

- Существенно увеличенное адресное пространство;
- Упрощена работа маршрутизации (нет разбивки пакета на части, нет контрольной суммы в структуре пакета);
 - Не смотря то, что длина адреса выросла в 4 раза (с 32 до 128 бит), общее удлинение заголовка пакета выросло всего в 2 раза с 20 до 40 байт;

- В сверхскоростных сетях появилась поддержка огромных пакетов - джамбограм, длиной до 4 гигабайт;
- Появились метки потоков и классы трафика, что дает возможность эффективно контролировать приоритеты передачи данных;
- Появилось многоадресное вещание, что, в теории, должно дать возможность упростить, например, эфирное вещание (ТВ, радио) по IP-сетям [2,3,8].

1.2 Маршрутизация

Маршрутизация является процессом выбора лучшего пути в сети. Протоколы и таблицы маршрутизации используются для маршрутизации, эти протоколы реализуют алгоритмы маршрутизации, чтобы определить лучшего и наиболее приемлемый путь для пересылки пакета данных.

Устройство, определяющее наиболее рациональный путь для передачи данных из одной сети в другую, называется маршрутизатор. Таблица маршрутизации, представляет собой таблицу данных, хранящихся в маршрутизаторе или сетевом компьютере, который перечисляет маршруты к определенным сетевым направлениям, а в некоторых случаях, метрики (расстояния), связанные с этим маршрутам. В таблице маршрутизации содержит информацию о топологии сети вокруг него. Таблица может хранить следующие виды записей (одна запись для каждой сети):

Статические – информация о маршруте заполняется вручную, но этот способ приводит к проблемам в случае изменения топологии сети или отказа на каком-либо участке;

Динамические – заполнение происходит благодаря обмену данных маршрутизации между устройствами, полученных по протоколу

маршрутизации, то есть маршрутизаторы обмениваются информацией друг с другом путем передачи сообщений об обновлении. В зависимости от протокола обновления могут поступать периодически или же только при изменении топологии.

При возникновении ситуации когда есть несколько путей передачи информации от источника до места назначения, применяется административное расстояние.

Административное расстояние является функцией, которая используется маршрутизаторами для того, чтобы выбрать наилучший путь, когда есть два или более различных маршрутов к одному месту назначения. Административное расстояние определяет надежность протокола маршрутизации. Каждый протокол маршрутизации использует свои метрики для определения наилучшего пути. Если используются различные протоколы, то приемлемый путь выбирается на основе административного расстояния – это число от 0 до 255 (Таблица 1.3.) [4-7].

Таблица 1.3 – Значения административного расстояния

Источник маршрутов	Расстояние по умолчанию
Подключенная сеть	0
Статический маршрут	1
EIGRP	90
IGRP	100
OSPF	110
RIP	120
Не известный	255(не будет использоваться для передачи трафика)

Чем ниже значение, тем более предпочтительным источником маршрута. Административное расстояние от 0 является наиболее предпочтительным. Только непосредственно подключенной сети имеет административное расстояние, равное 0, который не может быть изменен.

Протокол с наименьшим значением выбирается как более надежный.

Как уже известно, маршрутизаторы узнают о соседних сетях, которые подключены непосредственно и об удаленных сетях путем использования статических маршрутов и протоколов динамической маршрутизации.

На самом деле, маршрутизатор может узнать о пути к той же сети из более чем одного источника. Например, статический маршрут может быть сконфигурирован для той же маски сети / подсети, которая было изучено динамически с помощью протокол динамической маршрутизации, таких как RIP. Маршрутизатор должен выбрать, какой маршрут следует установить.

Хотя менее распространены, более чем один протокол динамической маршрутизации могут быть развернуты в той же сети. В некоторых ситуациях это может быть необходимо для маршрутизации тот же сетевой адрес, используя несколько протоколов маршрутизации, например RIP и OSPF. Поскольку различные протоколы маршрутизации используют различные метрики- RIP использует количество переходов и OSPF использует полосу пропускания не возможно сравнить метрику, для определения наилучшего пути.

Таким образом маршрутизатор определяет, какой путь для установки в таблице маршрутизации, когда он узнал о той же сети из более чем одного источника маршрутизации на основе административной расстоянии источника маршрутизации.

На рисунке 1.8 показана топология с R2 управляющими EIGRP и RIP. R2 управляет EIGRP с R1 и RIP с R3.

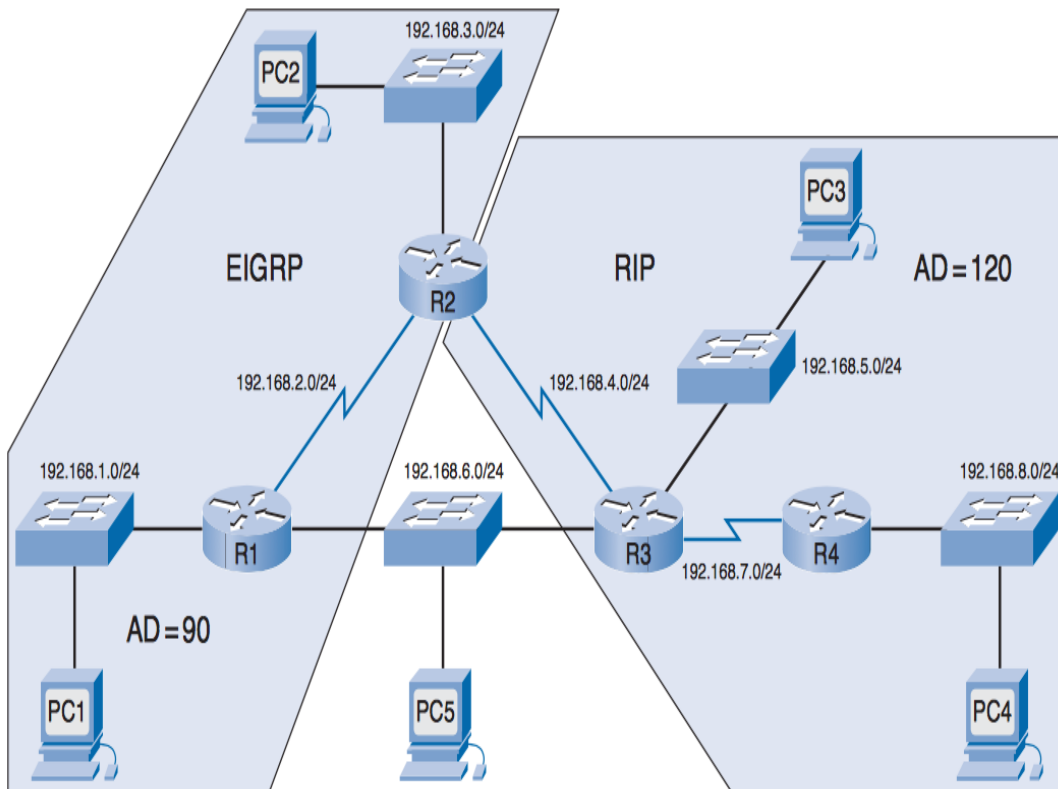


Рисунок 1.8 – Сравнение Административных Расстоянии

Пример ниже показывает вывод команды маршрута Show IP для R2.

```
R2# show ip route
```

```
<output omitted>
```

```
Gateway of last resort is not set
```

```
D 192.168.1.0/24 [90/2172416] via 192.168.2.1, 00:00:24, Serial0/0
```

```
C 192.168.2.0/24 is directly connected, Serial0/0/0
```

```
C 192.168.3.0/24 is directly connected, FastEthernet0/0
```

```
C 192.168.4.0/24 is directly connected, Serial0/0/1
```

```
    R 192.168.5.0/24 [120/1] via 192.168.4.1, 00:00:08, Serial0/0/1
```

D 192.168.6.0/24 [90/2172416] via 192.168.2.1, 00:00:24,

Serial0/0/0

R 192.168.7.0/24 [120/1] via 192.168.4.1, 00:00:08, Serial0/0/1

R 192.168.8.0/24 [120/2] via 192.168.4.1, 00:00:08, Serial0/0/1

Величина AD (административное расстояние) является первое значение в скобках для записи таблицы маршрутизации. Обратите внимание на то, что R2 имеет маршрут к сети 192.168.6.0/24 со значением AD 90.

D 192.168.6.0/24 [90/2172416] via 192.168.2.1, 00:00:24, Serial0/0/0

R2 управляет и RIP и EIGRP протоколы маршрутизации. Как уже написано выше не обычно для маршрутизаторов запускать несколько протоколов динамической маршрутизации, но используется здесь, чтобы продемонстрировать, как работает административный расстояние. R2 узнал о 192.168.6.0/24 маршрута из R1 с помощью обновлений EIGRP и из R3 с помощью обновлений RIP. RIP имеет административное расстояние 120, но EIGRP имеет более низкую административную дистанцию 90. Таким образом, R2 добавляет маршрут узнав использованием EIGRP в таблице маршрутизации и передает все пакеты для 192.168.6.0/24 сети на маршрутизатор R1 [8].

Протокол маршрутизации – это набор правил, которые маршрутизатор использует для обмена информацией о достижимости и состоянии сети. Существуют два понятия, которые нельзя путать:

- Маршрутизируемый протокол – любой протокол с адресом сетевого уровня, который осуществляет пересылку пакетов между хостами. У этого протокола, как правило, нет информации обо всем маршруте от источника до места назначения. Например, протокол IP;
- Протокол маршрутизации – набор сообщений, правил и алгоритмов которые используются маршрутизаторы для общей цели обучения маршрутов. Этот процесс включает в себя обмен и анализ информации о маршрутизации.

Протоколы маршрутизации различаются по типу взаимодействия между сетями. Это различие связано с понятием автономная система (рисунок 1.8) [9].

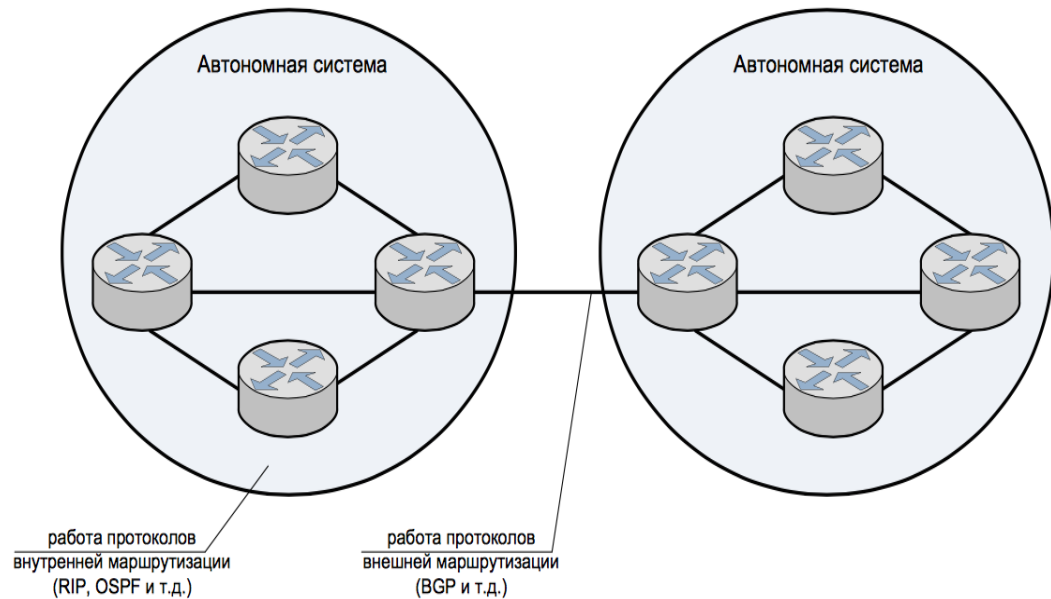


Рисунок 1.8 – Классификация протоколов по типу взаимодействия между сетями

Автономная система (АС) – является совокупностью сетей под административным управлением одной организации.

В соответствии с этим понятием существует два типа протоколов маршрутизации:

Внутренний протокол маршрутизации – протокол, служащий для обмена информации внутри АС. Например: RIP, OSPF, EIGRP, IS-IS и др.;

Внешний протокол маршрутизации – протокол, служащий для обмена информации между автономными системами. Например: BGP. Такое разделение протоколов определяет иерархический метод маршрутизации.

Протоколы маршрутизации еще можно классифицировать по использованию определенного алгоритма маршрутизации, который необходим

для определения оптимального пути прохождения пакетов от источника к месту назначения.

Требования, которым должны отвечать алгоритмы маршрутизации:

- оптимальность – способность алгоритма выбрать лучший путь;
- простота – алгоритм не должен требовать большой программной реализации;
- живучесть – алгоритм должен функционировать в случае непредвиденных обстоятельств, например отказ оборудования, высокие нагрузки на сети и т.д.;
- быстрая сходимость – процесс соглашения между всеми маршрутизаторами по оптимальным путям. Т.е., например, при отказе какого либо маршрутизатора, сообщения об обновлении топологии сети должны дойти до других маршрутизаторов с минимальной задержкой. В итоге маршрутизаторы пересчитывают пути и выбирают оптимальный. Алгоритмы, которые сходятся медленно, могут привести к нежелательным последствиям, такой как выход из строя всей сети.
- гибкость – алгоритм должен точно и быстро адаптироваться к изменениям в сети. Например, изменение топологии сети, полосы пропускания определенных линий, задержка и т.п.;

Различают следующие основные алгоритмы маршрутизации:

Статические – при статическим методом маршрутизации системный администратор вручную прописывает записи в таблице маршрутизации. Такой метод маршрутизации непригоден для больших сетей, кроме этого его сложно настраивать при изменении топологии сети;

Динамические – этот алгоритм учитывает изменения на сети, с помощью поступающим сообщениям. При изменении топологии произойдет пересчет путей, после чего осуществится новая рассылка сообщений об изменении маршрутов [8,10].

Таблица 1.4 сравнение особенностей динамической и статической маршрутизации.

Особенность	Динамическая маршрутизация	Статическая маршрутизация
Сложность конфигурации	В общем независимый от размера сети	Увеличивает с размером сети
Требуемое знание администратора	Дополнительные знания требуется	Не требует дополнительных знаний
Изменения топологии	Автоматически адаптируется к изменениям топологии	требуется вмешательство администратора
Масштабирование	Подходит для простых и сложных топологий	Подходит для простых топологий
Использование ресурса	Использует процессора, памяти и пропускной способности канала	Никакие дополнительные ресурсы необходимые

Преимущества и недостатки статической маршрутизации

Преимущества статической маршрутизации заключаются в следующем:

- Минимальная обработка центрального процессора
- Проще для администратора, чтобы понять
- Легко настроить

Недостатки статической маршрутизации заключаются в следующем:

- Конфигурация и обслуживание требуют больших затрат времени.
- Конфигурация подвержено ошибкам, особенно в больших сетях.
- Вмешательство администратора требуется для поддержания изменения информации о маршруте.
- Не масштабировать хорошо с растущей сети; техническое обслуживание становится громоздким.
- Требуется полное знание всей сети для надлежащего осуществления.

Преимущества и недостатки динамической маршрутизации

Преимущества динамической маршрутизации заключаются в следующем:

- Администратор имеет меньше работы в поддержании конфигурации при добавлении или удалении сетей.
- Протоколы автоматически реагируют на изменения топологии.
- Конфигурация меньше подвержены ошибкам.
- Более масштабируемым; рост сети обычно не представляют собой проблему.

Недостатки динамической маршрутизации заключаются в следующем:

- Используются ресурсы маршрутизатора (циклы процессора, памяти и пропускной способности линии связи).
- Больше знания администрации требуется для конфигурации, проверки, и поиска неисправностей [9-13].

Динамические протоколы маршрутизации и конвергенция

Важной характеристикой протокола маршрутизации является, как быстро она сходится, когда есть изменения в топологии.

Сходимость – это процесс согласования между всеми маршрутизаторами сети информации о доступных маршрутах. При изменениях состояния сети необходимо, чтобы обмен модификациями восстановил согласованную сетевую информацию. Время конвергенции это время, затрачиваемое маршрутизатором для обмена информацией, расчета лучшего пути и обновления своих таблиц маршрутизации. Сеть не полностью функционирует, пока сеть не сходится. Таким образом, большинство сетей требуют короткое время конвергенции.

Конвергенция является и совместной и независимой. Маршрутизаторы разделяют информацию друг с другом, но должны независимо вычислять влияние изменения топологии на их собственные маршруты. Свойства конвергенция включают скорость распространения информации маршрутизации и расчет оптимального пути. Протоколы маршрутизации могут быть оценены на основе скорости сходимости; чем быстрее конвергенция, тем лучше протокол маршрутизации. Как правило RIP и IGRP медленно сходятся, относительно таких протоколов как EIGRP, OSPF и IS-IS, которые сходятся гораздо быстрее.

Метрики

Метрики являются способом для измерения или сравнения. Протоколы маршрутизации используют метрики, чтобы определить, какой маршрут является наилучшим путем. Метрика является значениями, связанные с определенными маршрутами, оценивая их от наиболее предпочтительного до наименее предпочтительного.

Параметры, используемые для определения метрики отличаются для различных протоколов маршрутизации. Путь с наименьшей метрикой выбирается в качестве оптимального пути и устанавливается в таблице маршрутизации.

Цель метрики

Бывают случаи, когда протокол маршрутизации узнает более одного маршрута к одному пункту назначения. Для того, чтобы выбрать наилучший путь, протокол маршрутизации должен иметь возможность оценивать и дифференцировать среди доступных путей. Для этой цели используется метрика.

Каждый протокол маршрутизации вычисляет его метрику различным способом. Например, RIP использует счетчик переходов, EIGRP использует комбинацию пропускной способности и задержки, и OSPF использует стоимость.

Метрики и протоколы маршрутизации

Две разные протоколы маршрутизации могут выбрать разные пути к одному месту назначения из-за использования различных метрик.

Метрики, используемые в протоколах маршрутизации IP включают в себя следующие:

- Количество переходов: простая метрика, которая подсчитывает количество маршрутизаторов пакет должен пройти.
- Полоса пропускания: влияет на выбор пути, предпочитая путь с самой высокой пропускной способностью.
- Нагрузка: считает использование трафика определенные ссылки.
- Задержка: считает время, которое пакет нужен чтобы пройти путь.
- Надежность: оценивает вероятность отказа канала, рассчитанное по количеству ошибок интерфейса или предыдущих отказов каналов.
- Стоимость: значение определяется либо IOS или сетевым администратором, чтобы указать предпочтение маршрута. Стоимость может представлять собой метрику, сочетание метрик или политики.

Рисунок 1.9 показывает, как R1 достигнет 172.16.1.0/24 сеть. RIP будет выбрать путь с наименьшим количеством переходов через R2, тогда как OSPF будет выбирать путь с высокой пропускной способностью через R3.

RIP выбирает кратчайший путь, основанный на количестве переходов.

OSPF выбирает кратчайший путь, основанный на пропускной способности.

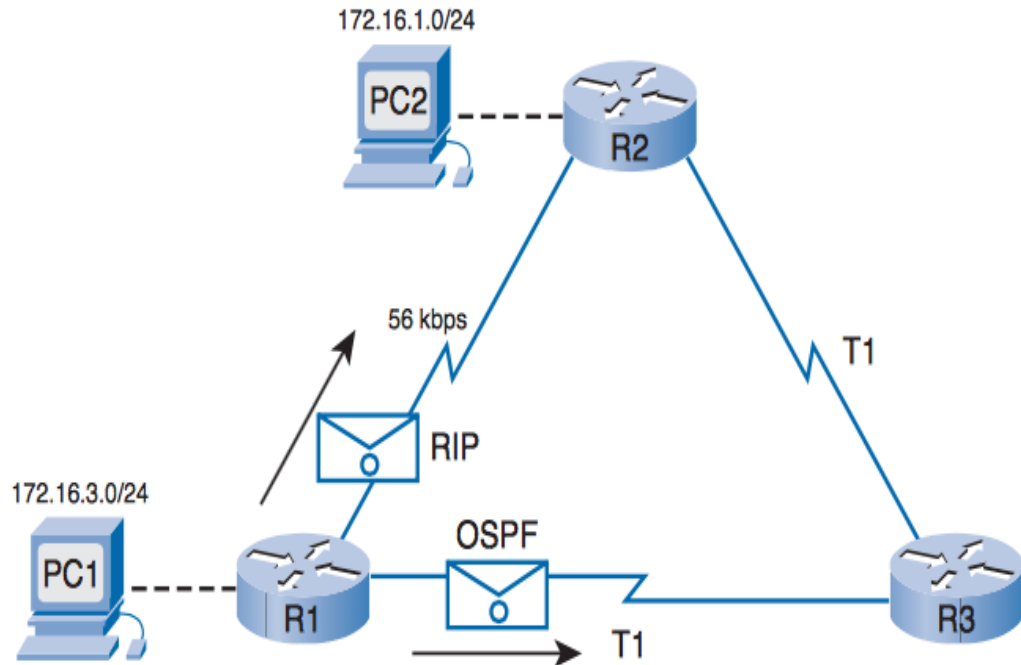


Рисунок 1.9 – выбор наилучшего пути в сети

метрики для каждого протокола маршрутизации

- **RIP: количество переходов:** Лучший путь выбирается маршрут с наименьшим числом переходов.
- **IGRP и EIGRP: полоса пропускания, задержка, надежность и нагрузка:** Лучший путь выбирается маршрут с наименьшим значением композиционного показателя рассчитанного из этих нескольких параметров. По умолчанию используются только пропускная способность и задержка.
- **OSPF: стоимость:** Лучший путь выбирается маршрут с наименьшими затратами. Реализация OSPF в Cisco использует пропускную способность для определения стоимости.

Балансировка нагрузки

Протоколы маршрутизации используют метрики, чтобы определить, какой маршрут наилучший путь как уже объяснено выше. Но когда два или более маршрутов к одному месту назначения имеют одинаковые значения метрики, маршрутизатор не выбирает только один маршрут.

Вместо этого маршрутизатор распределяет нагрузку (балансирует нагрузку) между этими путями равных стоимости. Пакеты передаются с использованием всех пути равных стоимости. Механизм работает для всех стандартных протоколов маршрутизации за исключением BGP, в котором по умолчанию используется только один маршрут.

Балансировка нагрузки по месту назначения или по пакетам

Можно настроить балансировку нагрузки на основе адресата назначения или на основе пакетов.

Балансировка нагрузки по адресату назначения значит, что маршрутизатор распределяет пакеты на основе адреса назначения. При наличии двух путей доступа к одной сети, все пакеты для назначения 1 в этой сети пересылаются по первому пути, а все пакеты для назначения 2 в этой сети пересылаются по второму пути и.т.д. При этом сохраняется порядок пакетов с потенциально неравномерным использованием каналов. Если один узел получает большую часть трафика, все пакеты используют один канал, тогда как полоса пропускания других каналов остается неиспользуемой. Увеличение числа адресов назначения приводит к более равномерному использованию каналов.

Балансировка нагрузки по пакетам означает, что маршрутизатор отправляет один пакет для назначения 1 по первому пути, а второй пакет для этого же назначения 1 по второму пути и т.д. Балансировка нагрузки по пакетам гарантирует равномерное распределение нагрузки между всеми каналами. Однако существует вероятность нарушения порядка следования пакетов, при их достижении адресата назначения, из-за возможного существования дифференциальной задержки в сети.

На рисунке 1.10 показан пример балансировки нагрузки, предполагая что R2 балансирует нагрузку трафика к PC5 на две пути равной стоимости [13-20].

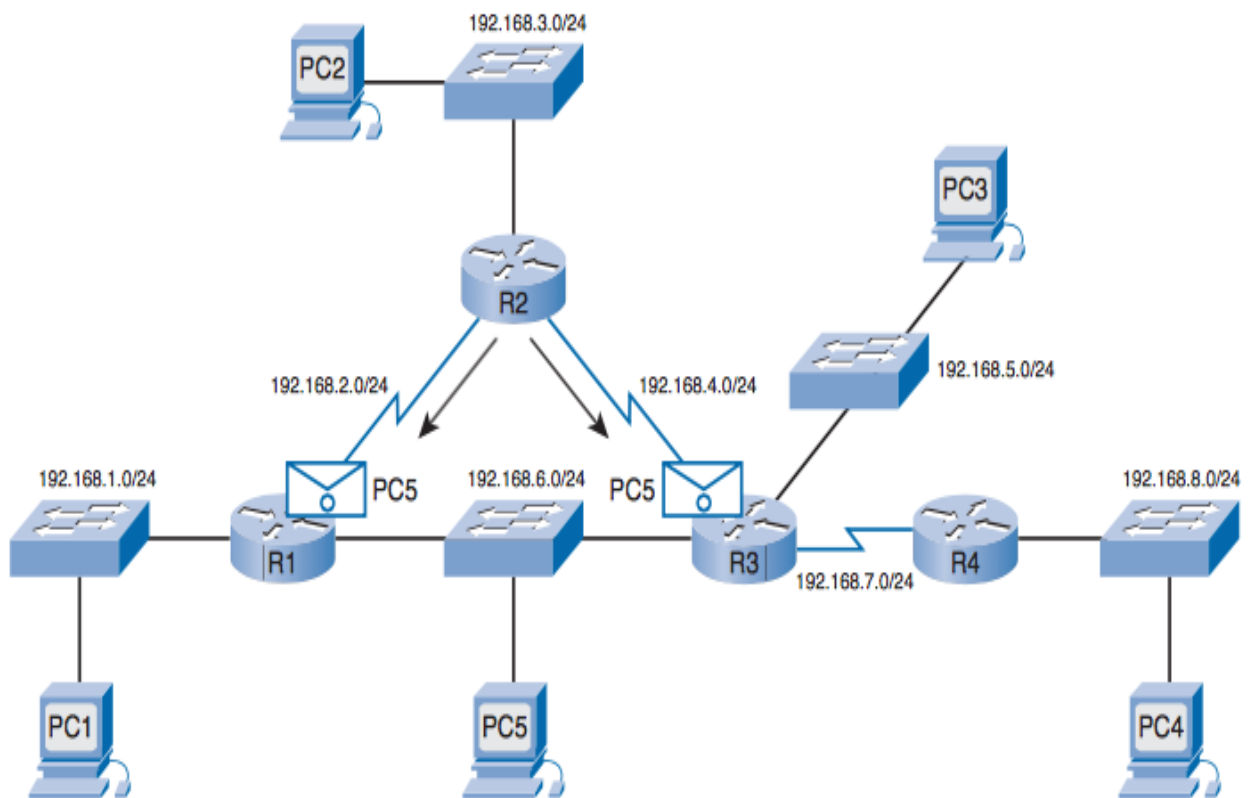


Рисунок 1.10 – балансировка нагрузки между Путиами равной стоимости

Балансировка нагрузки в действие, если два или более маршрутов связаны с тем же самым назначением в таблице маршрутизации.

Команда маршрута Show IP (показать IP) в примере 3-1 показывает, что сеть назначения 192.168.6.0 доступна через 192.168.2.1 (Serial 0/0/0) и 192.168.4.1 (Serial 0/0/1). Маршруты равной стоимости показаны снова здесь:

```
R2# show ip route
```

```
<output omitted>
```

```
R      192.168.6.0/24 [120/1] via 192.168.2.1, 00:00:24, Serial0/0/0
                               [120/1] via 192.168.4.1, 00:00:26, Serial0/0/1
```

Механизм балансировка нагрузки работает для всех стандартных протоколов маршрутизации.

Протоколы внутренней маршрутизации можно классифицировать по использованию одного из следующих динамических алгоритмов маршрутизации:

Метод маршрутизации на основе вектора расстояний: является методом определяющим направление и расстояние (например, количество переходов) к любому каналу другой сети, путем рассылки вектора. При получении вектора от соседа маршрутизатор увеличивает расстояние, а также добавляет информацию об известных ему сетях и рассылает новое значение вектора по сети. Минус этого метода в том, что в больших сетях ширококовечательная рассылка отрицательно скажется на работе сети.

Метод маршрутизации на основе состояние канала: при методом на основе состояние канала маршрутизаторы обмениваются сообщениями о состоянии канала со своими соседями, при этом каждый маршрутизатор создает базу данных топологии сети, на основе полученных сообщений. После этого алгоритм снимает лишние пути и составляет свое дерево кратчайших путей.

В алгоритмах маршрутизации используется много различных показателей, называемых метрикой. Это число, которое генерирует алгоритм для каждого пути. Меньшая метрика обычно означает наилучший путь. Сложные алгоритмы маршрутизации при выборе маршрута могут базироваться на множестве показателей или их комбинации. Ниже перечислены метрики, которые чаще всего используются в алгоритмах маршрутизации.

- Количество переходов. Число которое показывает, сколько переходов через оборудование должен совершить пакет, чтобы добраться от источника к месту назначения.

- Скорость передачи данных в канале (полоса пропускания).

- Задержка. Время, которое необходимо для передачи пакета от источника до места назначения. Задержка может зависеть от многих факторов, таких как загрузка сети, пропускная способность каналов и т.д.

- Надежность. Это, относится к достоверности канала связи. Некоторые каналы сети могут отказывать чаще, чем другие. Отказы одних каналов могут быть устранены легче или быстрее, чем отказы других каналов сети. При назначении оценок надежности могут быть приняты в расчет любые факторы надежности.

- Стоимость. Это является настраиваемым значением [17-27].

2 ОБЗОР ПРОТОКОЛОВ МАРШРУТИЗАЦИИ

2.1 Протокол маршрутизации на базе вектора расстояний

Одним из наиболее распространенных протоколов маршрутизации на основе вектора расстояний, является протокол RIP (Routing Information Protocol). Основные характеристики протокола RIP:

- дистанционно-векторный протокол маршрутизации; метрика – число переходов;
- максимальное число переходов – 15;
- широковещательная рассылка обновлений маршрутизации по умолчанию – раз в 30 секунд.

Эволюция протокола RIP заключалась в переходе от классового протокола маршрутизации (RIPv1) к бесклассовому протоколу (RIPv2). В соответствии с этим RIPv2:

- поддерживает маску переменной длины;
- отправляет маску подсети вместе с обновлением маршрутизации;
- групповая рассылка (RIPv1– широковещательная рассылка);
- поддержка суммирования маршрутов вручную;
- поддержка аутентификации (процедура проверки подлинности).

Сразу возникает вопрос чем состоит основное отличие классовой маршрутизации от бесклассовой. Существует такое понятие как маска подсети которая является набором битов, определяющий, какая часть в IP-адресе показывает адрес сети, а какая показывает адрес узла в этой сети. Набор представляет собой непрерывную последовательность единиц и нулей .

IP Адрес – хоста 13.14.49.121

13 14 49 121
 00001101.00001110.00110001.01111001

Маска

255 255 255 0 = /24

11111111.11111111.11111111.00000000

сеть

хосты

Компактная запись

IP Адрес – хоста 13.14.49.121/24

IP Адрес – сети 13.14.49.0

Классовая адресация необходима для разделения сетей на подсети, при этом используются «стандартные» маски, таким образом

Для сетей класса А – маска 255.0.0.0, для сетей класса В – маска 255.255.0.0, для сетей класса С – маска 255.255.255.0.

Так как маленьких сетей намного больше, чем представлено в классе С, ввели бесклассовую адресацию. Для организации такой адресации используют маски переменной длины.

IP Адрес – хоста 13.14.49.121

13 14 49 121

00001101.00001110.00110001.01111001

Маска

255 255 255 192 = /26

11111111.11111111.11111111.11000000

сеть

хосты

IP Адрес – сети

13 14 49 121

00001101.00001110.00110001.01111001

00001101.00001110.00110001.01000000

Компактная запись

IP Адрес – хоста 13.14.49.121/26

IP Адрес – сети 13.14.49.64

Учитывая это, можно сказать, что протокол RIPv2 с поддержкой бесклассовой маршрутизацией имеет больше возможностей.

Принцип работы протокола RIP

Маршрутизаторы обмениваются сообщениями о маршрутизации только со своими соседями (прямое подключение). Эти обновления происходят периодически, вне зависимости изменилась топология сети или нет, и включают в себя полную таблицу маршрутизации. Получив таблицу, маршрутизатор вносит определенные изменения в свою таблицу.

Существует ряд проблем, которые возникают с работой протокола RIP. Например, есть три маршрутизатора, которые соединены последовательно (рис. 2.1) . У каждого маршрутизатора уже составлена своя таблица маршрутизации до каждой сети. Неожиданно, сеть No4 отказала в доступе, соответственно маршрутизатор No3 прекращает отправлять пакеты в эту сеть. Но маршрутизаторы No1 и No2 не знают об отказе сети No4.

Маршрутизатор No1 видит, что сеть доступна через маршрутизатор No2, то есть в таблице маршрутизации указана сеть No4 с метрикой 2. Соответственно эта сеть так же записывается на втором маршрутизаторе, как известная. Таблица маршрутизации отправляется маршрутизатору No3, и он считает, что он имеет доступ к сети No4 через маршрутизатор No2.

Таким образом, метрика будет расти по кругу до бесконечности. Эта проблема решается путем задания максимума, в случае с протоколом RIP этот максимум равен 16 переходам.

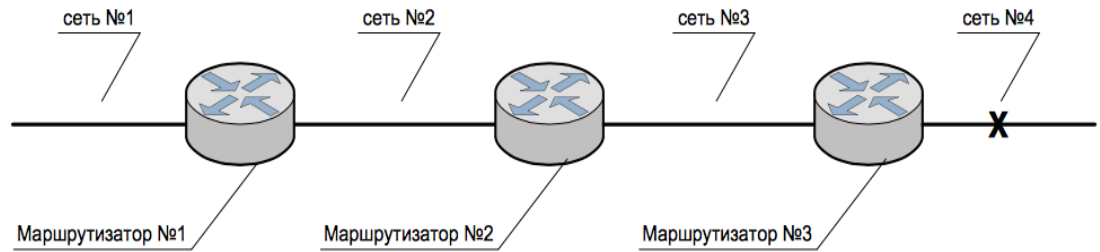


Рисунок 2.1 - Пример последовательного соединения маршрутизаторов

Иногда в сетях, которые используют протокол RIP, возникают петли. Из рассмотренного примера видно, что при отказе сети No4 посланный пакет из сети No1 будет бесконечно блуждать между маршрутизаторами No2 и No3, то есть образуется петля. Есть несколько методов, которые не допускают образование петель.

1 Split Horizon.

Суть метода заключается в том, что маршрутизатор не будет отправлять данные о маршруте в обратную сторону.

2 Route Poisoning

При отказе сети No4 маршрутизатор No3 присваивает каналу в этом направлении метрику 16 переходов (то есть сеть недоступна). Благодаря этому маршрутизатор не будет воспринимать поступающие обновления (информация, что сеть доступна) от других маршрутизаторов.

3 Таймеры удержания.

Таймер удержания информации позволяет предотвратить петли, однако увеличивает время сходимости сети. Стандартное время удержания в протоколе RIP составляет 180 секунд. Это время можно изменять. Идеальным решением является установка этого периода чуть большим максимального времени обновления маршрутов данной сети.

Так, если отказала сеть No4, сразу же на маршрутизаторе No3 запускается таймер удержания, и маршрут к сети No4 отмечается как недоступный. Если от

соседних маршрутизаторов придет обновление с лучшей метрикой, то сеть станет доступна, и таймер будет удален. В ином случае обновления будут игнорироваться. Благодаря этому увеличится время, чтобы распространить обновления об изменении сети.

Вывод:

В современных сетях протокол RIP не самое лучшее решение для выбора в качестве протокола маршрутизации, так как его возможности уступают более современным протоколам, таким как EIGRP и OSPF. Ограничение на 15 переходов(хопов) не позволяет применять его в больших сетях. Преимущество этого протокола является простотой конфигурирования. Поэтому, если сеть небольшая, то протокол RIP вполне приемлем как протокол маршрутизации [26,29,33].

2.2 Протокол маршрутизации на основе состояния канала

Одним из распространенных протоколов на основе состояния канала является протокол OSPF. Это бесклассовый протокол маршрутизации. Технология работы протокола заключается в отслеживании состояния каналов и поиска кратчайших путей (Shortest Path First – SPF), используя алгоритм Дейкстры. Протокол поддерживает сложную топологическую базу данных. Если протоколы на базе вектора расстояний не содержат информацию об удаленных сетях, то протоколы на основе состояния канала поддерживают всю информацию об удаленных маршрутизаторах и их соединениях.

Состояние канала в этом протоколе подразумевает описание интерфейса (например, IP-адрес, маска, тип сети и т.п.) и его отношение с соседними маршрутизаторами. На основе выше указанных описаний интерфейсов формируется база данных состояния каналов.

База данных заполняется благодаря получению сообщений о состоянии канала (Link-State Advertisement – LSA), которые распределяются часто или же сразу после изменения топологии сети, или при каких-либо изменениях на маршрутизаторах. Эти сообщения представляют собой небольшие пакеты. В LSA содержится информация о подключенных интерфейсах, метриках и других параметрах.

На основе полученных сообщений LSA маршрутизатор использует алгоритм SPF, который строит дерево кратчайших маршрутов. Алгоритм производит расчет над базой данных топологии сети, удаляя лишние ветви (ветви – все возможные пути). Полученные маршруты записываются в таблицу маршрутизации.

Протокол OSPF – внутренний протокол маршрутизации и работает внутри одной автономной системы. Ее можно разбить на зоны или области, которые представляют собой логические разделы автономной системы.

Рассмотрим двухуровневую сетевую иерархию, в которой у всех маршрутизаторов свой принцип работы.

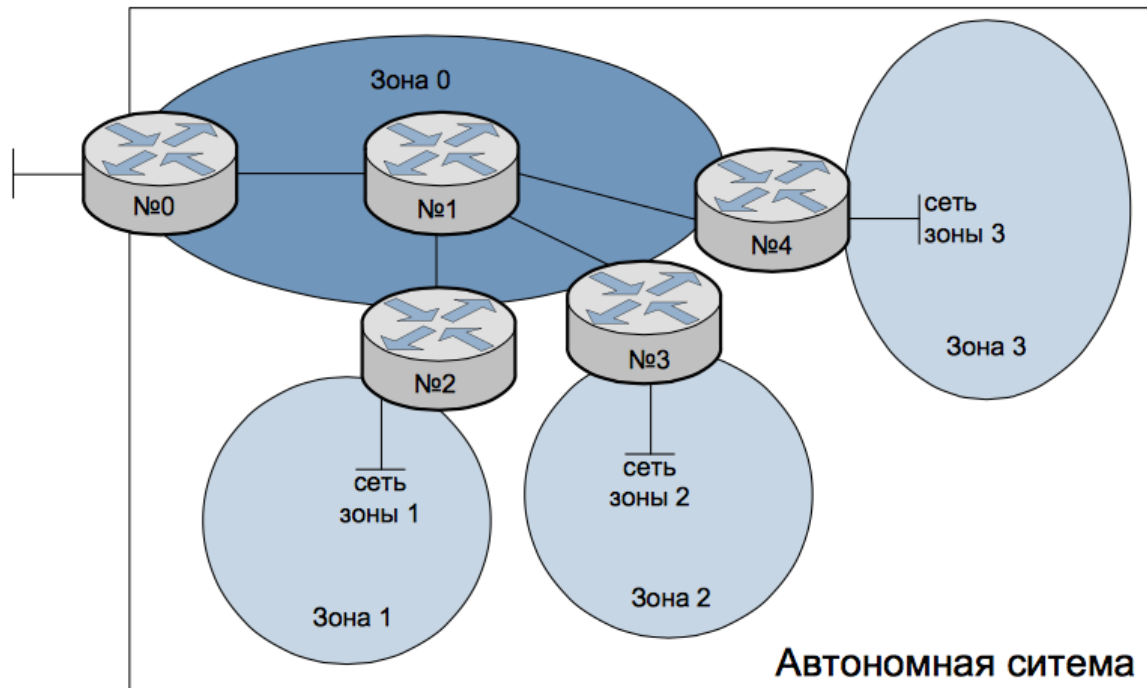


Рисунок 2.2 - Двухуровневая сетевая иерархия

На рисунке 2.2 представлена одна автономная система, имеющая один пограничный маршрутизатор (марш. No0), который служит для связи с внешней сетью (например, с другой автономной системой).

Автономная область включает в себя:

- зону 0 – область, которая отвечает за соединение всех областей, иногда ее можно называть магистральной областью. Маршрутизатор No1 в этой области называют магистральным;
- зоны 1-3 – маршрутизаторы в этих областях называются не магистральными. Это маршрутизаторы, которые знают топологию области, в которых они находятся, и ведут базу данных состояний каналов только своих областей;

- на стыке зоны 0 и зон 1-3 находятся пограничные маршрутизаторы No2-4. Эти маршрутизаторы ведут базу данных состояний каналов всех областей, к которым они подключены;
- маршрутизатор No0 так же является пограничным, но уже для автономной системы.

OSPF выполняет следующие функции:

- формирует отношения с соседями;
- рассылает LSA для формирования на каждом маршрутизаторе базы данных;
- запускает SPF для расчёта наилучших маршрутов ко всем получателям;
- заполняет таблицы маршрутизации наилучшими маршрутами ко всем получателям.

Протокол OSPF формирует отношения с соседями следующим образом. Два маршрутизатора, т.е. маршрутизаторы-соседи, которые работают по протоколу OSPF, должны «видеть» друг друга в сети, прежде чем будут обмениваться информацией. Этот процесс реализуется с помощью протокола Hello. Маршрутизаторы, в которых реализован протокол OSPF, со всех интерфейсов рассылают hello-пакеты (многоадресная рассылка – 224.0.0.6), которые содержат следующую информацию:

- Router ID – идентификатор маршрутизатора – 32-х битный уникальный номер для маршрутизатора. По умолчанию выбирается самый большой IP- адрес активного интерфейса. Эта идентификация важна для установления соседских отношений и устранения неполадок в них, а также для координации обмена данными маршрутизации;

- Hello и Dead интервалы – интервалы приветствия и простоя. Интервал приветствия определяет период отправки hello-пакетов маршрутизатором (по умолчанию – 10 секунд). Интервал простоя – это время, в течение которого маршрутизатор ожидает hello-пакет от соседнего маршрутизатора, прежде чем объявить его неисправным (по умолчанию интервал простоя в четыре раза превышает интервал приветствия). Эти интервалы должны быть одинаковыми на соседних маршрутизаторах, иначе соседские отношения не будут реализованы;

- Neighbors – соседи, в этом поле перечислены все соседние маршрутизаторы, с которыми установлено двусторонне соединение;

- Area ID – идентификатор области. Для взаимодействия между собой, маршрутизаторы должны находиться в одном сегменте и их интерфейсы должны принадлежать к одной области OSPF в этом сегменте. Так же, соседние узлы должны использовать одинаковую подсеть и маску;

- Router priority– приоритет маршрутизатора – 8-ми битный номер, который необходим для выбора выделенного маршрутизатора (designated router, DR) и запасного выделенного маршрутизатора (backup designated router, BDR). Эти два типа маршрутизаторов необходимы для предотвращения проблемы рассылки копий LSA в сетях.

DR– управляет процессом рассылки LSA в сети. Информация об изменениях в сети рассылается всем маршрутизаторам от DR маршрутизатора, обнаружившего это изменение.

BDR – при выходе из строя DR, BDR становится DR и выполняет все его функции. DR и BDR также устанавливают отношения соседства и между собой. Роль DR (BDR) является свойством интерфейса, а не свойством всего маршрутизатора;

- DR и BDR ip-адреса – если известны;
- Authentication password – пароль для аутентификации, если аутентификация включена. Пароль на всех маршрутизаторах должен быть одинаковый;
- Stub area flag – флаг тупиковой области. Тупиковая область – особая область среды OSPF. Два маршрутизатора должны согласовать флаг тупиковой области в hello-пакетах.

Для формирования соседства поля hello-пакета – Hello interval, Dead interval, Area ID, Authentication Password и Stub Area Flag – должны совпадать.

Вывод:

Протокол OSPF имеет ряд преимуществ:

- маршруты, вычисленные протоколом OSPF, не могут быть циклическими;
- протокол обеспечивает масштабируемость для больших сетей;
- быстрая перенастройка при изменении топологии сети.

К недостатком же относится:

- иерархическая топология;
- отсутствует распределение нагрузки при неэквивалентных путях;
- метрика использует только стоимость маршрута [29,32-40].

2.3 Усовершенствованный протокол маршрутизации на базе вектора расстояний

Усовершенствованным протоколом маршрутизации на базе вектора расстояний является протокол EIGRP. Он был разработан компанией Cisco Systems, следовательно, часто используется на оборудовании этой компании.

Протокол обладает следующими качествами.

- Более быстрая сходимость в сравнении с другими протоколами на базе вектора расстояний, которая достигается благодаря алгоритму DUAL (Diffusing Update Algorithm). Алгоритм составляет таблицу топологий, в которой указано два лучших пути к сети назначения (основной и резервный). На обоих этих маршрутах не возникают петли.

- Снижение потребления полосы пропускания достигается за счет того, что при любых изменениях в сети, алгоритм DUAL отправляет только новые обновления, а не всю таблицу маршрутизации.

- Поддержка нескольких протоколов сетевого уровня (IP, IPX, AppleTalk).

- Бесклассовый протокол маршрутизации.

- Использование многоадресной (224.0.0.10) и одноадресной рассылки, вместо широковещательной. Благодаря этому обновления маршрутизации не влияют на ненужные маршрутизаторы.

Принцип работы протокола EIGRP

1. Протокол EIGRP сначала должен обнаружить своих соседей, для этого он использует протокол Hello, который в свою очередь рассылает hello- пакеты (по умолчанию каждые 5 секунд). Для отправки пакетов используется многоадресная рассылка. Пока hello-пакеты приходят от соседа, маршрутизатор определяет его как функционирующий. Если в течение определенного времени (по умолчанию 15 секунд) от соседа не пришел hello- пакет, он считается недоступным.

2. После того, как соседи установлены, происходит обмен информацией о топологии сети. Сначала пересылается информация о полной топологии сети

между маршрутизаторами. А далее, при изменении на сети, маршрутизаторы обмениваются следующими пакетами:

- Пакет обновления маршрутов (Update). В этих пакетах хранится информация об изменении маршрутов. Пакеты могут пересылаться по многоадресной или одноадресной рассылке.

- Пакет запросов (Query). Этот пакет необходим, когда маршрутизатор пересчитывает какой-либо маршрут, и у него нет резервного. Маршрутизатор отправляет запрос соседям. Если у соседей есть маршрут, то они отвечают путем посылки пакета ответа на запрос (Reply). Если маршрута нет, то они отправляют запрос уже своим соседям.

- Пакет подтверждения (Acknowledgment). при получении выше указанных пакетов (update, query, reply), ответно посылаются пакеты подтверждения. Для надежной и гарантированной доставки отправленных пакетов протокол EIGRP использует надежный транспортный протокол (Reliable Transport Protocol — RTP). Протокол неоднократно пересылает маршрутную информацию, если сообщение было потеряно. За счет использования протокола RTP уменьшается вероятность возникновения петель.

3. Далее происходит выбор наилучшего пути. Маршрутизаторы анализируют топологическую таблицу и выбирают из нее путь с наименьшей метрикой. Протокол считает ее с помощью весовых коэффициентов (по умолчанию $K1=1$; $K2=0$; $K3=1$; $K4=0$; $K5=0$), а также полосы пропускания (bandwidth) и задержки (delay).

Формула для расчета полосы пропускания выглядит так:

$$\text{bandwidth} = \frac{10000000}{\text{bandwidth}} * 256$$

bandwidth(m) – это минимальная пропускная способность канала на всем пути следования к сети назначения.

Формула для расчета задержки выглядит так:

$$\text{delay} = \text{delay}(s) * 256$$

delay(s) – это суммарная задержка на всех маршрутизаторах по пути следования к сети назначения.

Полученные значения используются для подсчета метрики:

$$\text{Metric} = (K1 * \text{bandwidth} + \frac{K2 * \text{bandwidth}}{256 - \text{load}} + K3 * \text{delay}) * \frac{K5}{\text{reliability} + K4}$$

Если коэффициенты оставить по умолчанию, то:

$$\text{Metric} = K1 \text{ bandwidth} + K3 \text{ delay}$$

В таблице топологий находятся все известные маршрутизатору пути. Приведем пример строки в таблице.

R 192.168.30.0/24, 1 successors, FD is 156160 via 10.0.0.1 (156160/128256),
FastEthernet0/0

R – отвечает за состояние записи. Их два: Passive (пассивный) и Active(активный). Первый значит, что маршрут используется и его пересчет не нужен. Состояние Active обозначает, что происходит пересчет маршрута. 192.168.30/24 IP-адрес сети и маска.

Successor – это маршрутизатор, через который проходит оптимальный маршрут в сеть.

FD (Feasible distance) – это метрика, которую будет использовать маршрутизатор. В данном случае она равна 156160.

10.0.0.1 – IP-адрес соседа. 128256 тоже метрика, называется она Advertised distance (AD) и показывает метрику маршрута в сеть для того маршрутизатора, который объявляет об этом маршруте.

Так же в таблице топологий могут встретиться следующие понятия:

FS (Feasible Successor) – это резервный маршрутизатор, через который можно попасть в некоторую сеть, если выйдет из строя Successor (маршрутизатор, через который проходит оптимальный маршрут).

Feasible Condition (FC). Чтобы маршрутизатор мог стать резервным для какого-то маршрута, необходимо, чтобы значение Advertised distance (AD) для этого маршрутизатора было меньше, чем Feasible distance (FD) для основного маршрута.

Таким образом, маршрутизаторы, которые работают на основе протокола EIGRP, поддерживают три таблицы.

- Таблица соседей, в которой указаны все соседи.
- Таблица топологии, в которой ведутся записи маршрутов до каждого места назначения, известные маршрутизатору.
- Таблица маршрутизации, куда заносятся лучшие маршруты из таблицы топологии [28,33,35-42].

Вывод:

К преимуществам протокола EIGRP относятся:

- быстрая сходимость в больших сетях;
- значительно меньшая загрузка каналов и CPU при работе протокола;
- Возможность балансировки трафика по неэквивалентным каналам.




Недостатком протокола EIGRP, является то что он закрыт, то есть может быть реализован только на оборудовании компании Cisco Systems.

2.4 Сравнительная характеристика внутренних протоколов маршрутизации

Таблица 2.1 – характеристика внутренних протоколов маршрутизации

	RIPv2	OSPF	EIGRP
Тип протокола	Вектор расстояний	Состояние канала	Усовершенствованный дистанционно-векторный
Алгоритм	Беллмана-Форда	Дейкстры	Алгоритм диффузного обновления (Diffused Update Algorithm – DUAL).
Метрик	Количество переходов	Полоса пропускания	Полоса пропускания, Задержка, Надежность и Нагрузка
Обновление маршрутной информации	Вся таблица	Только изменения	Только изменения
Административное расстояние	120	110	90
Бесклассовый	да	да	да
Максимальное количество маршрутизаторов в сети	15	безлимитный	255
Открытый стандарт	да	да	нет
Метрика	Одна основная	Одна основная	Комбинированная

Продолжение таблицы 2.1

Планирование сети	нет	Да(выбор зон)	нет
Сложность конфигурации			

Можно сделать вывод (таблица 2.1), что лучшими внутренними протоколами маршрутизации является OSPF и EIGRP. Особенно в применении к большим и сложным сетям. Но так же эти протоколы, не смотря на широкий спектр положительных качеств, имеют и свои минусы. Протокол OSPF имеет высокие требования к ресурсам маршрутизации из-за слишком сложного вычислительного расчета кратчайших путей. Хотя протокол EIGRP выигрывает в этом плане, он все же является закрытым. Его реализация возможна только на оборудовании Cisco Systems. Но в наше время в сетях применяется оборудование разнообразных фирм. Поэтому в крупных сетях выгоднее применять протокол OSPF [27,42-45].

3 МОДЕЛИРОВАНИЕ В СРЕДЕ RIVERBED MODELER

3.1 Технология Riverbed Modeler

Под технологией Riverbed Modeler подразумевают совокупность действий для создания модели сети и проведение на ней имитационных экспериментов. С помощью редактора проекта можно создавать модель сети, выбирать требуемую статистику, собираемую с каждого объекта сети или со всей сети, запускать процесс моделирования и осуществлять просмотр результатов.

Использование высокоуровневого моделирования позволяет гарантировать полноту и правильность выполнения информационной системой функций, определенных заказчиком.



Рисунок 3.1 – Алгоритм работы с программной системой Riverbed Modeler

Программная система Riverbed Modeler предоставляет широкие возможности моделирования вычислительной сети, представленной в

графическом виде, что является одним из основных преимуществ, так как пользователь имеет возможность видеть как всю сеть в целом, так и при необходимости отдельные ее участки.

Riverbed Modeler Academic Edition является бесплатной утилитой предназначенная абсолютно в образовательных целях для студентов учебных заведений. Установка производится после регистрации, указывая данные студента и учебного заведения.

Riverbed Modeler предоставляет собой виртуальную сетевую среду, которая моделирует поведение сетей, включая маршрутизаторы, коммутаторы, протоколы и конкретные приложения. Дружественный интерфейс Guru с технологией «перетаскивания» дает возможность эффективно моделировать, управлять, искать и устранять неполадки в реальных сетевых структурах. Эта среда позволяет IT менеджерам, проектировщикам сетей, систем и штату операторов более эффективно решать трудные проблемы, моделировать изменения прежде, чем они осуществляются, и планировать будущие сценарии, такие как рост трафика и выход из строя сегментов сети.

Можно проводить моделирование сценариев (отдельных схем и планов действий) при проектировании сетей. Программа позволяет анализировать воздействия приложений типа клиент-сервер и новых технологий на работу сети; моделировать иерархические сети, многопротокольные локальные и глобальные сети с учетом алгоритмов маршрутизации; осуществлять оценку и анализ производительности смоделированных сетей. Также с помощью пакета можно осуществить проверку протокола связи, анализ взаимодействий протокола, оптимизацию и планирование сети. В процессе моделирования можно проследить, как будут изменяться время запаздывания отклика и другие сетевые характеристики при различных подходах к конструированию сети. В результате моделирования пользователю предоставляется информация о узких

местах сети (по пропускной способности, загрузке устройства или линии связи), трафике между заданными узлами, задержки между узлами сети и др.

Чтобы создать модель сети (называемую в Riverbed Modeler проектом), необходимо определиться с узлами сети (с компьютерами, коммутаторами, маршрутизаторами и т.д.), соединениями между узлами и приложениями, которые будут работать на том или ином узле[43-50].

3.2 Топология сети

Для исследования параметров сети была разработана сетевая структура с использованием пакета Riverbed Modeler версии 17.5. Сетевая модель разработана для протоколов маршрутизации RIP, OSPF и EIGRP. Для того, чтобы получить адекватные результаты, топология и структура сети была одинакова для всех трех протоколов (количество маршрутизаторов, серверов и клиентов).

Исследуемыми параметрами являются; время конвергенции, потери пакетов, задержка голосового/ видео трафика, задержка в очереди, использование канала связи и время отклика страницы HTTP. В сетевой модели имитировалась передача голоса, видео ряда и HTTP-трафика с использованием всех трех исследуемых протоколов маршрутизации т.е. RIP, OSPF и EIGRP. При передаче информации имитировалось обрыв соединения на одной из соединительных линий в сети [51-55]. В сетевой модели применялось 6 маршрутизаторов Cisco 7000, 3 сервера (каждый из которых предоставляет рабочей станции услуг видео, голосовой или HTTP) и 6 Рабочих станций (с каждой несущей видео, голоса или HTTP-трафика). На рисунке 1 показан вид имитируемой сетевой структуры для реализации передачи голоса, видео и HTTP-трафика.

Объект определения приложения используется для описания трафика, генерируемого различными приложениями, такими как Email, HTTP, видеоконференции и т.д. Трафик каждого приложения имеет возможность генерироваться с различной интенсивностью, которая может быть дополнительно настроена или описана с использованием предварительного настроенных параметров.

Объект Определения Профиля определяет все профили, которые могут быть использованы в пределах сценария. Только профили, которые были определены в объекте определения профиля, могут быть применены на рабочие места или LAN проекта и только приложения, которые были определены в объекте определения приложения, могут быть использованы на определённых участках профиля. Как правило, конфигурация приложения и конфигурации профиля используются совместно для генерации трафика в сети.

Объект отказ и восстановление может быть использован для моделирования сценариев отказа-восстановление в данной модели. Он предоставляет атрибуты для управления временем и статусом объектов в модели. Это помогает имитировать нестабильность в сети и локальные разрывы соединений. Одна ссылка (связь между маршрутизатором 2 и маршрутизатором 3) была установлена в неустойчивое положение между маршрутизаторами R2 и R3. Для этой реализации используется утилита отказа и восстановление.

Рабочая станция Ethernet это узел модели, который представляет собой рабочую станцию с клиент-серверными приложениями, работающих через TCP/IP и UDP/IP. Рабочая станция поддерживает одно основное соединение Ethernet 10Mbps, 100Mbps и 1000Mbps. Есть 6 рабочих станций с каждой несущей видео, голоса или HTTP-трафика. Рабочие станции подключены к сети через маршрутизаторы 1 и 3, с использованием 100BaseT соединений.

Ethernet-сервер представляет собой устройство, которое обеспечивает функциональные возможности или услуги для клиентских устройств. В исследуемой модели мы имеем 3 сервера, каждый из которых предоставляет рабочей станции услуги видео, голосового или HTTP трафика. Серверы связаны с сетью через маршрутизатор 5 с использованием 100BaseT соединений.

PPP_DS3 соединяет маршрутизаторы друг с другом. Это полный дуплексное звено, которое соединяют два IP-узла.

100BaseT линия связи с полным дуплексом, которая используется для предоставления соединений Ethernet. К этим линиям можно подключить любую комбинацию из узлов, таких как станции, мост, коммутатор и узлы LAN [56].

Формулы параметров

1 Задержка в очереди связана с задержкой передачи d_{trans} по следующей приближенной формуле.

$$T_{queue} = d_{trans} \cdot l_{queue} \quad (1)$$

Здесь l_{queue} - средняя длина очереди. Средняя длина очереди зависит от коэффициента нагрузки, который является отношение попытки скорости передачи линии связи со максимальной скоростью передачи данных линии связи. Средняя длина очереди, как правило, меньше 1 для коэффициента нагрузки меньше, чем 1/2. Когда коэффициент нагрузки превышает 1, длина очереди неограниченно возрастает.

2 Сквозная задержка или односторонняя задержка (OWD) относится к времени пакет передается по сети от источника к месту назначения.

$$d_{end-end} = N [d_{trans} + d_{prop} + d_{proc} + d_{queue}] \quad (2)$$

где:

$d_{end-end}$ - Сквозная задержка; d_{trans} - задержка передачи; d_{prop} - Задержка распространения; d_{proc} - задержка обработки; d_{queue} - Задержка в очереди; N - количество ссылок (Количество маршрутизаторов - 1)

3 Время сходимости (Convergence_Time) определяется в соответствии с выражением :

$$T_{conv} = T_{FD} + LSA_{Gt} + T_{EP} + SPF_{rt} + RIB_{FIB} \quad (3)$$

где: T_{FD} - время, необходимое для обнаружения отказа; LSA_{Gt} – время генерации и начала рассылки LSA - сообщения об отказе элемента сети и изменении топологии; T_{EP} - время, необходимое для распространения LSA-сообщений о топологии всем маршрутизаторам в сети; SPF_{rt} - время, необходимое для запуска алгоритма поиска кратчайших путей SPF после получения новых LSA-сообщений; RIB_{FIB} - время, необходимое для выполнения алгоритма SPF и обновления таблиц маршрутизации RIB/FIB.

4 Время отклика страницы *Http*

$$R \approx \frac{Payload}{C} + AT \cdot RTT + Cs + Cc \quad (4)$$

где:

R - время отклика страницы; ***Payload (Полезная нагрузка)*** - является содержание информации (в байтах), который должен быть доставлен в / из устройства пользователя.

C (Пропускная способность) - является минимальной пропускной способности (в битах в секунду) по всем сетевым каналам связи между пользователем и сервером приложений.

AT – является прикладными взаимодействиями программного обеспечения клиент-сервер (счет поворота) необходим для генерации отклика системы на уровне пользователя или задачу.

RTT - время путешествия туда и обратно (в секундах) между пользователем и прикладным сервером.

Cc (Compute Client) общее время обработки (в секундах), необходимое клиентским устройством.

Cs (Compute Server) общее время обработки (в секундах), требуемое для сервера (ов).

5 Использование канала связи

$$\lambda = \frac{T_{bin} + T_{bout} * 8 * 100}{speed * time}$$

Где : T_{bin} – общее количество входящих байтов; T_{bout} - общее количество исходящих байтов; *speed* – скорость; *time* - время

На рисунке 3.2 показан основной топологии для реализации передачи голоса, видео и HTTP-трафика [57-60].

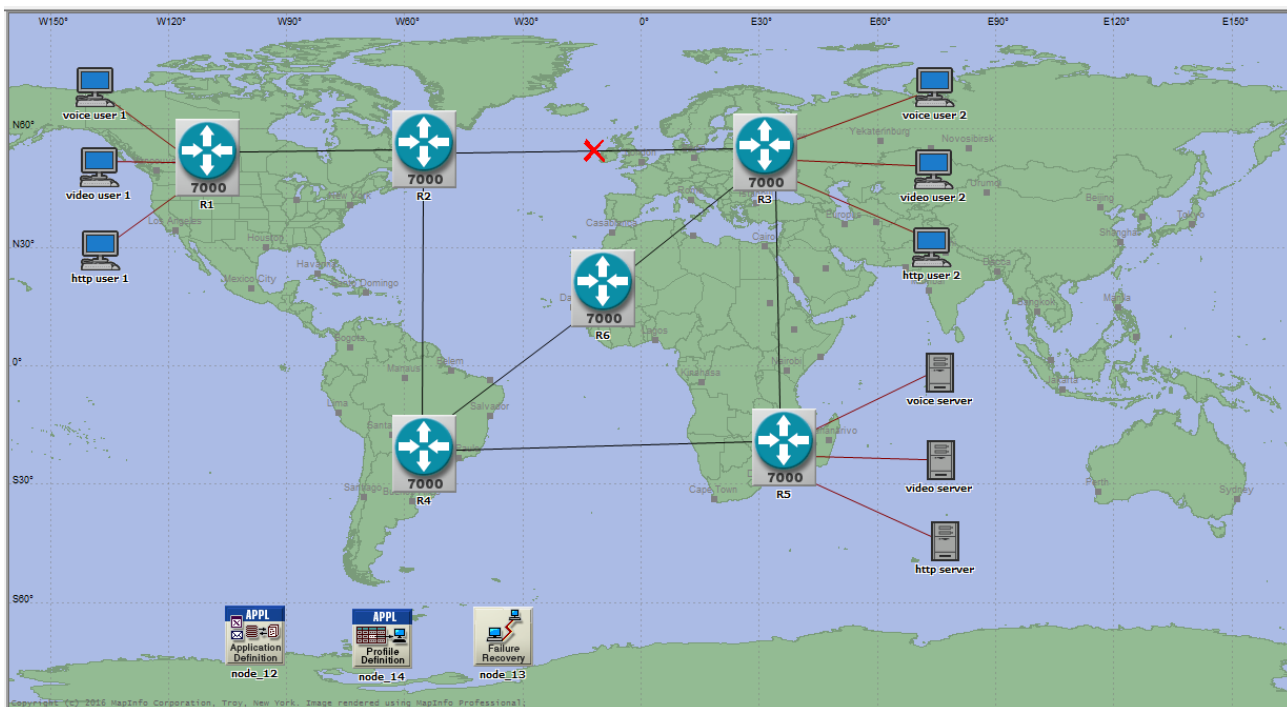


Рисунок 3.2 – Сетевая модель для исследуемых протоколов

Временные параметры обрывов соединений и их восстановление представлены в таблице 3.1.

Таблица 3.1 – Значения срыва и восстановления сетевого соединения между маршрутизаторами R2 и R3

Состояние	Время (sec)
Срыв	240
Восстановление	420
Срыв	520
Восстановление	580
Срыв	610
Восстановление	620
Срыв	625
Восстановление	626

Продолжение таблицы 3.1

Срыв	726
Восстановление	826

3.3 Результаты исследований и анализ симуляции

Время конвергенции сеть IP (в секундах)

Рисунок 3.3 показывает время конвергенции сети для всех трех протоколов маршрутизации. Из рисунка можно наблюдать, что EIGRP занимает наименьшее количество времени сходимости.

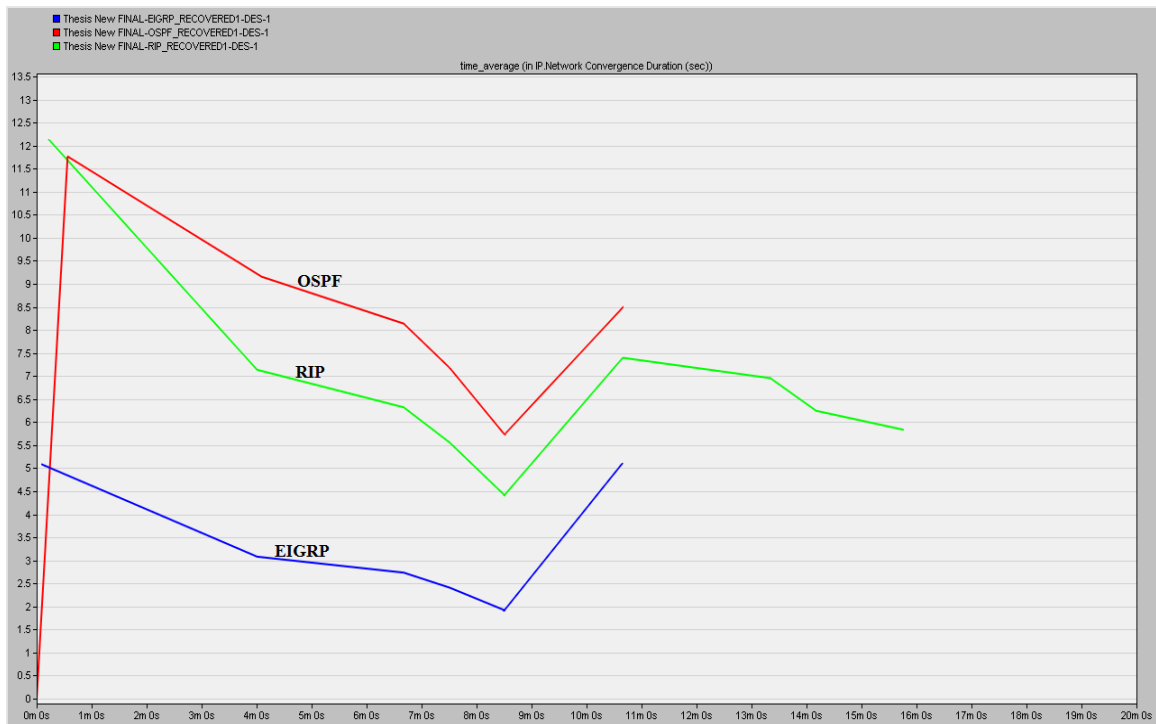


Рисунок 3.3 – Конвергенция сетей для RIP, OSPF и EIGRP.

Потери трафика IP (packet/sec)

На рисунке представлена характеристика потери пакетов в секунду в IP

сети. На рисунке видно, что протокол RIP имеет наибольшее количество отброшенных пакетов по сравнению с OSPF и EIGRP.

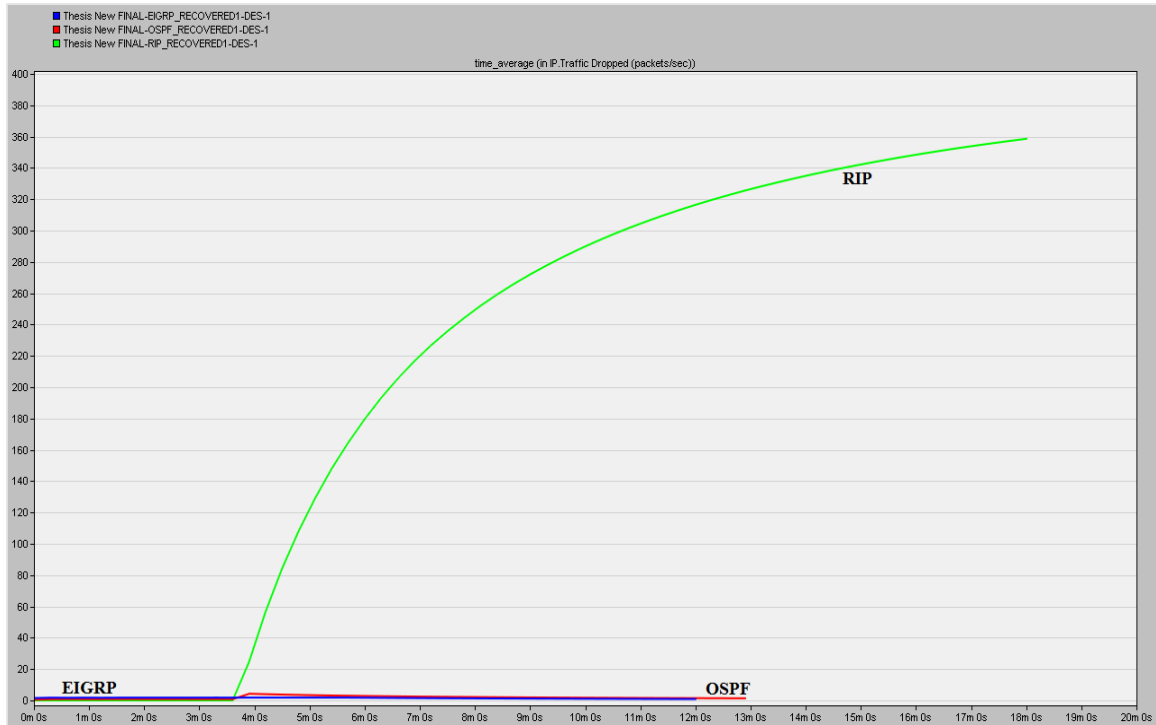


Рисунок 3.4 – Потери траффика IP

Задержка голосового пакета (в секундах)

EIGRP и OSPF показали более устойчивую и лучшую производительность для задержки голосовых пакетов по сравнению с RIP, но лучший результат продемонстрировал протокол OSPF. Это показано на рисунке 3.5 .

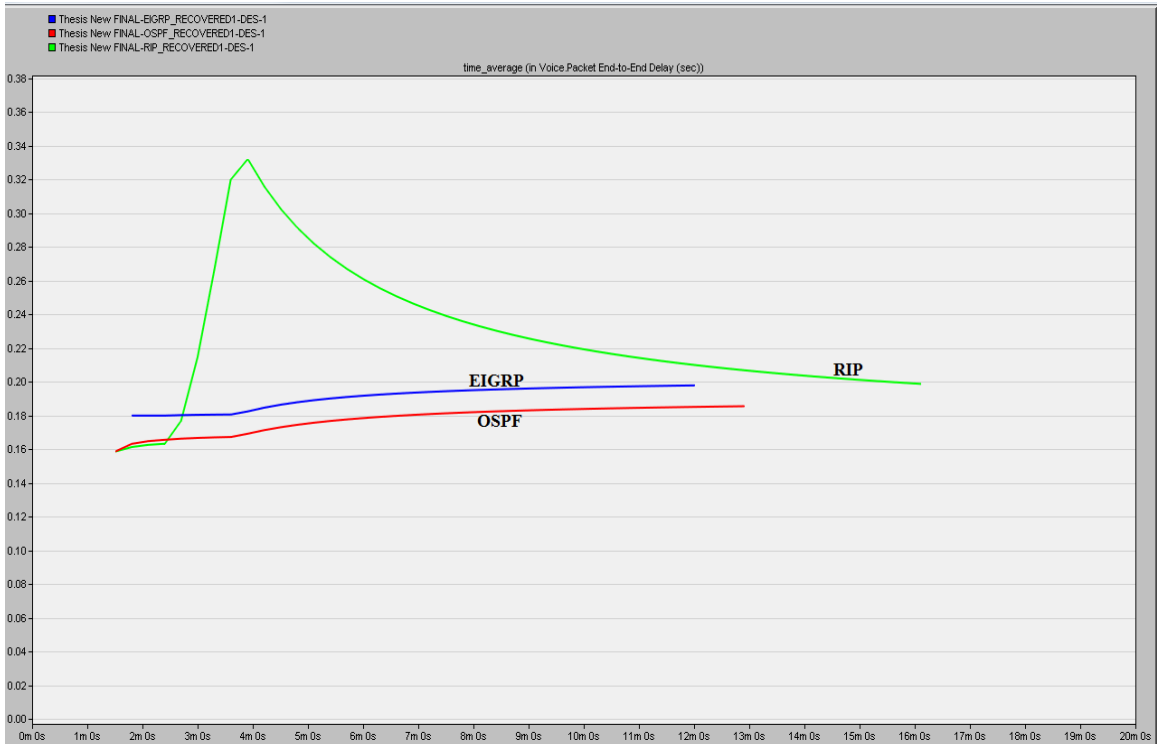


Рисунок 3.5 – задержка голосового пакета

Задержка пакета видеоконференции (в секундах)

EIGRP и OSPF показали лучшую производительность для задержки пакетов видеоконференции по сравнению с RIP. Это показано на рисунке 3.6 .

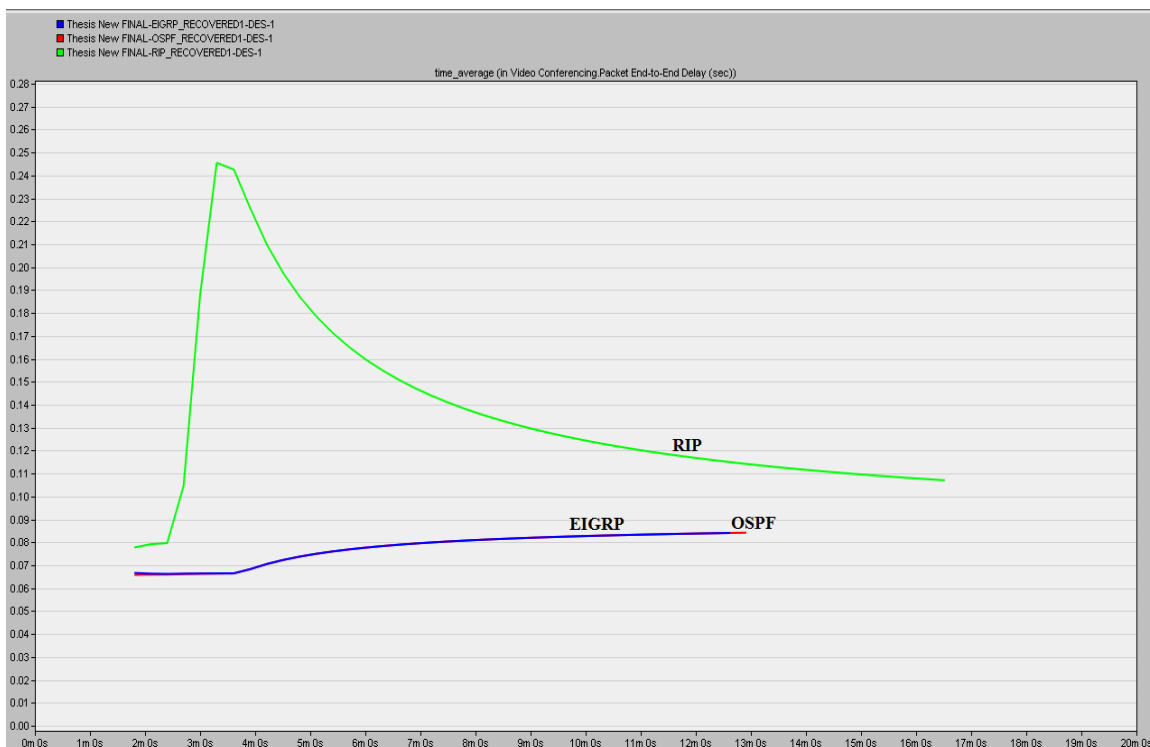


Рисунок 3.6 – задержка пакета видеоконференции

Время отклика страницы HTTP (в секундах)

EIGRP показал наименьшую производительность для просмотра веб-страниц и HTTP трафика. Для HTTP-трафика время отклика сети EIGRP выше по сравнению с OSPF и RIP.

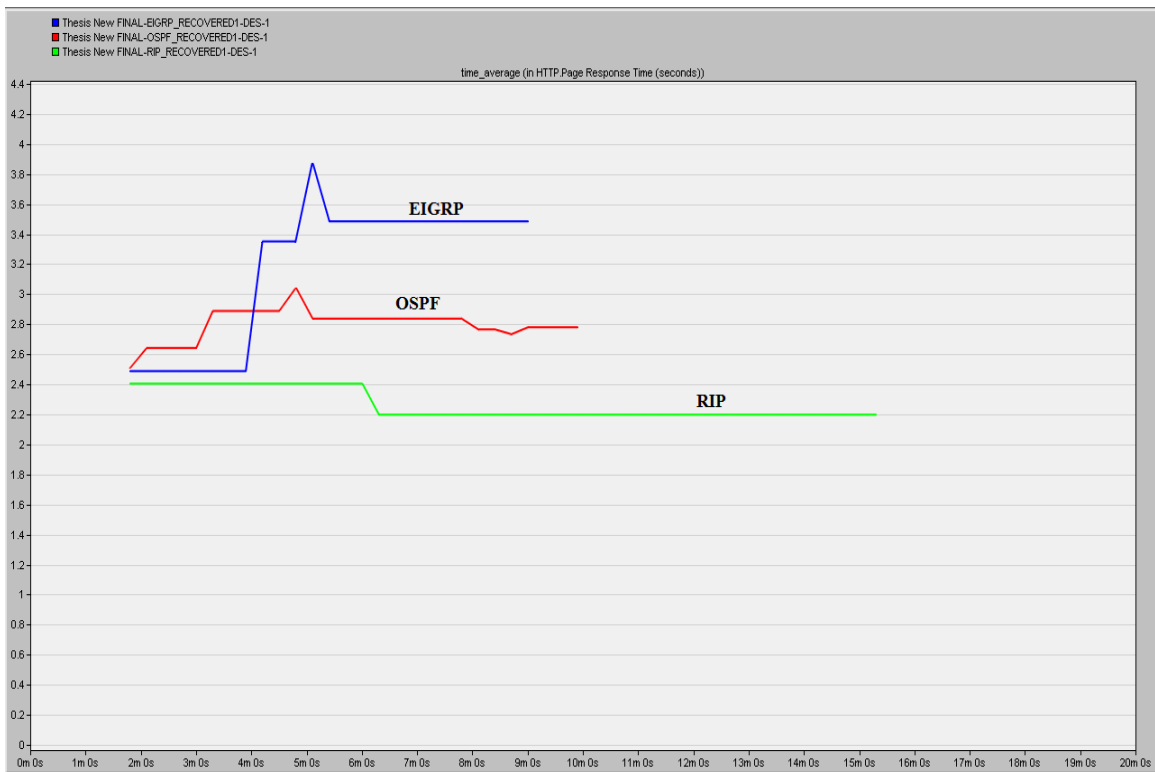


Рисунок 3.7 – Время отклика страницы http

Использование канала связи (%)

EIGRP использует частичные обновления состояния канала. Частичные обновления генерируются только тогда, когда происходит изменение. Из-за этого, EIGRP является достаточно эффективным с точки зрения использования канала связи.

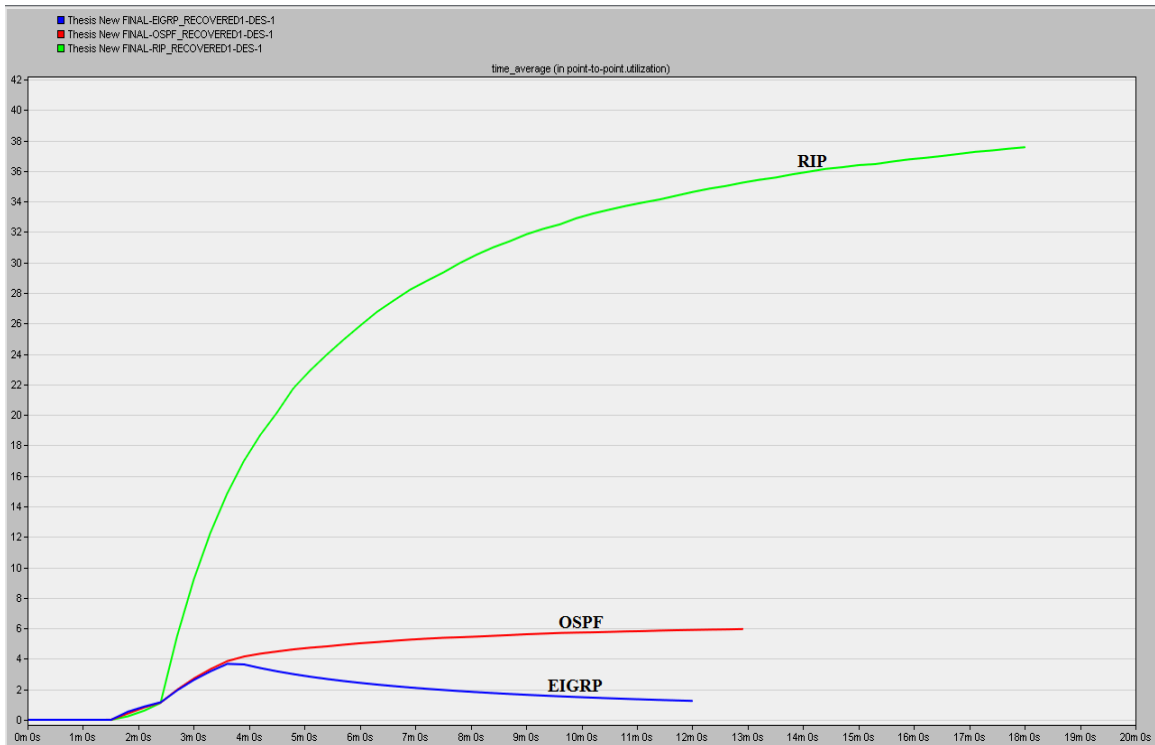


Рисунок 3.8 – Использование канала связи

Задержка в очереди (в секундах)

При исследовании задержки трафика в сети - протокол EIGRP показал наилучшую производительность с минимальными задержками.

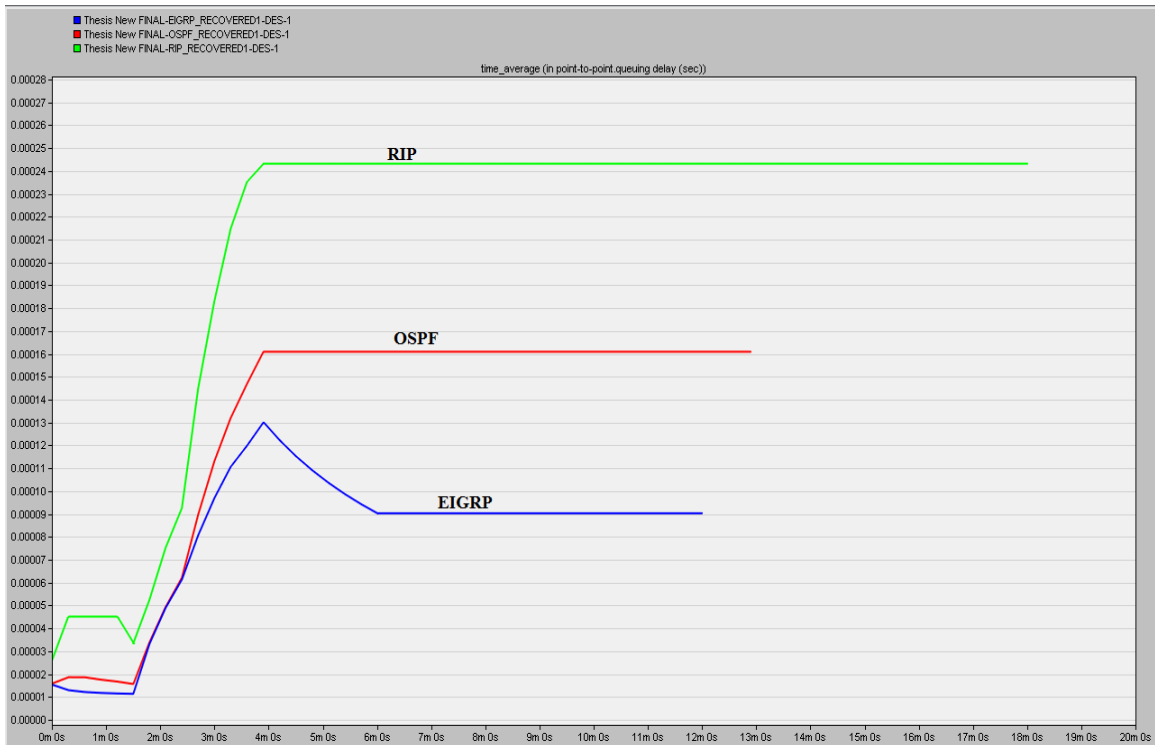


Рисунок 3.9 – Задержка в очереди

Таблица 3.2 – значение полученных от симуляции параметров

Параметры	RIP 900	OSPF 900	EIGRP 900
Время конвергенции сеть IP (sec)	5.8355	8.4854	5.1124
Потери трафика IP (packet/sec)	375.25	1.3547	0.8861
Задержка голосового пакета (sec)	0.1982	0.1855	0.1979

Продолжение таблицы 3.2

Задержка пакета видеоконференции (sec)	0.1071	0.0842	0.0841
Время отклика страницы Http (sec)	1.9779	2.1869	2.7526
Задержка в очереди (sec)	0.00024	0.000160	0.000090
Использование канала связи(%)	37.560	5.951	1.239

ЗАКЛЮЧЕНИЕ

В работе представлены результаты моделирования телекоммуникационной сети с точки зрения оценки её производительности по следующим параметрам: время конвергенции, потери пакетов, задержка голосового/видео трафика, задержка в очереди, использование канала связи и время отклика страницы HTTP. В компьютерной модели имитировался сценарий обрыва и восстановления соединения между транспортными маршрутизаторами при использовании исследуемых протоколов маршрутизации RIP, OSPF и EIGRP при передаче голоса, видео ряда и HTTP-трафика.

Из полученных при моделировании результатов можно сделать вывод, что протокол EIGRP имеет лучшую производительность по сравнению с другими протоколами по ряду обозначенных выше критериев.

Конвергенция в протоколе EIGRP как показывает моделирование быстрее, так как он использует алгоритм, называемый двойной алгоритм обновления (DUAL), который использует особенности отслеживания состояния канала (link-state technology) и расстояние вектора алгоритма. Также наблюдалось, что RIP имеет наибольшее количество отброшенных пакетов и максимальную задержку пакетов в сети по сравнению с OSPF и EIGRP. При оценке эффективности использования канала связи - EIGRP показал наибольшую производительность по сравнению с протоколами RIP и OSPF.

Результаты моделирования, представленные в этой работе могут быть полезны при проектировании больших сетей, так как выбор правильного протокола маршрутизации позволяет обеспечивать хорошую производительность и стабильность работы сети в целом при передаче чувствительного к задержкам трафика через нестабильные линии связи.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Хабрейкен Дж., Хайден М. Сетевые технологии. М.: «Вильямс», 2007. – 138 с.
2. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. СПб.: ПИТЕР, 2008. – 604 с.
3. Томас М. Структура и реализация сетей на основе протокола OSPF. CiscoPress, Вильямс, 2004. – 783 с.
4. ARSALAN I.,SAMEER L.A. Performance Evaluation of Real Time Applications for RIP, OSPF and EIGRP for flapping links using OPNET Modeler.
5. Макаренко С. И. Время сходимости протоколов маршрутизации при отказах в сети.
6. Поповский В. В., Лемешко А. В., Мельникова Л. И., Андрушко Д. В. Обзор и сравнительный анализ основных моделей и алгоритмов многопутевой маршрутизации в мультисервисных телекоммуникационных сетях // Прикладная радиоэлектроника. 2005. Т. 4. No 4. С. 372-382. – URL: http://alem.ucoz.ua/_ld/0/10_Lemeshko_PRE_20.pdf (дата доступа 01.05.2015).
7. Thorenoor, S.G.”Dynamic Routing Protocol Implementation Decision between EIGRP, OSPF and RIP Based on Technical Background Using OPNET Modeler” (Wipro, Bangalore, India) Source: Proceedings of the 2010 Second International Conference on Computer and Network Technology (ICCNT 2010), p191-5, 2010.
8. Поповский В. В., Волотка В. С. Методы анализа динамических структур телекоммуникационных систем // Восточно-Европейский журнал передовых технологий. 2013. No 5/2 (65). С. 18-22.
9. Попков В. К., Блукке В. П., Дворкин А. Б. Модели анализа устойчивости и живучести информационных сетей // Проблемы информатики.

2009. No 4. С. 63-78.

10. Литвинов К. А., Пасечников И. И. Подходы к решению задачи маршрутизации в современных телекоммуникационных системах // Вестник Тамбовского университета. Серия: Естественные и технические науки. 2013. Т. 18. No 1. С. 64-69.

11. Kalyan, G., P., S., Prasad, D., V., V.: Optimal selection of Dynamic Routing Protocol with real time case studies. 2012 International Conference on Recent Advances in Computing and Software Systems [online]. IEEE, 2012, s. 219-223 [cit. 2014-01-13]. DOI: 10.1109/RACSS.2012.6212727

12. Hendrick, C. (1988). Routing Information Protocol - RFC 1058, 133. URL: <http://tools.ietf.org/rfc/rfc1058.txt>.

13. Сорокин А. А., Дмитриев В. Н. Описание систем связи с динамической топологией сети при помощи модели «мерцающего» графа // Вестник АГТУ. Серия: Управление, вычислительная техника и информатика. 2009. No 2. С. 134-139.

14. Сорокин А. А., Дмитриев В. Н., Чан Куок Тоан, Резников П. С. Оценка результатов использования протокола RIP в системах связи с динамической топологией сети методом имитационного моделирования // Вестник АГТУ. Серия: Управление, вычислительная техника и информатика. 2014. No 4. С. 85-93.

15. Malkin, G. (1998). RIP Version 2 - RFC 2453, 1–40. URL: <http://tools.ietf.org/rfc/rfc2453.txt>.

16. Fitigau, I.; Todorean, G., "Network performance evaluation for RIP, OSPF and EIGRP routing protocols," International Conference on Electronics, Computers and Artificial Intelligence (ECAI), 2013 , vol. 1, no. 1, pp.1-4, 27-29 June 2013.

17. Мейкшан В. И. Анализ влияния отказов оборудования на

функционирование мультисервисной сети с адаптивной маршрутизацией // Доклады академии наук высшей школы Российской Федерации. Технические науки. 2010. No 2 (15). С. 69-80.

18. Lan, L., Li, L., & Jianya, C. (2012). A Multipath Routing Algorithm Based on OSPF Routing Protocol. 2012 Eighth International Conference on Semantics, Knowledge and Grids, 269–272. doi:10.1109/SKG.2012.7.

19. Szigeti, T., Hattingh, C. End-to-End QoS Network Design: Quality of Service in LANs, WANs, and VPNs. Cisco Press, 2004.

20. Park, I. K. QoS in Packet Networks. Springer, 2005.

21. Velte, J. T. Cisco: A Beginner's Guide. McGraw-Hill, 2001.

22. Flannagan, M. E. Administering Cisco QoS for IP Networks. Syngress Publishing, 2001.

23. Blake, S., Black, D., Carlson, M., Davies, E., Wang, Z., Weiss, W.: An Architecture for Differentiated Service, RFC2475, 1998.

24. Chandra W. "Performance Analysis of Dynamic Routing Protocol EIGRP and OSPF in IPv4 and IPv6 Network," 2011 vol. 36, no. 1, pp. 76-84, March 2011.

25. Kisten, S. Ping-Tsai C., "Analysis and experimentation on dynamic routing protocols: IGRP and OSPF," in Proceedings of the International Conference on Internet Computing, pp. 591-3 vol.2, June 2003.

26. Baranski J., Crocker M., Lazarou G. "Dynamic routing protocol performance in a faulttolerant Ethernet-based IP network, " in Proceedings of the International Conference on Systemics, Cybernetics and Informatics, pp. 1-5 Vol. 8, Sept 2004.

27. Yee, J.R., "On the International routing protocol enhanced interior gateway routing protocols: is it optimal?" in International Transactions in Operational Research, v 13, n 3, pp. 177-94, May 2006.

28. Al-Saud, K.A. Tahir, H.M., El-Zoghabi, A.A., Saleh, M.” Performance evaluation of secured versus non-secured EIGRP routing protocol,” in Proceedings of the International Conference on Security & Management (SAM 2008), pp. 292-7, July 2008.
29. Dimitri B., Robert G., “Data Networks – 2nd ed”. Prentice Hall, New Jersey, ISBN 0-3-200916-1.
30. Talal M. J., “Simulation-Based Routing Protocols Analysis ” in Ph. D thesis, The Faculty of Electrical Engineering at Georgia Institute of Technology, 2007.
31. Xianhui C., Lee J. C., “VoIP Performance over Different Interior Gateway Protocols”, in Proceedings of the International Journal of Communication Networks and Information Security (IJCNIS), Vol. 1, No. 1, April 2009.
32. Nohl, A.R, Molnar, “The convergence of the OSPF routing protocol” in Proceedings of the International Conference on Systemics, Cybernetics and Informatics, v 47, n 1-2, p 89-100, May 2002.
33. B. Fortz, J. Rexford, M. Thorup., “Traffic engineering with traditional IP routing protocols,” in IEEE Communications Magazine, pp. 118-124, vol. 40, Oct. 2002.
34. K. Salah, P. Calyam, and M.I. Buhari, “Assessing readiness of IP networks to support desktop videoconferencing using OPNET,” International Journal of Network and Computer Applications, vol. 31, issue. 4, pp. 921-943, November, 2008.
35. Md N. I., Md. Ahsan U.A., "Simulation Based EIGRP over OSPF Performance Analysis", MSc. Thesis, Dept. of Elect. Eng., Blekinge Institute of Technology, 2010.
36. Ljiljana T., Final Project OSPF, EIGRP, and RIP performance analysis based on OPNET.

37. Usuari, Comparative analysis of the routing protocols RIPv2, OSPFv2 and Integrated IS-IS (Opnet & La Salle Reports).
38. Marchese, M. QoS Over Heterogeneous Networks. Wiley Publishing, 2007. ISBN 9780470017524.
39. Sifta, R.; Munster, P.; Krajsa, O.; Filka, M. Simulation of bidirectional traffic in WDM- PON networks. *Przeglad Elektrotechniczny*, 2014, roč. 90, č. 1, s. 95-100. ISSN: 0033- 2097.
40. Имитационное моделирование компьютерных сетей // Ресурс. URL:<http://referat.resurs.kz/ref/imitatsionnoe-modelirovanie-kompyuternih-se...>
41. J. Slay, M. Simon., "Voice over IP forensics, " in Proceedings of the 1st international conference on Forensic Applications and Techniques in Telecommunications, Information, and Multimedia, and Workshop, Vol.10, issue 3, pp.
42. Wu, Bing, "Simulation Based Performance Analyses on RIPv2, EIGRP, and OSPF Using OPNET", Math and Computer Science Working Papers. Paper 11.
43. ZHENG LU H.Y. Unlocking the Power of OPNET Modeler .
44. Moy J. T. OSPF: Anatomy of an Internet Routing Protocol. Addison-Wesley Professional, 1998. 338 p.
45. Goyal M., Xie W., Hosseini S. H., Vairavan K., Rohm D. Improving OSPF Dynamics on a Broadcast LAN // Simulation. 2006. vol. 82. No 2. pp. 107-129. doi: 10.1177/0037549706065924
46. Amir S., Biswajit N. Improving Network Convergence Time and Network Stability of an OSPF-Routed IP Network // Lecture Notes in Computer Science. 2005. Vol. 3462. pp. 469-485. doi: 10.1007/11422778_38
47. GoyalM., XieW., SoperiM., HosseiniS.H., VairavanK. Scheduling routing table calculations to achieve fast convergence in OSPF protocol // Proc. IEEE BROADNETS 2007. 2007. pp. 863–872. doi: 10.1109/BROADNETS.2007.4550524

48. Bidirectional Forwarding Detection for OSPF. Cisco, 2005. 18 p. URL:https://www.cisco.com/en/US/technologies/tk648/tk365/tk480/technologies_white_paper0900aecd80244005.pdf (дата доступа 01.05.2015).
49. Kompella K., Rekhter Y. RFC 4203. OSPF extensions in support of generalized multi-protocol label switching (GMPLS) // Internet Engineering Task Force, Request for Comments (Standards Track), 2005. URL: <https://www.ietf.org/rfc/rfc4203.txt> (дата доступа 01.05.2015)
50. Shand M., Bryant S., Previdi S., IP fast reroute using not-via addresses // Network Working Group, Internet-Draft (Experimental), 2010. URL: <https://tools.ietf.org/html/draft-ietf-rtgwg-ipfrr-notvia-addresses-06> (дата доступа 01.05.2015).
51. Dilber M. N., Raza A. Analysis of successive Link Failures effect on RIP and OSPF Convergence time delay // International Journal of Advances in Science and Technology. 2014. pp. 42-48. URL: <http://sciencepublication.org/documents/sp/7.pdf> (дата доступа 01.05.2015).
52. Zhao D., Hu X., Wu C. A Study on the Impact of Multiple Failures on OSPF Convergence // International Journal of Hybrid Information Technology. 2013. vol. 6. No 3. pp. 75-74. URL: http://www.sersc.org/journals/IJHIT/vol6_no3_2013/7.pdf (дата доступа 01.05.2015).
53. Sankar D., Lancaster D. Routing Protocol Convergence Comparison using Simulation and Real Equipment // Advances in Communications, Computing, Networks and Security. 2013. Vol. 10. pp. 186-194.
54. Ogier R., Spagnolo P. RFC 5614. Mobile Ad-Hoc network MANET extension of OSPF using connected dominating set CDS flooding // Internet Engineering Task Force, Request for Comments (Experimental), 2009.
55. Zaballos A., Seguí C. Analysis and simulation of IGP routing protocols // University Ramon Llull (La Salle Engineering), Barcelona (Spain). 2006. URL:

<http://users.salleurl.edu/~zaballos/opnet/Trame.pdf> (дата доступа 01.05.2015).

56. Макаренко С. И., Михайлов Р. Л., Новиков Е. А. Исследование канальных и сетевых параметров канала связи в условиях динамически изменяющейся сигнально–помеховой обстановки // Журнал радиоэлектроники. 2014. No 10. URL: <http://jre.cplire.ru/jre/oct14/3/text.pdf> (дата доступа 01.03.2015)

57. Антонова А.А. Оценка эффективности протоколов динамической маршрутизации при передаче потокового видео // Автоматизация и управление в технических системах. 2013. No4.2. URL: <http://auts.esrae.ru/7-151> (дата обращения: 02.05.2015). doi: 10.12731/2306-1561-2013-4-36

58. Villamizar C. Convergence and restoration techniques for ISP interior routing // NANOG [Электронный ресурс], 2002. URL: <http://www.nanog.org/mtg-0206/ppt/curtis.pdf> (дата доступа 01.05.2015).

59. LabovitzC., AhujaA., BoseA., JahanianF. Delayed Internet Routing Convergence // IEEE/ACM Transactions on Networking (TON). 2001. Vol. 9. No 3. pp. 293-306.

60. Pun H. Convergence Behavior of RIP and OSPF Network Protocols. Ph.D. thesis. B.A.Sc., University of British Columbia. 2001. 59p. URL: <http://www2.ensc.sfu.ca/~ljilja/cnl/pdf/hubert.pdf> (дата обращения: 02.05.2015).