Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего профессионального образования
«Южно-Уральский государственный университет»
(Национальный исследовательский университет)
«Высшая школа электроники и компьютерных наук»
Кафедра «Инфокоммуникационные технологии»

ДОПУСТИТЬ К ЗАЩИТЕ
Руководитель направления
Даровских С.Н.
«____» _____20__ г.

Рецензент
Рукавишников А.В.
«____» _____20__ г.

Моделирование и анализ работы сетей связи с поддержкой IP протоколов 4й и 6й версий

*Направление*11.04.02 **«Инфокоммуникационные технологии и системы связи»**
*магистерская программа***«Системы мобильной связи»**
ЮУрГУ – М 11.04.02.2020.576.00 ПЗ ВКР

Научный руководитель
Новиков В.В._____
«____» _____2020 г.

Магистрант:
студент группы
Боженков С.В. _____
«____» _____2020 г.

Нормоконтролер,
Спицына В.Д._____
«____» _____2020 г.

Челябинск 2020

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего профессионального образования
«Южно-Уральский государственный университет»
(Национальный исследовательский университет)
«Высшая школа электроники и компьютерных наук»
Кафедра «Инфокоммуникационные технологии»

Высшая школа электроники и компьютерных наук
Кафедра «Инфокоммуникационных технологий»

Направление «**11.04.02** Инфокоммуникационные технологии и системы связи»

УТВЕРЖДАЮ

Зав. кафедрой ИКТ

_____ С.Н. Даровских

“____”_____2018г.

ЗАДАНИЕ

по выпускной квалификационной работе магистра

Боженкова Сергея Владимировича

Группа КЭ–223

1 Тема работы (проекта): «Моделирование и анализ работы сетей связи с поддержкой IP протоколов 4й и 6й версий»

2 Срок сдачи студентом законченной работы (проекта):“____”_____2020 г.

3 Исходные данные к работе (проекту)

3.1 Цель работы: анализ и оценка быстродействия и производительности сетей связи, работающих с помощью межсетевых протоколов IPv4 и IPv6, с использованием программы для моделирования работы сети RiverbedModeler.

3.2 Используемые методы

3.2.1 Разработка моделей сети на основе межсетевого протокола IPv4 в среде моделирования сети RiverbedModeler

3.2.2 Разработка моделей сети на основе межсетевого протокола IPv6 в среде моделирования сети RiverbedModeler

3.2.3 Разработка модели сети с использованием виртуальных каналов VLANs, на основе межсетевых протоколов IPv4 иIPv6в среде моделирования сети RiverbedModeler

3.2.4 Проведение сравнительного анализа работы сетей и формирование выводов

4 Содержание пояснительной записки

4.1 Реферат

4.2 Введение

4.3 Постановка задачи

4.4 Технологии, применяемые в работе

4.5 Схема организации сети связи в жилом микрорайоне

4.6 Исследование качества работы сети жилого района с использованием различных протоколов.

4.7 Заключение

4.8 Список использованных источников

5 Перечень графического материала

5.1 Плакат 1

5.2 Плакат 2

5.3 Плакат 3

5.4 Плакат 4

5.5 Плакат 5

5.6 Плакат 6

6 Календарный план работы

№ п/п	Наименование этапов выпускной квалификационной работы	Сроки выполнения этапов работы (начало – конец)	Отметка о выполнении руководителя
1	Анализ технического задания		
	Теоретические основы		
	Анализ компонентов системы		
	Практические эксперименты		
	Заключение		
2	Контрольный срок		
3	Заключительные разделы		
4	Написание и оформление ТЗ		
5	Графическая часть		
6	Защита проекта		

7 Дата выдачи задания: _____

Руководитель: _____ / Новиков В.В./

Задание принял к исполнению :_____/ Боженков С.В./

РЕФЕРАТ

БоженковС.В. Моделирование и анализ работы сетей связи с поддержкой IP протоколов 4й и 6й версий Челябинск: ЮУрГУ, ВШЭКН, 2020, илл.38, с.74, список использованных источников - 17 наименований, 6 плакатов формата А1

В данной выпускной квалификационной работе был проведен анализ и сравнение работы моделей сетей, работающих с использованием межсетевых протоколов четвертой и шестой версий. В первой главе дына некоторая теоретическая информация о IPv4 и IPv6, а так же о технологии виртуальных локальных сетей. Во второй главе описан пакет программ RiverbedModeler, использовавшийся для моделирования и сами модели. В третьей главе проводился непосредственной анализ и представлены сравнительные характеристики работы моделей сетей с использованием различных протоколов.

В работе кратко описана работа с программным обеспечением для конфигурации сетей и приведены сравнительные графики для оценки эффективности использования различных протоколов. На основании результатов работы сделаны выводы и некоторые рекомендации по использованию протоколов во внутренних сетях.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ 6
1Технологии, применяемые в работе 8
1.1 Межсетевой протокол четвертой версии 8
1.1.1 Общие сведения……..……..…...8
1.1.2 Состав пакета……..……..…..11
1.1.3 Разделение пакета.....13
1.1.4 Деление адресов на классы.....14
1.1.5 Маски при адресации.....16
1.1.6 Специальные зарезервированные адреса.....19
1.1.7 IP-адреса, используемые в локальных сетях.....22
1.2ПротоколИнтернета шестой версии.....22
1.2.1 Особенности протокола шестой версии……...…24
1.2.2 Виды адресов……..26
1.3 Виртуальныесети(VLAN - VirtualLocalAreaNetwork)……30
1.3.1 Общее описание виртуальных сетей……..……30
1.3.3 Методы организации виртуальных сетей……...…33
1.3.3.1 Организация виртуально сети с помощьюпротоколов…….33
1.3.3.2 Организация виртуальной сети с помощью портов……....34
1.3.3.3 Организация виртуальной сети с помощью MAC-адресов……...34
2. Моделирование инфокоммуникационной сети……..36
2.1 Описание сети……..36
2.2 Riverbed Modeler……..39
3 Исследование качества работы сетей связи с использованием различных протоколов……..43
3.1 Сравнение работы протоколов четвертой и шестой версий…….....43
3.2 Исследование сети, разделенной на виртуальные каналы.....63
ЗАКЛЮЧЕНИЕ.....71
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ.....73

ВВЕДЕНИЕ

Широкое распространение и развитие инфокоммуникационных технологий и сетей обусловило образование в почти всех областях деятельности людей информационных сетей, способных поддерживать большой объем услуг. **Вследствие** чего сегодня информационные сети учреждений, а также городские сети, поддерживающие различные сервисы, способны достичь немалых размеров, содержать большое количество услуг и быть хорошо масштабируемы. Данная сетевая организация не может быть реализована без группировки в отдельные сетевые кластеры активных устройств сети, что в свой черед ведет к созданию большой численности служебного сетевого трафика, создающего лишние задержки при передаче информационных пакетов, более длительному пребыванию пакетов в сети и сложности управления сетью. Нередко старание организаций, отвечающих за сеть связи, увеличить эффективность работы сети с различными сервисами ограничивается к улучшению следующих ее параметров: скорости работы активного оборудования сети, ее пропускная способность, нагрузка на серверы, время прохождения пакета. Сегодня эта цель достигается благодаря внедрению новых технологий, например использование VLAN (локальных виртуальных сетей) и протокола IPv6, дающих прирост качество работы сети. Но, не все современные методы могут дать достаточно хороший результат в различных ситуациях. Следовательно, перед тем как решить использовать какую либо технологию при построении инфокоммуникационной сети в определенном случае используют имитационное моделирование, с помощью которого на предварительном этапе проектирования определить необходимую мощность и параметры будущей сети.

В этой работе будет проведено моделирование и анализ работы сетей связи с поддержкой IP протоколов 4й и 6й версий с использованием имитационного моделирования по параметрам: время прохождения сети пакетом, нагрузке на активное оборудование, его пропускной способности.

Для достижения назначенной цели требуется найти решение поставленных задач:

- проанализировать имеющиеся в отрасли средства для моделирования и анализа инфокоммуникационных сетей.
- оценить параметры сети с различными сервисами посредством моделирования.
- провести исследование параметров и характеристики работы сети при разных конфигурациях и предоставляемых сетью типов услуг с использованием VLAN.
- провести исследование параметров и характеристики работы сети при разных конфигурациях и предоставляемых сетью типов услуг с использованием IPv6.

Выпускная квалификационная работа магистра состоит из введения, трех глав, заключения, списка использованной литературы. Текст работы изложен на 74 листах машинописного текста, включающий 38 рисунков, 3 таблицы и списка литературы из 17 названий.

1 Технологии, применяемые в работе

1.1 Межсетевой протокол четвертой версии

1.1.1 Общие сведения

Протоколы, соответствующие 3-ему уровню модели OSI, показывают то, как пакеты идут от создавшего их устройства к устройству, которое должно получить их. На данный момент единственным протоколом 3-его уровня, который широко используется, служит лишь стек протоколов TCP/IP, а в основном это межсетевой InternetProtocol (IP). Неотделимой частью данного протокола служит IP-адрес. Адреса IPv4 (InternetProtocolversion 4 – протокол Интернета 4-й версии) – самый используемый вид адресов, служит в модели OSI на сетевом уровне для транспортировки пакетов данных между различными сетями. Адреса IPv4 содержат 4 байта, например 192.168.100.001.

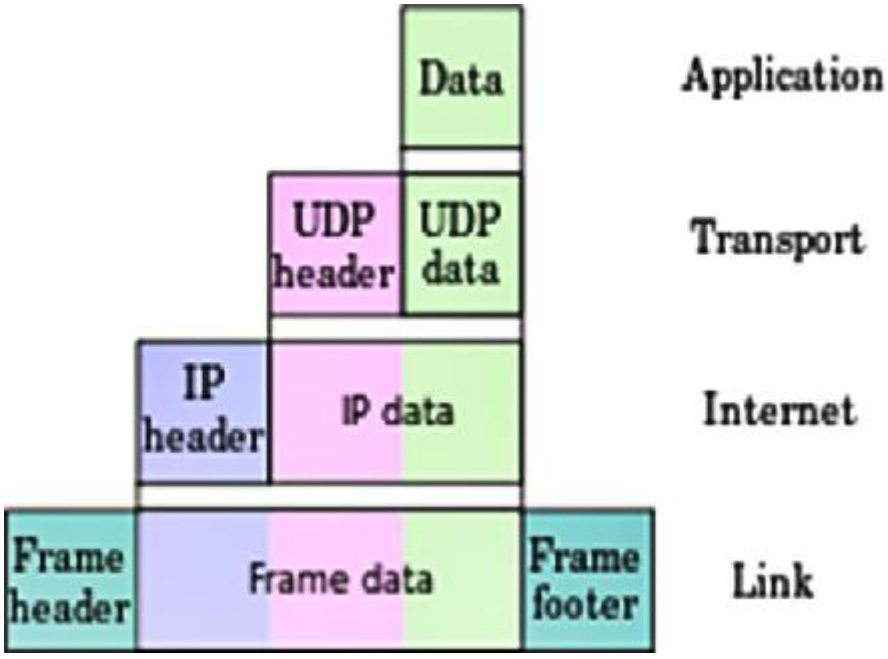

Рисунок 1.1 – Вид пакета и его частей заголовка
на каждом уровне модели OSI

Присваивание IP-адреса хостам происходит двумя способами:

– задается вручную сетевым администратором в процессе настройки информационной сети;
– присваивается автоматически, благодаря задействованию некоторых специализированных протоколов динамической настройки, например, DHCP (DynamicHostConfigurationProtocol).

Протокол интернета четвертой версии был создан в сентябре 1981 года. Он является честью протокола IP. Его предназначение заключается в передаче информационных пакетов непосредственно устройству-получателю, для чего каждому сетевому устройству присваивается адрес.

Главное назначение протокола четвертой версии- реализация передачи дейтаграмм (блоков данных) от отправителя к получателю, каждый из которых является устройством с однозначно определяемыми адресами строго фиксированного размера (IP-адресами). Вдобавок протокол этой версии способен, если необходимо, выполнять деление пакета на части и отправление их дальше через другие сети, размер пакета которых меньше.

У протокола IPприсутствует ненадежность и основной недостаток в том, что не происходит подтверждение доставки пакетов при передаче, не контролируется цельность полученных пакетов данных (например, используя контрольной суммы) и не производится опрос узла-назначения о его способности принять данные.

Каждый блок данных посылается и расшифровывается протоколом IP обособленно, без учета других блоков данных, переданных раньше или позже.

Отправляющее устройство не следит за последующими действиями с отправленным пакетом, после отправки протоколом IP. Если пакет, не достигший целевого устройства, по какой либо причине не может быть передан дальше по сети, он уничтожается. Узел, уничтоживший пакет, способен сообщить о сбое и его причине устройству-отправители (например, используя пакет ICMP). Функция

обеспечения гарантированного прохождения пакета лежит на протоколах более высокого уровня модели OSI (транспортного), у которого есть для этого особые возможности (протокол TCP).

Общеизвестно, что на сетевом уровне модели OSI производят работу маршрутизаторы. Следовательно, наиболее важной задачей протокола интернетаявляется осуществление организации маршрутизирования пакетов данных, то есть нахождение лучшего пути их прохождения (используя алгоритмы маршрутизации) от устройства-отправителя к устройтву-получателю с определенным IP-адресом.

Алгоритм приема пакета данных из сети на любом узле сети с использованием протокола IP выглядит так:

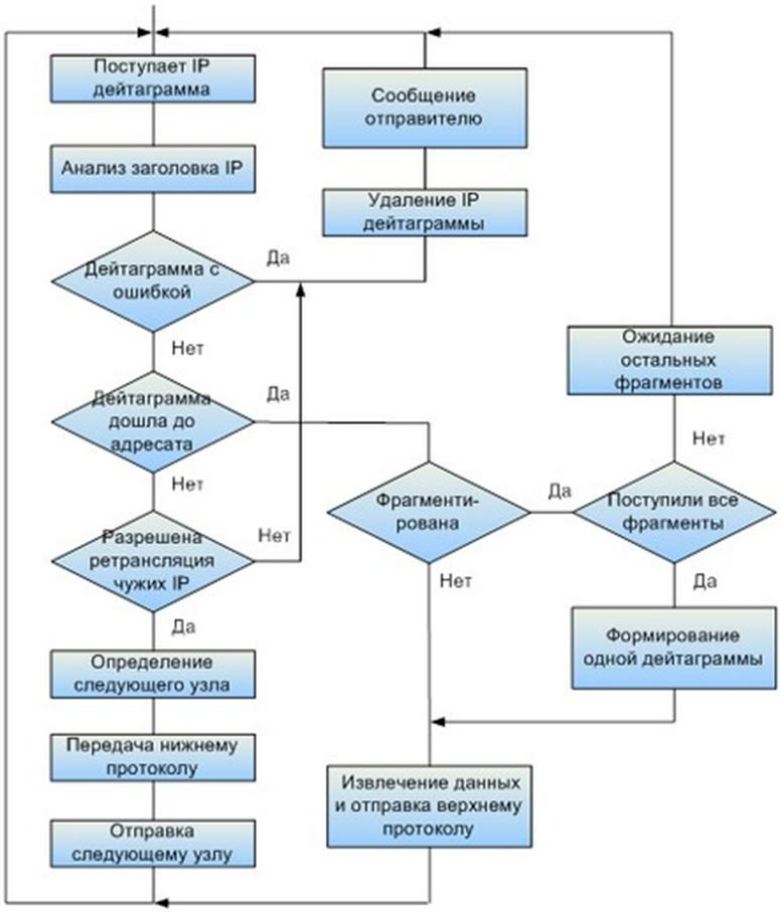

Рисунок 1.2 – Алгоритм работы протокола IPv4

1.1.2 Состав пакета

Состав пакетов версии 4 представлена на рисунке 4:

Октет	0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31				
0	Версия	Размер заголовка	Дифференци-рование услуг	УП	Длина пакета
4	Идентификатор			Флаги	Смещение фрагмента
8	Время жизни		Протокол	Контрольная сумма заголовка	
12	IP-адрес отправителя				
16	IP-адрес получателя				
20	Параметры от 0-я до 10-и 32-х битовых слов				
20 или 24+	Данные				

Рисунок 1.3 – Состав пакета четвертой версии

Поле Версия — у протокола IPv4 значение этого поля -4.

Поле Размер заголовка (InternetHeaderLength) — количество dword (32-х битных слов) в заголовке IP-пакета.Здесьпоказываетсяначалоблокаданных. Это поле может принимать значение от 5-ти (т.е. 5 32-х битных слов – 20 байт), до 15-ти (60 байтов).

Поле Точка кода дифференцированных услуг (DifferentiatedServicesCodePoint) — эти 6бит служатдляуказанияклассаобслуживания.

Поле ECN (Указательперегрузки -ExplicitCongestionNotification)— служит для предупреждает о превышении нагрузки на сеть без потери пакетов. Необязателен.

Поле Длина пакета — количество октетов, составляющих пакет (данные и заголовок). Согласно этому полю пакет может принимать размер от 20 до 65535 октетов.

Поле Идентификатор — присваивается устройством-отправителем и служит для задания правильной последовательности частей пакета при сборке. Если пакет разделен на части, у всех они имеютодинаковыйидентификатор.

Поле Биты флагов (3).Бит номер 1всегдапринимает значениеноль,бит номер 2 показывает можно ли фрагментировать пакет, бит номер 3 показывает, является ли этот пакетпоследним в череде отправленныхпакетов.

Поле Смещение фрагмента — это поле из одного битапоказывает какое место занимает фрагмент в общем потоке данных. Эта величина задается количеством блоков по 8 байт, следовательно, для перевода вбайты ее требуется умножить на 8.

Поле Время жизни — количество роутеров, которые требуется миновать этому пакету. При прохождении каждого маршрутизатора это число декрементируется. Когда цифра в этом поле становится равной нулю, то данные удаляются и устройству-отправителю пакета посылается сообщение об этом событии.

Поле Протокол — указатель на протокол следующего уровня показывает, данные какого протокола находятся в пакете (К примеру ICMP или TCP).

Контрольная сумма заголовка.

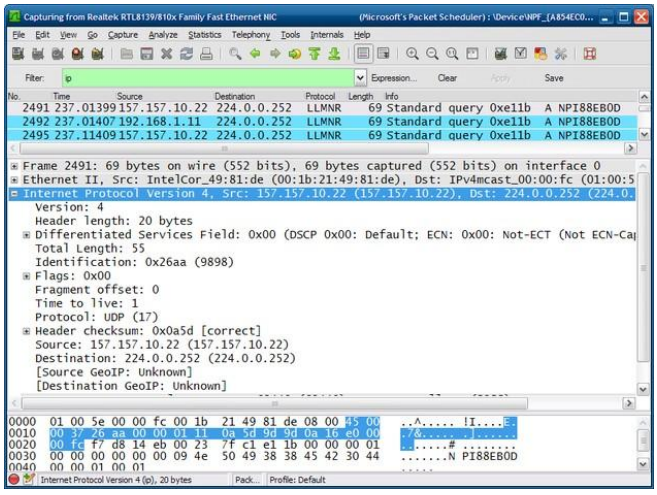

Рисунок 1.4 – Пакет IPv4, перехваченный с помощью сниффера

1.1.3 Разделение пакета

То, что протокол IPспособен фрагментировать пакеты – важная особенность, выгодно отличающая его от сетевого протокола IPX. Однако, при прохождении пакетов через различные инфокоммуникационные сети вариативных типов возникает проблема в том, что у них разные размеры полей данных кадров канального уровня (MaximumTransferUnit – MTU). Например, в сети Ethernetразмер передаваемых кадров до 1500 байт данных, в сети X.25 размер передаваемого поля данных кадра 128 бай, в сетях FDDI - до 4500 байт, в других сетях по-своему. Протокол IPумеет разбивать “большой пакет” на несколько частей, размеры которых соответствуют MTUсетей, и передавать их в дейтаграммах. Эти дейтаграммы будут собраны обратно в один пакет после передачи их через промежуточную сеть. Следует обратить внимание, что пакет собирает из фрагментов только устройство-получатель, но не роутеры, через которые они проходят. Роутеры не могут складывать данные в пакет, а лишь делить их на части, потому что разные части пакета могут идти разными путями через разные роутеры.

То, к какому пакету данных относится часть данных, указано в поле заголовка Идентификация. С помощью этого поля при сборке частей в пакет не перепутываются с частями других пакетов данных. Требуется чтобы число в поле Идентификация совпадало у всех частей, принадлежащих к одному пакету данных, и не совпадало для разных пакетов, по крайней мере до истечения их TTL. Когда данные пакета делятся, размер всех частей кратен 8 байтам. Это служит для того, чтобы поле Смещение фрагмента занимало меньше бит.

Если второй бит в поле Флаги равен 1, то это означает что это не последняя часть пакета. В случае, если этот бит был установлен в ноль, и биты поля Смещение фрагмента также заняты нулевыми битами, то это означает что пакет должен быть отправлен в сеть без деления на части.

В случае если в начальном бите поля Флаги записано значение, равное 1,

то деление пакета на части запрещено. В случае если такой пакет требуется передать через сеть с максимальной единицей передачи, недостаточной для него, то пакет уничтожается роутером, а устройству отправителю посылается сообщение с помощью ICMP. Этот флаг используется тогда, когда устройство-отправитель знает, что устройство-получатель не сможет восстановить пакет из частей.

1.1.4 Деление адресов на классы

Адреса в протоколе четвертой версии состоят из двух логических частей – сетевого номера и узлового номера. По тому, какие цифры записаны в первые разряды адреса можно понять, какие разряды адреса — это сетевой номер, а какая – узловой. Также, по этим разрядам можно понять класс адреса протокола.

Ниже показана структура адресовразных классов четвертой версии протокола интернета.

Рисунок 1.5 – Состав адресов протокола четвертой версии

Когда первый бит IP-адреса равен нулю, то это сеть класса A. Длина номера сети класса A – один байт. Остальные три байта занимает узловой номер. В сети этого класса номер 0 не может применяться как адрес сети, а номер 127 был занят для особых нужд. Следовательно остаются номера 1-126. Из этого следует, что сетей класса A не может быть много, зато они могут иметь большое

количество узлов.

Сеть относят к классу B в случае если первые два бита адреса равны 10. В сетях этого класса под узловой и сетевой номера отводят по два байта (по 16 бит). В этих сетях наибольшее число узлов равно 65 536. Это сети среднего размера.

Сеть относится к классу C если первые три разряда в адресе - 110. В этих сетях на собственно сетевой номер отводится 3 байта, а на узловой – 1 байт. Это наиболее часто встречающиеся сети, число узлов в которых может составлять 256.

Особый класс сетей — это сети класса D. Их адрес начинается с 4х бит 1110 и является групповым. Если пакет содержит такой адрес, то его должны получить абсолютно все узлы, имеющие данный сетевой адрес.

В случае, если первые биты IP-адреса начинается с 11110, то этот адрес стоит определять как класс E. Адреса, относящиеся к этому классу, являются забронированными для будущего.

В таблице ниже показано соотношение номеров сетей и их максимального числа узлов.

Таблица 1.1 – Типы сетей интернет протокола четвертой версии

Класс	Первые биты	Наименьший номер сети	Наибольший номер сети	Максимальное число узлов в сети
A	0	1.0.0.0	126.0.0.0	2^{24}-2
B	10	128.0.0.0	191.255.0.0	2^{16}-2
C	110	192.0.0.0	223.255.255.0	2^{8}-2
D	1110	224.0.0.0	239.255.255.255	Multicast
E	11110	240.0.0.0	247.255.255.255	Зарезервирован

1.1.5 Маскипри адресации

Раньше предприятия и учреждения для выделения им диапазона IP-адресов вынуждены были заполнять регистрационную форму, содержащую текущее количество ЭВМ и то число, до которого его планировалось увеличивать. В соответствии с этой формой предприятию выделялся класс IP-адресов: A,Вили C в зависимости от параметров сети.

Эта процедура работала некоторое время – пока количество ЭВМ в организациях оставалось небольшим. Но с наступлением эпохи широкого распространения сети Интернет и сетевых технологий количество компьютеров во многих организациях стало превышать несколько сотен, для которых требовалась уже регистрация сети, относящейся к B-классу, потому что сеть класса C могла вместить в себя адреса только 254 компьютеров. В результате это привело к тому, что сетей B-класса стало не хватать всем заявителям, но при этом большое количество адресов оставалось не задействовано.

Для решения этой проблемы были введены и получили широкое распространение и использование маски подсети, позволяющие гибко определять границу между сетевым и узловым номерами.

Маска подсети – число, используемое в паре с адресом IP. Разряды, которые в маске содержат единицы, указывают на то какие разряды в IP-адресе являются номером сети. Т.к. биты номера сети в IP-адресе идут непрерывно, то и единичные биты в маске подсети тоже должны следовать в непрерывном порядке.

Для сетей обычных классов маски имеют следующий вид:

класс A - 11111111. 00000000. 00000000. 00000000(255.0.0.0);

класс B - 11111111. 11111111. 00000000. 00000000(255.255.0.0);

класс C - 11111111. 11111111.11111111. 00000000(255.255.255.0).

Давая каждому IP-адресу маску подсети можно избавится от привязки к классам протокола интернета четвертого поколения и сделать адресацию более универсальной. Для примера, если рассмотренному выше адресу 173.274.56.117 назначить маску 255.255.255.0, то полученный адрес сети будет 173.274.56.0, но не 173.27.0.0, как должно было бы быть, пользуйся мы обычной системой адресации.

В маске подсети количество бит, равных единице, и определяющих где оканчивается номер сети, не обязательно должно быть 8, 16 и 32, не должно делить адрес на части по 8 бит. Предположим, что для адреса IP134.124.87.6 назначена маска 255.255.128.0, что в битовой форме:

10000110. 01111100.01010111.00000110 – IP-адрес

11111111.11111111.10000000.00000000 – маска подсети.

Если не брать в расчет маску, а использовать систему обычных классов, адрес 134.124.87.6 следует отнести к классу B, а значит номер сети нужно определять по первым двум байтам – 134.124.0.0, а узловой номер по последним двум – 0.0.87.6.

В случае же, если для определения границы сетевого номера использовать маску подсети, то необходимо провести логическое умножение IP-адреса и маски в двоичной форме. В результате получаем:

$$\begin{array}{l} 10000001.01000000.10000110.00000101 \\ \& \quad 11111111.11111111.10000000.00000000 \\ \hline 10000001.01000000.10000000.00000000 \end{array}$$

Если полученный результат перевести в десятичную форму, то получим сетевой номер 134.124.87.0,аузловой - 0.0.6.5.

Возможен также краткий вариант записи маски подсети. Его суть в том, что сеть 172.255.97.117 с маской 255.255.255.252 записывают как

172.255.97.117/30, где «/30»обозначает что в маске 30 идущих подряд бинарных единиц.

В таблице ниже показано соответствие префикса и маски:

Таблица 1.2 – Соответствие префикса и маски

Маска	Префикс	Количество узлов в сети
255.255.255.252	/30	4
255.255.255.248.	/29	8
255.255.255.240	/28	16
255.255.255.224	/27	32
255.255.255.192	/26	64
255.255.255.128	/25	128
255.255.255.0	/24	256
255.255.0.0	/23	512

Маски стали очень широко применяться в построении логики сетей для самых разнообразных целей. Например, администратор сети благодаря им может увеличить количество узлов сети без получения от провайдера дополнительных сетевых номеров. Также провайдеры способны объединять пространства адресов разных сетей с помощью ввода «префиксов» и добиться уменьшения таблиц маршрутизации и улучшения благодаря этому качества и скорости работы роутеров. Также, записывать маску подсети как префикс значительно быстрее.

1.1.6 Специальные зарезервированные адреса

В протоколе интернета, в отличии от протоколов канального уровня локальных сетей, не поддерживается понятие «широковещательности» в том плане, что пакеты должны быть доставлены вообще всем узлам. И у широковещательногоадреса и у ограниченного широковещательногоадреса есть пределы распространения в сети. Они ограничены или сетью, куда входит устройство-отправитель, или сетью, адрес которой задан в адресе назначения. Следовательно, разделение сети роутерами на части ограничивает широковещательное распространение в пределах одной части

общей сети, потому что нет возможности послать пакет сразу на все узлы всей сети.

IPпротокол имеет некоторые соглашения о том как особенно интерпретировать некоторые IP-адреса:

0.0.0.0 – Адрес шлюза по умолчанию. Это адрес устройства, куда следует отправлять пакеты данных, если их адресат в локальной сети(таблицемаршрутизации);

255.255.255.255 – Адрес, предназначенный для широкого вещания. Пакеты данных, отправленные на этот адрес, следует передать на все узлы, которые содержат устройство-источник пакета.В случае, когда в поле адреса узла назначения находятся только единицы, то сообщение с таким адресом стоит отправить на все узлы в сети с таким номером сети. Например, если сообщение имеет адрес 138.172.169.255, то доставить его нужно всем узлам в сети 138.172.169.0. Это – широковещательная рассылка сообщений. При присвоении адреса элементам сети нужно брать во внимание условия, наложенные специальным предназначением определенных адресов. Например, сетевой номер и узловой номера не могут быть представлены только лишь одними единицами или одними нулями. Следовательно, на два уменьшается наибольшее количество узлов для сети любого класса, которые показаны в таблице выше. Так, в третьем классе сетей под адрес узла отведен один байт, которым можно задать номера от 0 до 255. Но на самом деле адреса 0 и 25 не могут применяться, следовательно остается доступным всего 254 номера. Так же понятно, что узел-адресат не может иметь адрес, выглядящий как 123.255.255.255, потому что узловой адрес в этой сети класса А не может состоять из одних единиц.

«Номер сети».«нули» - адрес сети без адреса узла (например 138.172.0.0).

«Нули».«номерузла» - адрес узла в данной сети (например 0.0.67.124). Используется для отправки пакета определенному узлу внутри сети.

Особо выделен адрес, начинающийся с байта 127. Такие адреса предназначены для взаимодействия процессов на одном компьютере и тестирования программ. Если запрос посылается на адрес 127.0.0.3, то образуется петля. Пакет не отправляется в сеть, а возвращается на устройство, как будто он был только что принят. В следствии этого сети не дают присваивать компьютерам адрес, который начинается со 127. Можно считать, что адрес 127.0.0.0 относится ко внутренней сети модуля маршрутизации узла, а адрес 127.0.0.1 относится к адресу этого модуля на внутренней сети. Так же каждый адрес в сети 127.0.0.0 предназначен для указания на свой модуль маршрутизации.

Таблица 1.3 – Описание адресов в сети

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

1.1.7 IP-адреса, используемыев локальныхсетях

Все адреса, которые используются в Интернете, подлежат регистрации для гарантирования их уникальности в мире. Эти адреса носят имя «реальных» или «публичных» IP-адресов.

Для сетей, у которых подключение к Интернету отсутствует, не требуется, потому что в них могут использоваться абсолютно любые возможные адреса. Но, во избежание конфликтных ситуаций при дальнейшем подключении этой сети к Интернету, следует применять в сети только те частные IP-адреса, не существующие в мировой сети и существование которых там невозможно, которые представлены в таблице 1.4.

Таблица1.4 – Диапазоны частных IP-адресов

Диапазоны IP-адресов, используемых в локальных сетях
10.0.0.0 – 10.255.255.255
172.16.0.0 – 172.31.255.255
192.168.0.0 – 192.168.255.255

1.2 ПротоколИнтернета шестой версии

Когда разрабатывался IPv4, уровень развития инфокоммуникационных технологий не предполагал такого большого числа устройств, находящихся в сети Интернет. В то время предполагалось, что более 4-х миллиардов всевозможных сетевых адресов будет более чем достаточно для подключения всех устройств в мире к сети Интернет. Но в 2020 году число устройств, включенных в сеть Интернет, превысило число в более чем 25 миллиардов и продолжает быстро увеличиваться.

Пока еще использование старого протокола Интернета четвертого поколенияпроходит нормально благодаря использованию разных технологий

экономии при использовании IP-адресов. Однако всем давно понятно, что жизнь протокола интернета 4-го поколениязаканчивается, т.к. уже сейчас предусматривается возможность предоставления доступа к сети Интернет различных бытовых устройств и приборов (микроволновых печей, холодильников), для возможности удаленного управления всеми этими приборами через Интернет из любого места на планете.

В текущей ситуации просто жизненно необходим переход на новую версию формата сетевых адресов. Так как многие специалисты предсказывали проблему возникновения дефицита адресов в глобальной сети еще в начале 90х годов прошлого века, тогданачалась работа над новой, шестой версией протокола Интернета, способного решить вышеизложенные проблемы.

Он должен был решать следующие задачи:

- уменьшить размер таблиц маршрутизации.
- увеличить протокольный уровень безопасности.
- совместимость с протоколом версии IPv4.
- упростить протокол для ускорения обработки пакетов относящихся к маршрутизации.
- с помощью прямого указания на области рассылки упростить работу многоадресных рассылок.
- протокол должен иметь перспективы развития в будущем.
- даже при нерациональном использовании диапазона адресов давать миллиардам устройств доступ к сети Интернет.

Протокол шестой версии был представлен в 1992 году как абсолютно новая версия протокола Интернета, которая была создана для того, чтобы решить проблемы, которые не смогла решить предыдущая версия протокола Интернета при ее использовании. Эта версия использует длину адреса в 128 бит вместо 32-х у предыдущей.

Сейчас протокол 6-й версии еще не получил такого широкого распространения в сети Интернет, как протокол 4-й версии, но шаг за шагом его часть в масштабе планеты увеличивается и в начале 2020 года составляет почти 30%.

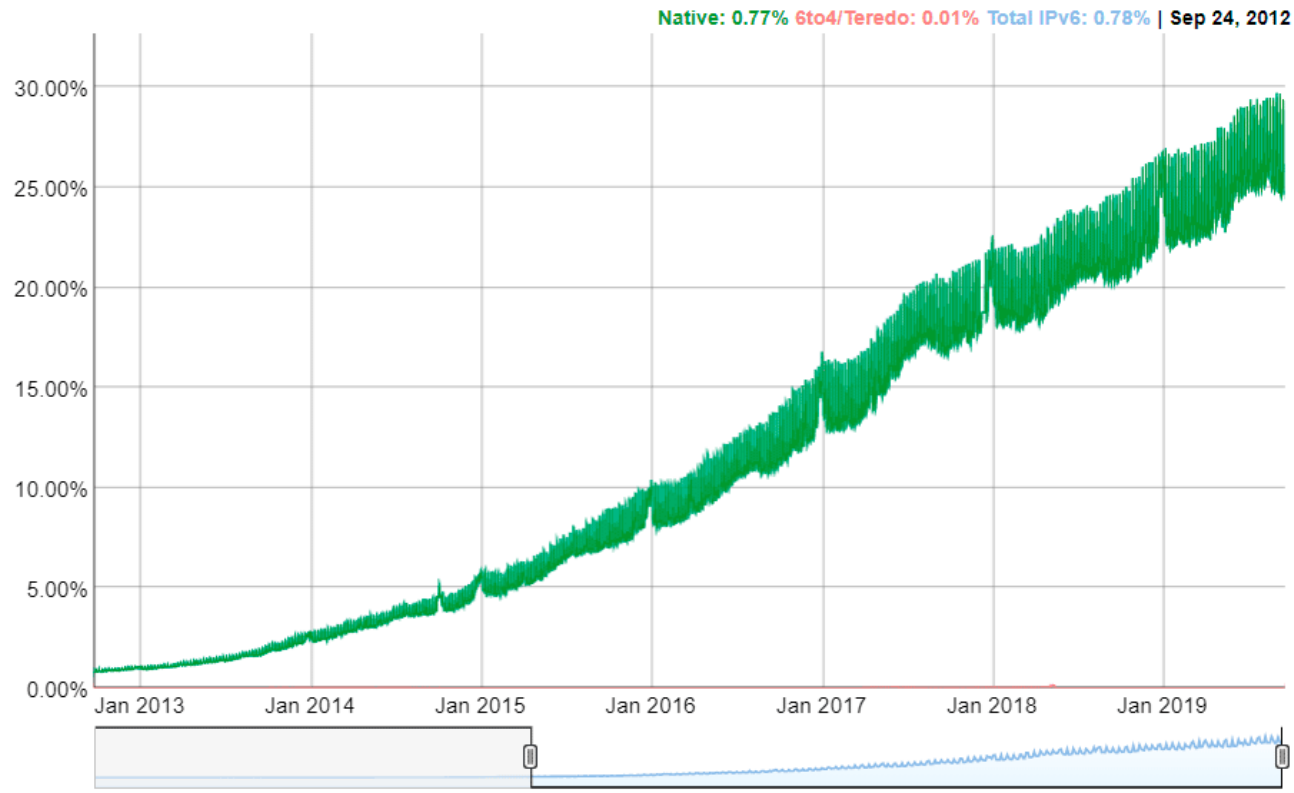

Рисунок 1.6 – График количества устройств использующих IPv6

Протокол Интернета 6-й версии достаточно хорошо решает все поставленные перед ним задачи. Он имеет все достоинства IP-протокола и некоторые новые возможности, но у него отсутствуют некоторые недостатки. В общем протокол этой версии не обладает совместимостью с протоколом 4-й версии, но обладает совместимостью со всеми другими протоколами Интернета, однако для ее реализации необходимы небольшие изменения.

1.2.1 Особенности протокола шестой версии

Для обеспечения практически неограниченного запаса адресов протокол Интернета 6-й версии имеет длину 16 байт.

Упрощенный заголовок у шестой версии по сравнению с четвертой. Это увеличивает скорость обработки пакетов роутерами, что ведет к увеличению скорости работы сети.

Произведено улучшение поддержки необязательных параметров. Это было действительно существенное изменение, потому что обязательные ранее поля в заголовке перестали быть такими.

Улучшена безопасность передачи данных. Обязательными частями IPv6 являются конфиденциальность и аутентификация.

Для выделения особого внимания типу услугу в заголовке пакета данных было выделено специальное поле.

Октет	0 1 2 3 4 5 6 7	8 9 10 11 12 13 14 15	16 17 18 19 20 21 22 23	24 25 26 27 28 29 30 31
0	Версия	Приоритет	Метка потока	
4	Длина полезной нагрузки		Следующий заголовок	Макс. число транзитных узлов
8-20	IP-адрес отправителя			
24-36	IP-адрес получателя			
	Дополнительны заголовок			
	Данные			

Рисунок 1.7 – Состав пакетов шестой версии

В состав заголовка IPv6 входят следующие поля:

Поле Версия — принимает значение 6 для протокола 6-го поколения.

Поле Метка потока – используется для создания между устройствами отправителем и получателем соединения, имеющего определенные свойства и отвечающего определенным требованиям. К примеру, между двумя

приложениями на разных устройствах может существовать поток данных, обладающий определенными требованиями к задержкам, для чего потребуется выделение определенной доли трафика сети.

Поле Приоритет – необходимо для своевременного различия пакетов по требованиям к доставке.

Поле Длинна полезной нагрузки – показывает сколько байт данных передается после заголовка.

Поле Следующий заголовок – указывает, какой дополнительный заголовков идет вслед за основным.

Максимальное число транзитных узлов – аналогично времени жизниу пакетов протокола четвертой версии.

Так же присутствуют дополнительные заголовки:

Заголовок Маршрутизация – ограниченный перечень роутеров, через которые проходит пакет.

Заголовок Параметры получения – дополнительные данные, предназначенные для устройства-получателя.

Заголовок Параметры маршрутизации – различные данные, предназначенные для роутеров.

Заголовок Аутентификация – проверка отправителя на подлинность.

Заголовок Фрагментация – поле, предназначенное для управления фрагментами пакета.

Шифрование данных – содержит информацию о зашифрованном содержимом.

1.2.2 Виды адресов

Unicast – Идентификатор одиночного интерфейса. Пакет, имеющий уникальный адрес, должен быть доставлен устройству, имеющему этот адрес.

Anycast – Идентификатор набора интерфейсов (которые относятся к разным маршрутизаторам). Данные, имеющие такой адрес как точку конечного назначения, должны быть доставлен одному из устройств, список которых указан в адресе.

Multicast – Идентификатор набора устройств (которые обычно относятся к разным узлам сети). Данные, которые отправляются по такому адресу, должен быть доставлен всем устройствам, которые указаны таким адресом.

В протоколе интернета шестой версии отсутствуют широковещательные адреса, так как их задачи отданы адресам типа milticast.

Так же в шестой версии протокола для любых полей являются допустимыми все единицы или все нули, если заранее не оговорено исключение.

АдресаIPv6 всех типов связаны не с узлами, а с интерфейсами. В следствии того, что каждый интерфейс может относиться только к одному узлу. Узел может быть определен с помощью уникального адреса интерфейса.

Уникальный адрес протокола шестой версии может относиться только к одному интерфейсу, но к одному интерфейсу может быть приписано большое количество адресов разных типов.

Но из этого правила есть два исключения.

1) Сразу нескольким реальным интерфейсам возможно назначит одинаковый уникастный адрес, тогда, когда эти несколько интерфейсов рассматриваются приложением как один цельный элемент на уровне представления его в глобальной сети.

2) У роутеров могут иметься в наличии интерфейсы без номера (к примеру, интерфейсу не назначен никакой сетевой адрес) в случае применения подключения точка-точка, для того, чтобы не было необходимости вручную объявлять и настраивать эти адреса. В случае соединения точка-точка не нужны адреса, если такие интерфейсы не используют при посылке частей пакета интернет протокола шестой версии в качестве начального и конечного пунктов. Прокладку пути в данном случае происходит в соответствии со схемой, похожей на применяемую протоколом CIDR впротоколе интернета четвертого поколения.

Протокол шестой версии имеет соответствие с протоколом четвертой версии, где подсеть ассоциируется с каналом. Несколько подсетей могут соответствовать одному каналу.

1.2.5 Представление адреса

С использованием шестнадцатеричных символов

В сетях в основном используется эта форма представления адресов IPv6. Она соответствует виду x:x:x:x:x:x:x:x, гдекаждому из знаков xсоответствует определенное четырехзначное число в шестнадцатеричной системе счисления (всего восемь таких чисел, каждому из которых соответствует два байта адреса), к примеру:

AF16:0000:783D:1122:56BE:FFAA:0016:5192.

Уменьшенная форма

Так как адрес имеет большую длину, он часто содержит много нулевых значений, которые идут подряд. Для того чтобы сделать более простой запись адресов IPv6, применяют уменьшенную форму. В ней соседние последовательности нулевых символов заменяются двойным

символом двоеточия,но такие символы могут находиться в адресе только в одном месте.

К примеру:

У адреса FFBC:0:0:0:0:BA29:1419:4867 имеется уменьшенная версияFFBC::BA29:1419:4867.

Адрес 0:0:0:0:0:0:0:1 в уменьшенной форме превращается в ::1.

Адрес 0:0:0:0:0:0:0:0 принимает форму ::.

Объединенная форма

Такая форма является формой, сочетающей формат адреса протокола четвертой версии с форматом протокола шестой версии. Р адрес представляет собой формат x:x:x:x:x:x:y.y.y.y. Здесь каждому x соответствует число, состоящее из двух байт (всего 6 таких чисел, на каждое приходится по два байта сетевого адреса), а y.y.y.y является частью адреса, которая записана в формате протокола четвертой версии (всего 4 байта).

Например:

0:0:0:0:0:0:17.154.67.12

Или в уменьшенной форме:

::17.154.67.12

Таблица 1.5 – Специальные адреса шестой версии

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

1.3 Виртуальныесети(VLAN - VirtualLocalAreaNetwork)

1.3.1 Общее описание виртуальных сетей

В настоящее время большая часть предприятий и компаний в мире не применяют такую порой нужную, а иногда и незаменимую функцию, как создание сети VLAN (виртуальной локальной сети) в рамках реальной сети. Такая возможность имеется в наличии у большей части современных сетевых роутеров. Это зависит от многих явления, поэтому нужно подробно рассмотреть технологию виртуальных локальных сетей с точки зрения применения ее в данных целях.

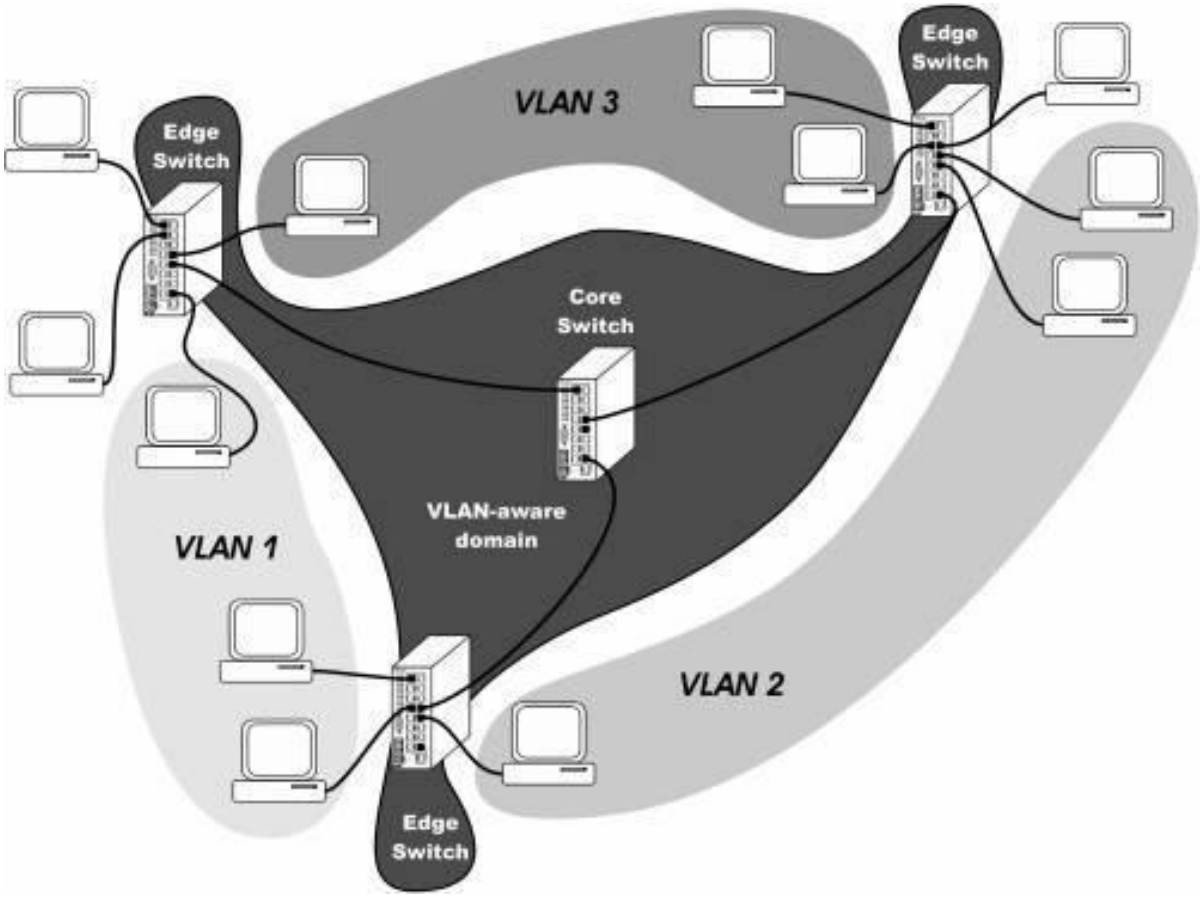

Рисунок 1.8 – Деление физической локальной сети на виртуальные локальные сети

Сначала нужно понятьсаму концепцию виртуальных локальных сетей. Под этим понятием скрывается некая, подключенная к локальной сети, часть ЭВМ, которые были сгруппированыпо некоему признаку в один домен логически для отправки всем им широковещательных сообщений. Так, например, некоторая часть вычислительных машин может быть сгруппирована в соответствии с составом учреждения, или по типу участия в общей работе с какой либо задачей. Виртуальная сеть дает некоторое количество дополнительных возможностей и выгод. Во-первых, это большое увеличение скорости работы (по сравнению с обычной физической локальной сетью), увеличение уровня защиты передаваемых данных, упрощение схемы управления сетью.

Таким образом, при применении виртуальной сети происходит деление всей физической сети на домены широкого вещания. Следовательно, данные внутри этой сети передается не всем компьютерам, входящим в нее, а только между членами виртуальной сети. Отсюда следует, что трафик, созданный сервером для распространения широкого вещания, исчерпывается одним заранее выбранным доменом и не распространяется к компьютерам в других доменах. Таким образом возможно добиться наилучшего распределения способности пропускать трафик сети между устройствами, выделенными в домены: устройства и сервера в разных виртуальных сетях не способны друг друга увидеть.

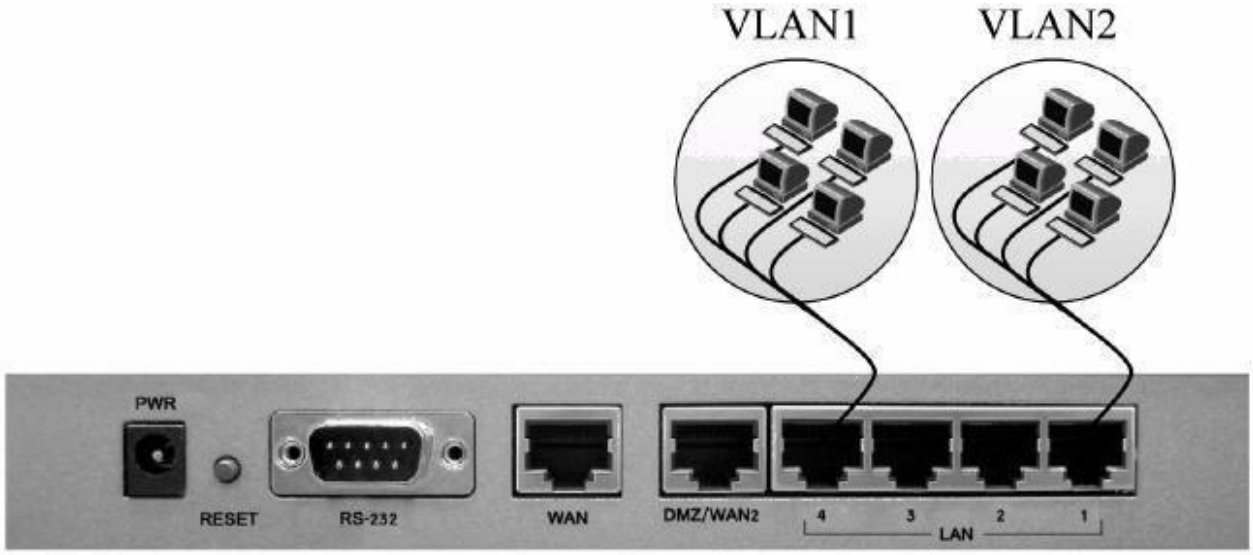

Рисунок 1.9 – Разделения локально сети на виртуальные на роутере

В виртуальных сетях, данные очень хорошо защищены от несанкционированного доступа потому что вся передача данных происходит внутри одной обособленной группы устройств, то есть они не получают пакеты данных, создаваемые в какой-либо другой похожей группе. Описывая виртуальные сети, необходимо заметить, что их достоинство заключается так же в том, что они дают значительное упрощение управления сетью. К администрированию относятся так же задачи добавления дополнительных элементов сети, перемещение этих элементов, и их удаление. Например, в случае если некий пользователь виртуальной сети перемещается в другое место в здании, администратору сети нет необходимости производить новую коммутацию кабелей. Ему требуется всего лишь настроить оборудование сети со своего рабочего терминала. При некоторых типах построения виртуальных сетейконтроль над перемещениями членов отдельных групп может происходить в режиме автомата, без необходимости вмешательства человека. Системному администратору требуется всего лишь знать, как настроить виртуальную сетьтак, чтобы сеть сама производила все нужные действия. Администратор способен создавать новые отдельные виртуальные локальные сети, не вставая со своего рабочего места. Все это значительно экономит рабочее время, которое может понадобиться для решения других самых важных проблем.

1.3.3 Методы организации виртуальных сетей

Есть несколько разных способов реализации сетей VLAN: с помощью мак-адресов, протоколов третьего уровня и с помощью портов коммутаторов. Каждый из этих методов относится к одному из нижних уровней (канальному, сетевому и физическому) модели OSI . Описывая, что же такое виртуальные сети, нужно заметить, что существует и четвертый способ реализации – используя правила. В наше время он практически не используется, но с его помощью можно обеспечить большую гибкость сети. Следует более подробно рассмотреть вышеперечисленные способы для лучшего понимания того, какими отличия в них есть.

1.3.3.1 Организация виртуально сети с помощьюпротоколов

Данный способ практически не применяется в роутерах низкого уровня (в отделе или группе). Он чаще встречается на магистральных роутерах, которые имеют встроенные средства управления потоками основных протоколов физических локальных.

В данном случае считается, что относящаяся к определенной виртуальной сетигруппа портов роутера будет группироваться в некую подсетью. Здесь, пластичность сети обеспечивается тем, что изменение порта устройства, относящийся к той же VLAN, будет обнаружено самим роутером и не нуждается в изменении настроек виртуальной сети. В этом случае построение виртуальной сети относительно просто, потому что роутер сам проводит анализ сетевых адресов компьютеров, определенные для каждой сети. Этот метод способствует поддерживанию и взаимодействия между разными виртуальными локальными сетями без использования дополнительных методов. Один из недостатков данного способа – большая стоимость коммутаторов, на которых он реализован.

1.3.3.2 Организация виртуальной сети с помощью портов

В данном способе предполагается логически объединять определенные, выбранные для объединения в виртуальную локальную сеть, физические порты роутеров. Например, администратор сети может задать условие, что некоторые определенные порты, к примеру, 1, 3 и 4 объединяются в виртуальную сеть номер 1, а порты с номерами 2, 5 и 6 объединяются виртуальную сеть номер 2 и тому подобное. Один и тот же разъем на роутере вполне может быть использован для включения нескольких устройств – для этого применяется хаб. Все эти устройства будут определяться как участники, относящиеся к одной виртуальной сети, к которой относится порт коммутатора, который их обслуживает. Такая не гибкая привязка участниковVLAN к портам – основной недостаток этой схемы организации виртуальной сети.

1.3.3.3 Организация виртуальной сети с помощью MAC-адресов

Во главе данного метода стоит назначение неповторимых адресов канального уровня модели OSI (в шестнадцатеричной системе), которые есть у каждой сетевой карты каждого устройства реальной сети. Описывая виртуальные сети нужно обратить внимание, что данный метод является более универсальный относительно метода организации виртуальной сети на основе портов, потому что к одному и тому же разъему роутера возможно подключать устройства, которые принадлежат к различным сетям VLAN. Так же в этом способе можно отследить изменение порта, на которое подключено устройство. Это позволяет сохранять отношение устройства к определенной сети в автоматическом режиме без вмешательства человека.

Сети на базе MAC-адресов имеет относительно простой принцип работы – на роутере находится таблица, в которой показано соответствие MAC-адресов рабочих устройств определенным VLAN. В случае, если происходит перенос какого либо устройства на другой разъем, сравнивается его поле MAC-адреса с данными, содержащимися в таблице. После этого делается верный вывод о том, к

какой виртуальной сети относится устройство. Одним из недостатков данного способа реализации виртуальных сетей является сложность конфигурирования сети, что может изначально стать причиной ошибок.

Хоть роутер и сам создает таблицу соответствия адресов и сетей, администратор сети должен сам проконтролировать работу устройства и просмотреть всю таблицу для того, чтобы понять, какие адреса каким группам соответствуют, после чего назначить определенный адрес соответствующей локальной виртуальной сети. Именно в этом месте могут появиться ошибки. Например, в некоторых роутерах, настройка которых относительно проста, но дальнейшее перераспределение сложнее, чем в способе с использованием портов

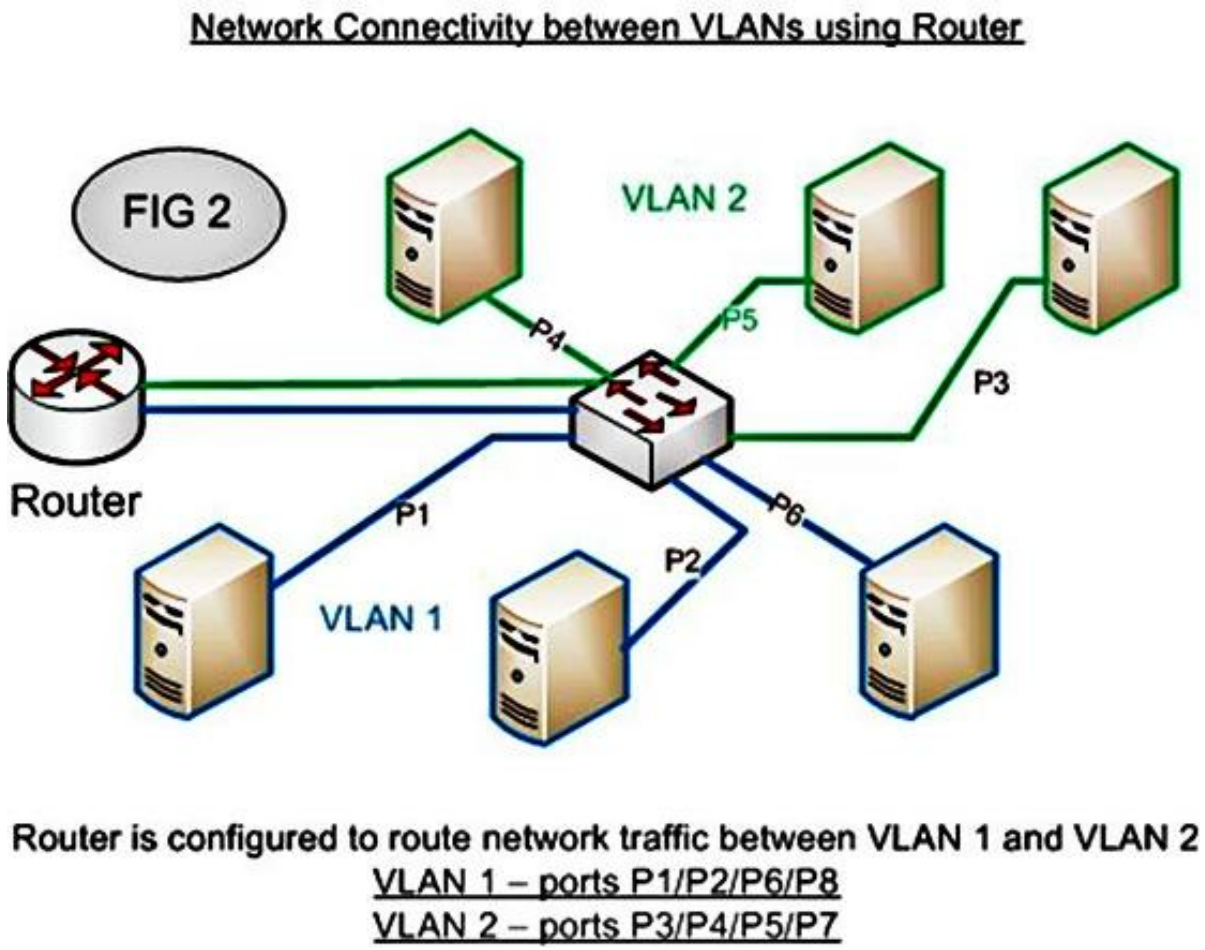

Рисунок 1.10 – Формирование VLANs на базе MAC-адресов

2 Моделирование инфокоммуникационной сети

2.1 Описание сети

Одной из целей данной работы является определение эффективности работы сети связи с поддержкой различных сервисов по времени задержки в прохождении пакета из-за превышения нагрузки на сервера обрабатываемыми пакетами данных при разных конфигурациях. Главный интерес в данной работе уделен моделированию и анализу работы сети связи с поддержкой различных сервисов при использовании сетевых протоколов 4-й и 6-й версий и их сравнения. Протокол IP сегодня является важнейшим в организации любой сети. Данный протокол, объединяющий части сети, обеспечивает передачу данных между различными узлами сети через случайное число промежуточных маршрутизаторов. Часть пакета, содержащая служебную информацию, очень влияет на работу сети. В зависимости от той информации, которая содержится в заголовке пакета IP, зависит доставка данных в точку назначения, более быстро и эффективно. Чем быстрее и эффективнее пакет обрабатывается наузловых маршрутизаторах, тем качественнее и быстрее работа всей сети. Протокол интернета шестой версии способствует более качественной работе сети по сравнению с протоколом четвертой версии за счет нескольких его особенностей.

В данном эксперименте была выбрана обычная схема сети жилого микрорайона, поддерживающая работу различных сервисов. Этой сети принадлежит 4000 абонентов, подключенных через маршрутизаторы и коммутаторы к различным Web, VoIP, видео, аудио сервисам. Между собой и с коммутаторами доступа маршрутизаторы соединены с помощью оптоволоконных кабелей. От коммутаторов через UTP кабель по технологии FastEthernet трафик передается подключенным абонентам. Для отслеживания влияния количества маршрутизаторов (узлов) и абонентов в сети при использовании двух исследуемых протоколов решено было использовать три разных модели различной емкости и масштаба.

Изначальная модель включает в себя 1000 абонентов, которые подключены к коммутатору, а дальше через маршрутизатор к группе серверов, от которых получают услуги.

Следующая модель имеет уже 2000 абонентов и еще один дополнительный маршрутизатор, отсутствующий в первой модели. В ней тоже весь траффик идет сквозь маршрутизаторы к серверам, дающим доступ к различным услугам для подключенных абонентов.

В последней модели имеется в четыре раза больше подключенных абонентов, которые используют услуги и объединяются друг с другом доступом к сервисным серверам с помощью трех маршрутизаторов.

2.2 RiverbedModeler

Для того, чтобы создать сеть, провести над ней имитационных экспериментов и дальнейшего анализа будет использована технология RiverbedModeler. Пакет программ RiverbedModelerдает большие возможности для моделирования работы сети. Модели сети в RiverbedModelerдают возможность уделять большое внимание к созданию определенного объекта архитектуры сети, вплоть до различных мелочей. Возможна выборка необходимой статистики, которая собирается с любого отдельного объекта сети или сразу со всей сети. Так же можно запускать процесс работы модели на определенное время, симулировать работу сети и осуществлять просмотр результатов симуляции.

Все вышеперечисленное далеко не все возможности, которые предоставляет пакет программ RiverbedModeler. Этот пакет имеет большой потенциал для решения разных вопросов в организации информационно-вычислительных сетей.

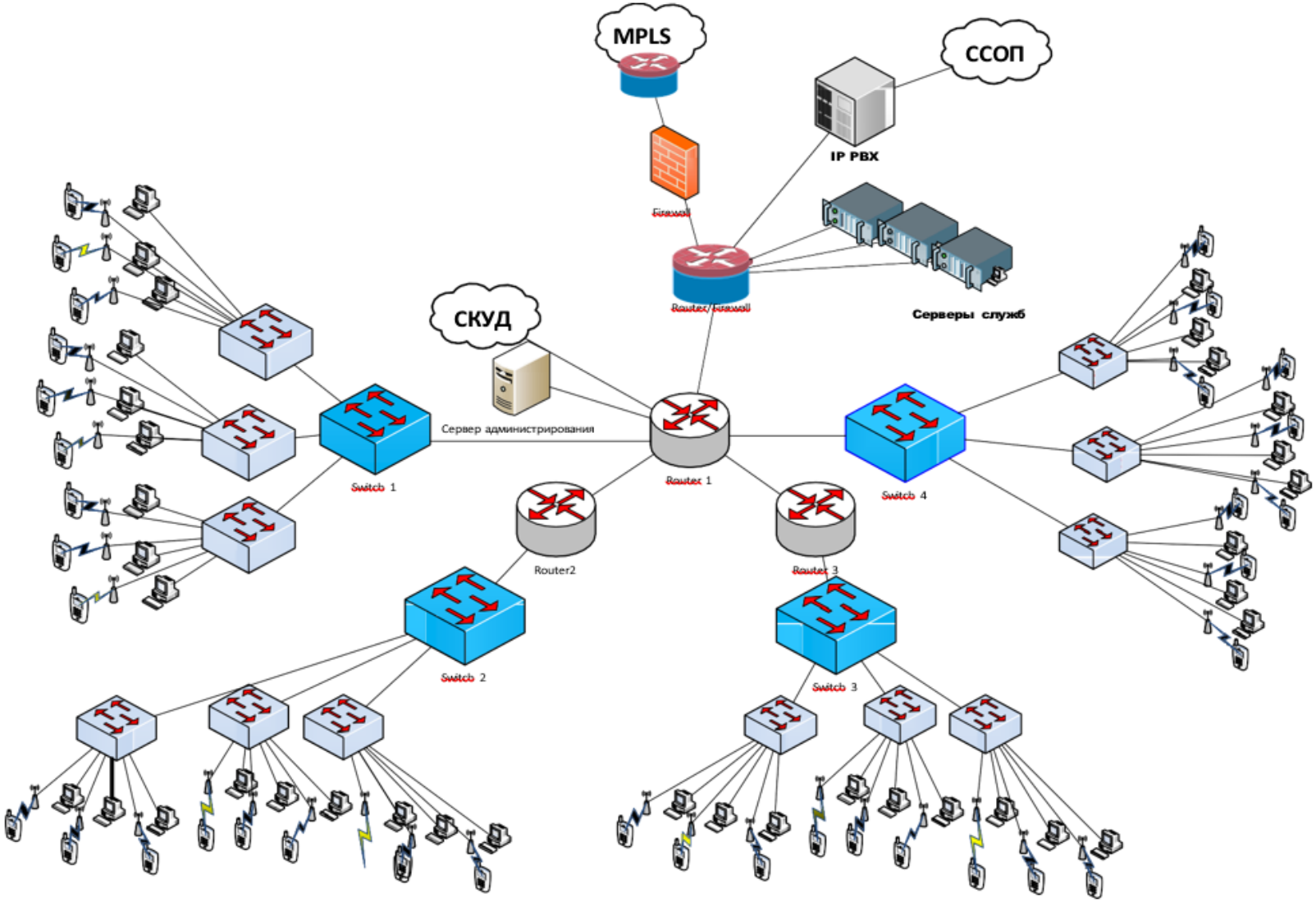

Рисунок 2.1 – Типовая схема мультисервисной сети микрорайона

Применение моделирования высокого уровня дает возможность гарантировать правильность и полноту выполнения системой тех функций, которые определил заказчик.

Рисунок 2.2 – Порядок работы с пакетом программ RiverbedModeler

Эта система программ дает большие возможности в построении моделей вычислительных сетей, представленных в графическом виде. Это является одним из главных преимуществ, потому что у разработчика есть возможность обозревать всю сеть как целиком, так и на некоторых отдельных частях. Также присутствует возможность принимать во внимание размеры реальной сети путем создания

проектов на изображении нужного масштаба (жилого района, кампуса, офиса) принимая в расчет расстояние между элементами. Или используя, например, схему некоторого здания, где находится или будет находиться сеть, можно получить уже готовый проект, который имеется возможность изменять только в рамках, которые ограничены средой размещения.

RiverbedModelerAcademicEdition – этосовершеннобесплатная утилита, предназначенная для образовательных целей студентов высших учебных заведений. Установка производится после регистрации, в которой необходимо указать данные ВУЗа и самого студента.

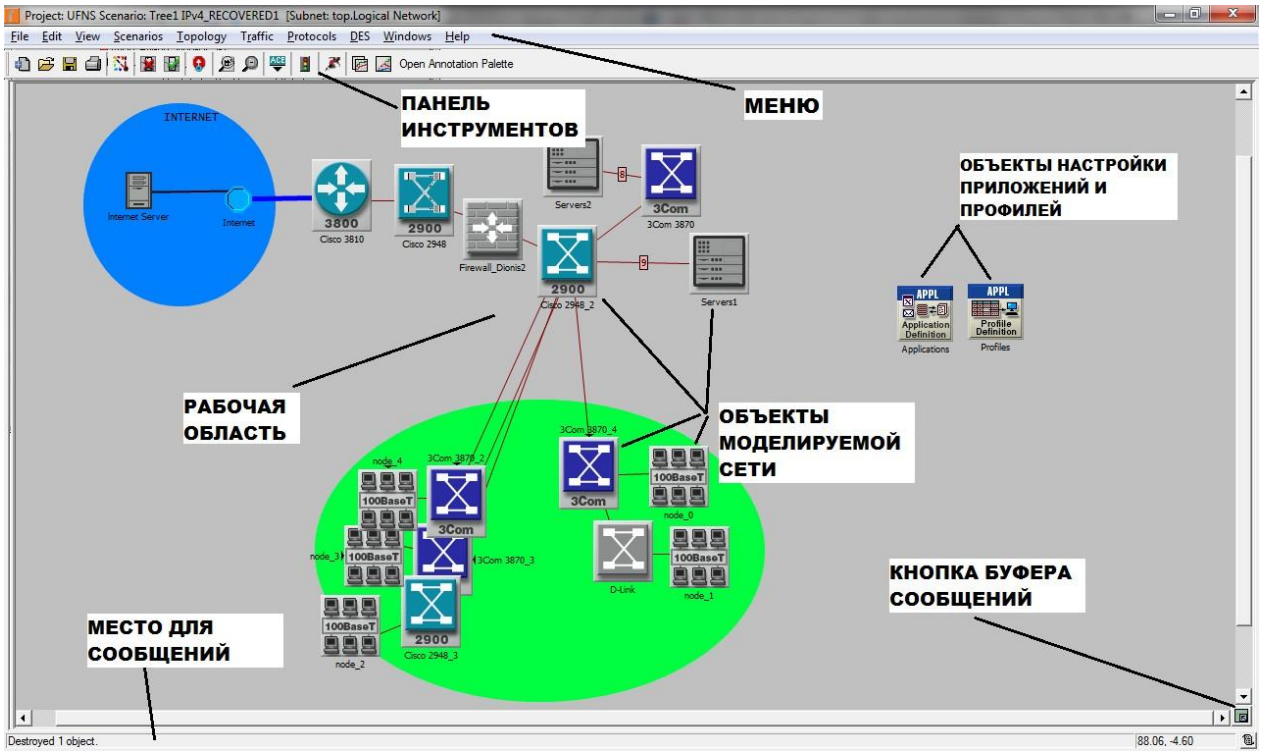

Рисунок 2.3 – Интерфейс программы RiverbedModeler

RiverbedModeler – это виртуальная сетевая среда, способная моделировать поведение сетей и их элементов, таких как маршрутизаторы, коммутаторы, серверы и рабочие станции, и даже протоколы и отдельные приложения. Дружественный к пользователю интерфейс RiverbedModeler имеет технологию «перетаскивания», дающую широкие возможности для моделирования, управления, поиска и устранения неполадок в реальных структурах сетей.

RiverbedModelerдает возможность проектировщикам, менеджерам и операторам сетей лучше решать труднейшие проблемы, перед внесением изменений в реальную сеть моделировать их, планировать на будущее различные сценарии, вроде увеличения трафика или выхода из строя элементов сети. Так же приложение дает возможность самостоятельно создавать различные уникальные сетевые устройства, отсутствующие в его базе моделей, что делает допустимым максимально точно построить проект сети для достижения лучших результатов.

Существует возможность при проектировании сети создавать модели сценариев – отдельных схем и планов действий. Приложение дает возможность проводить анализ воздействия на сеть отдельных клиент-серверных приложений и новейших технологических решений; проводить моделирование иерархии сетей, локальных и глобальных ЛВС, учитывающих алгоритмы маршрутизации; производить анализ и оценивание производительности моделей сетей. При моделировании имеется возможность проследить за тем, как изменяется запаздывание отклика и любые другие характеристики сети при разных подходах к ее проектированию. При окончании моделирования разработчику будет предоставлена информация о слабых местах сети – имеющих слабую пропускную способность загруженных устройствах и линиях связи, уровне трафика между определенными узлами, задержке между ними и прочее.

Перед созданием модели сети (которая в Modelerназывается проектом), нужно определиться с ее узлами: с рабочими станциями, маршрутизаторами и коммутаторами, соединениями между узлами, приложениями, работающими на разных узлах. Так же возможно создать некоторый специфический трафик, имеющийся в настоящей работающей сети, или же взять параметры работы из файла с характеристиками работы настоящей сетевой инфраструктуры.

3 Исследование качества работы сетей связи с использованием различных протоколов

3.1 Сравнение работы протоколов четвертой и шестой версий

При создании модели сети применялась программа RiverbedModeler, дающая возможность моделировать работу сетей и получать их характеристики в виде вывода графиков с теми или иными параметрами: временем задержки прохождения пакета, пропускной способностью узла, загрузке сервера и т.п.

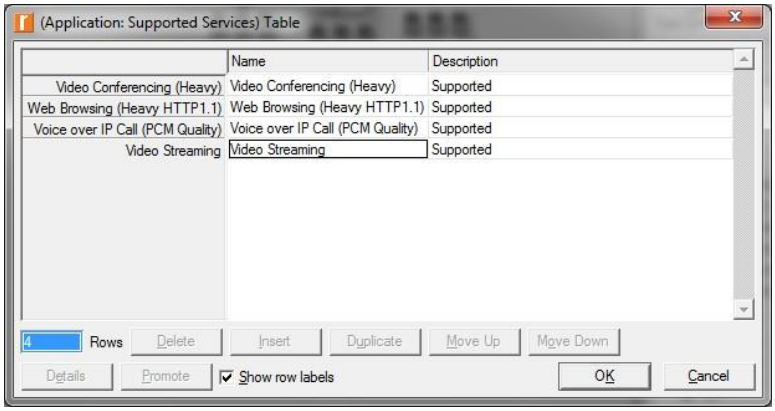

Рисунок 3.1 – Меню задания вида трафика

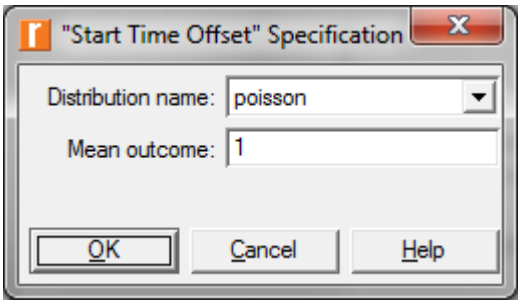

Рисунок 3.2 – Меню задания генерациитрафика

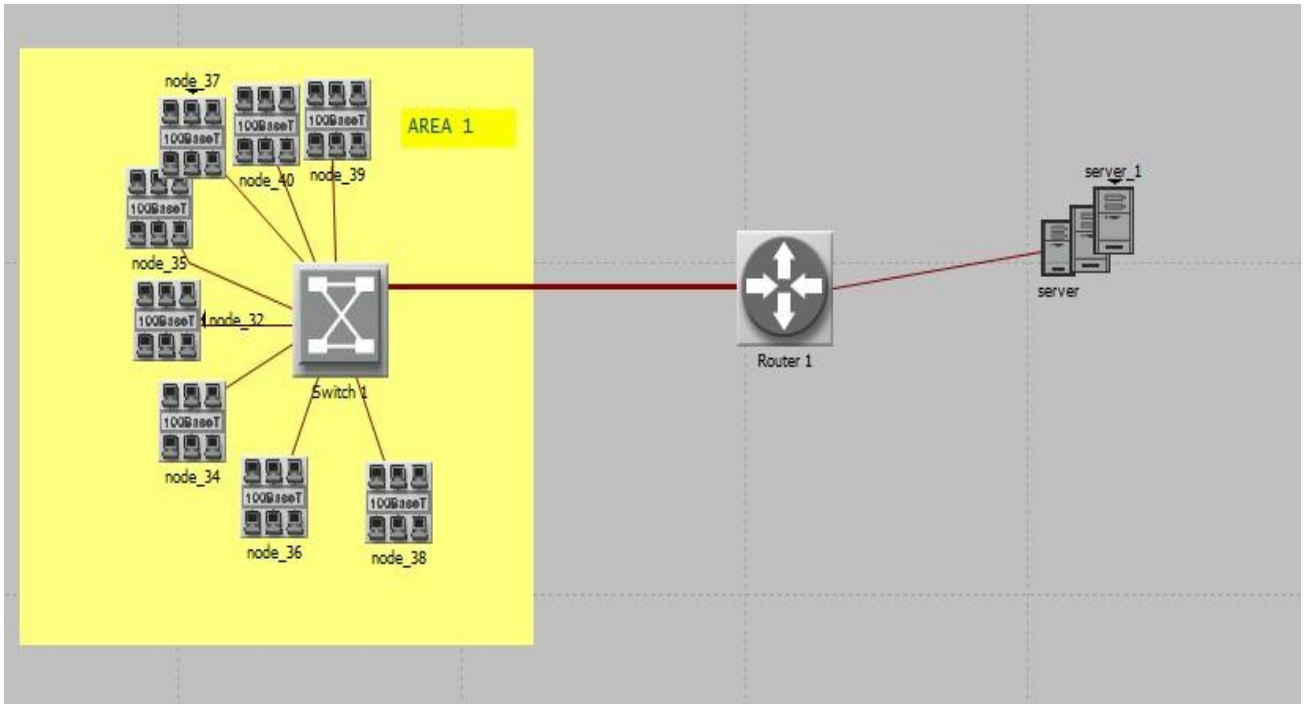

Рисунок 3.3 – Модель первой сети

В первой модели мы имеем тысячу абонентов, а так же один маршрутизатор, пропускающий через себя траффик к серверам, которые обслуживают абонентов предоставляя им разные сервисы: Web,VoIP,видео,аудиотрансляцииидругое. При моделировании были настроены спецификации генерирования трафика по определенному закону – 100 пакетов в секунду от каждого подключенного устройства. Каждому элементу в сети был присвоен личный IP-адрес. Сначала сеть была настроена согласно протоколу интернета IPv4, а потом компьютеры и маршрутизатор переконфигурировались для работы с протоколом IPv6.

После моделирования работы сети общей продолжительностью 15 минут были получены результаты. Как критерий оценки производительности сети было использовано среднее время прохождения пакета через сеть с несколькими узлами соединения, связанными друг с другом дуплексными линиями связи с пропускной способностью $d_{l,m}$байт/с между lи mузлами.

Все коммутирующие узлы имеют буфер с неограниченной емкостью. Длина пакета в среднем равна L_p=1/μ байт. Поток данных, который создается в

узле i и отправляющийся узлуj – простейший, и имеет среднюю интенсивность $I_{i,j}$(пакетовв секунду). Общую среднюю интенсивность можем найти согласно формуле:

$$I = \sum_{i=1}^{N} \sum_{j=1}^{N} I_{i,j}, \tag{1}$$

где N - число узловых роутеров.

Тогда время средней задержки пакета в сети можно найти по следующей формуле:

$$T = \frac{1}{I} \sum_{i=1}^{N} \sum_{j=1}^{N} \gamma_{kl} t_{kl}, \tag{2}$$

где t_{kl} – среднее время нахождения пакета в линии,

$$\gamma_{kl} = \sum_{i=1}^{N} \sum_{j=1}^{N} I_{ij} x_{kl}^{(i,j)}, \tag{3}$$

где$x_{kl}^{(i,j)}$ – часть потока данных, идущая через линию (k,l).

Кроме анализа времени задержки результаты сравниваются по проценту загруженности серверов услуг запросами и количеству обрабатываемых данных.

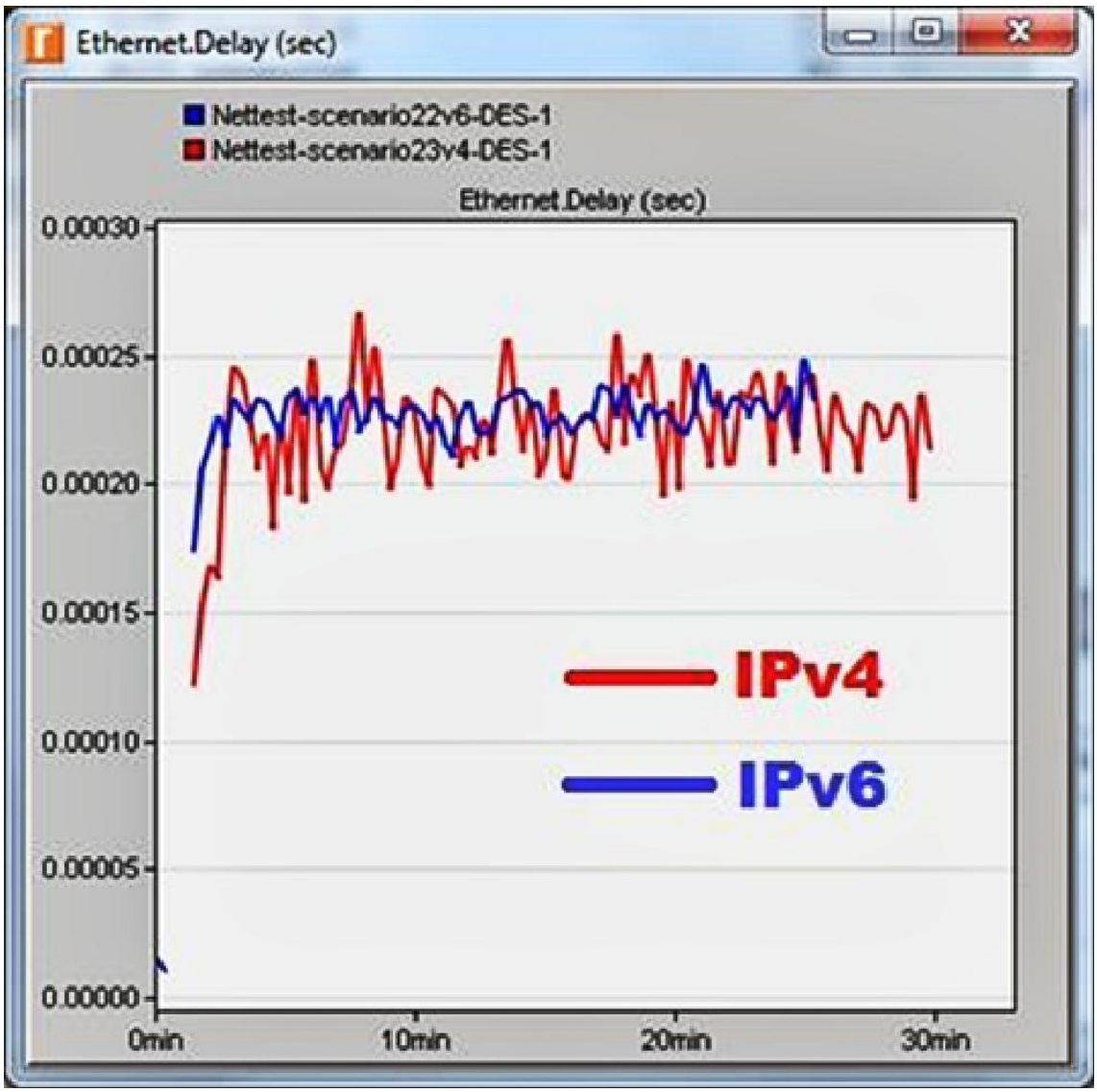

Рисунок 3.4 – Скорость прохождения первой сети пакетами IPv4 и IPv6

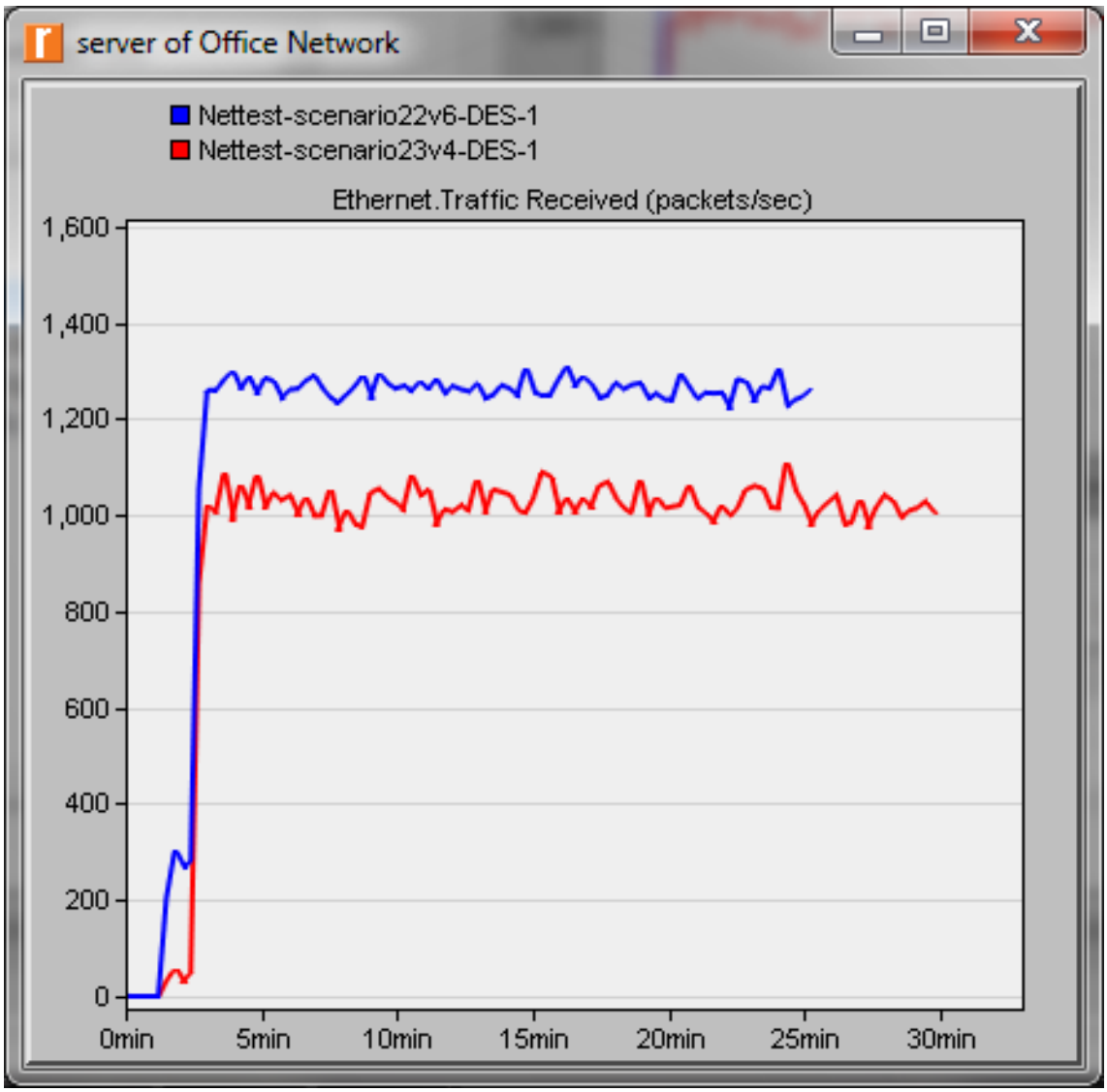

Рисунок 3.5 – Пакеты, обрабатываемые на сервере первой сети

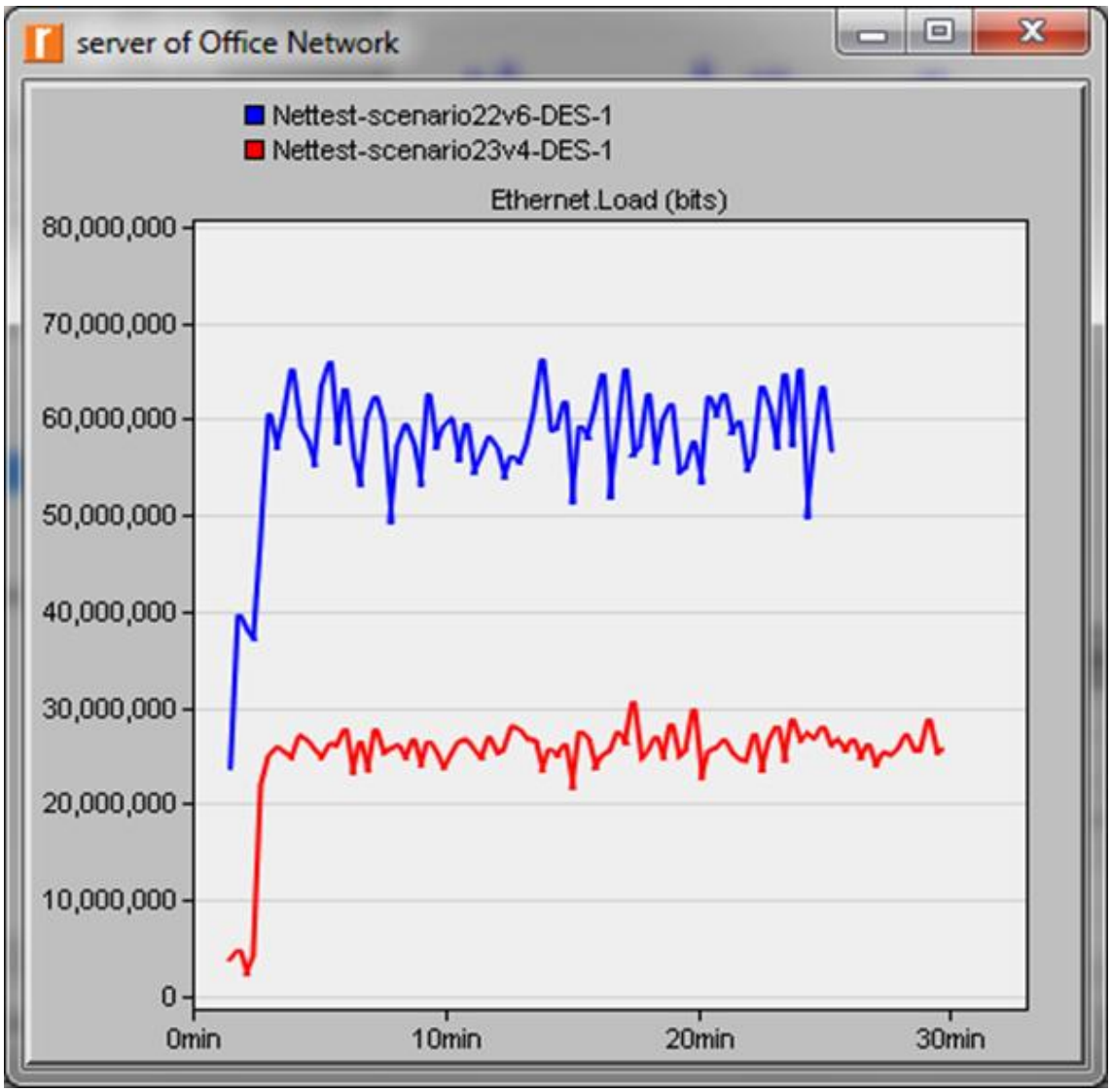

Рисунок 3.6 –Загрузка сервера первой сети в битах

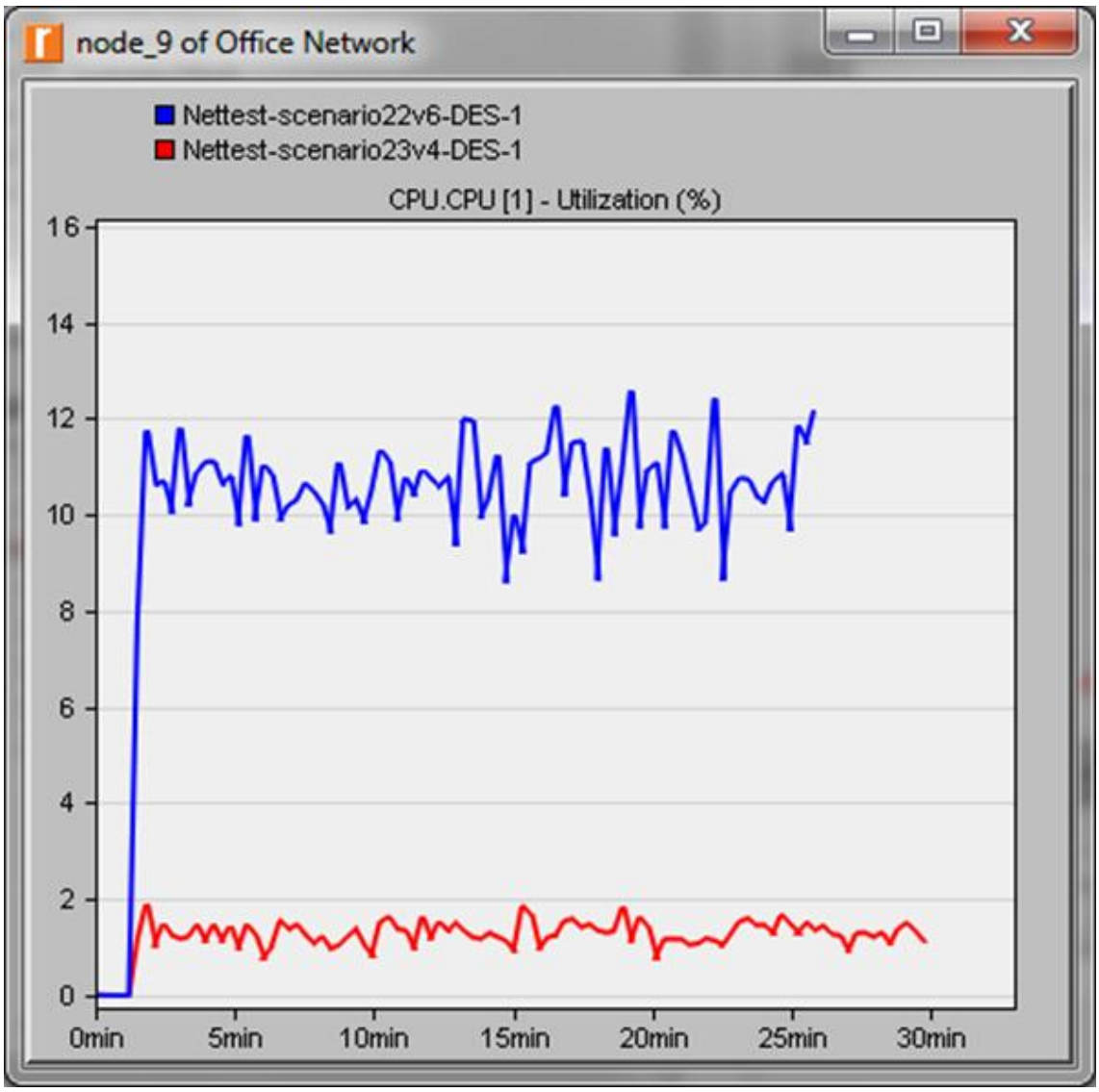

Рисунок 3.7 –Нагрузка на роутер в первой сети

По графикам на рисунке 3.4 мы можем увидеть, сколько времени нужно пакетам протоколов IPv4 и IPv6 на прохождение всего пути через сеть, представленную в модели, в секундах. Можно сделать вывод, что для небольших сетей разница в применении разных протоколов несущественно влияет на время, которое пакет находится в сети. Модель сети, настроенная для работы с протоколом четвертой версии в некоторых местах графика работает даже быстрее, чем модель, настроенная для работы с протоколом шестой версии.

Роутер имеет возможность пропустить через себя нужное количество данных не сильно увеличивая время прохождения пакета из-за того, что

обрабатывает его. Но из графиков на рисунке 3.6, показывающем загрузку процессора сервера, отвечающего за организацию серверов и обработку запросов к нему, видно, что использование протокола шестой версии гораздо больше ресурсоемко, чем использование протокола четвертой версии. Хотя, из рисунка 3.5 можно заметить, что разница в количестве обрабатываемых пакетов малосущественна.

Это происходит потому, что когда разрабатывался протокол шестой версии, то его создателями принимались во внимание более современный уровень развития инфокоммуникационных технологий, в которых существует возможность отправлять более крупные информационные пакеты. Это позволяет уменьшить количество отправляемых пакетов, но значительно увеличивается нагрузка на процессор роутера, что можно увидеть на рисунке 3.7.

Вторая (рисунок 3.8), модель сложнее первой имеет в два раза больше подключенных компьютеров, а так же дополнительный маршрутизатор. По плану, увеличение сети увеличит время прохождения пакета через сеть, нагрузку на роутер и сервера.

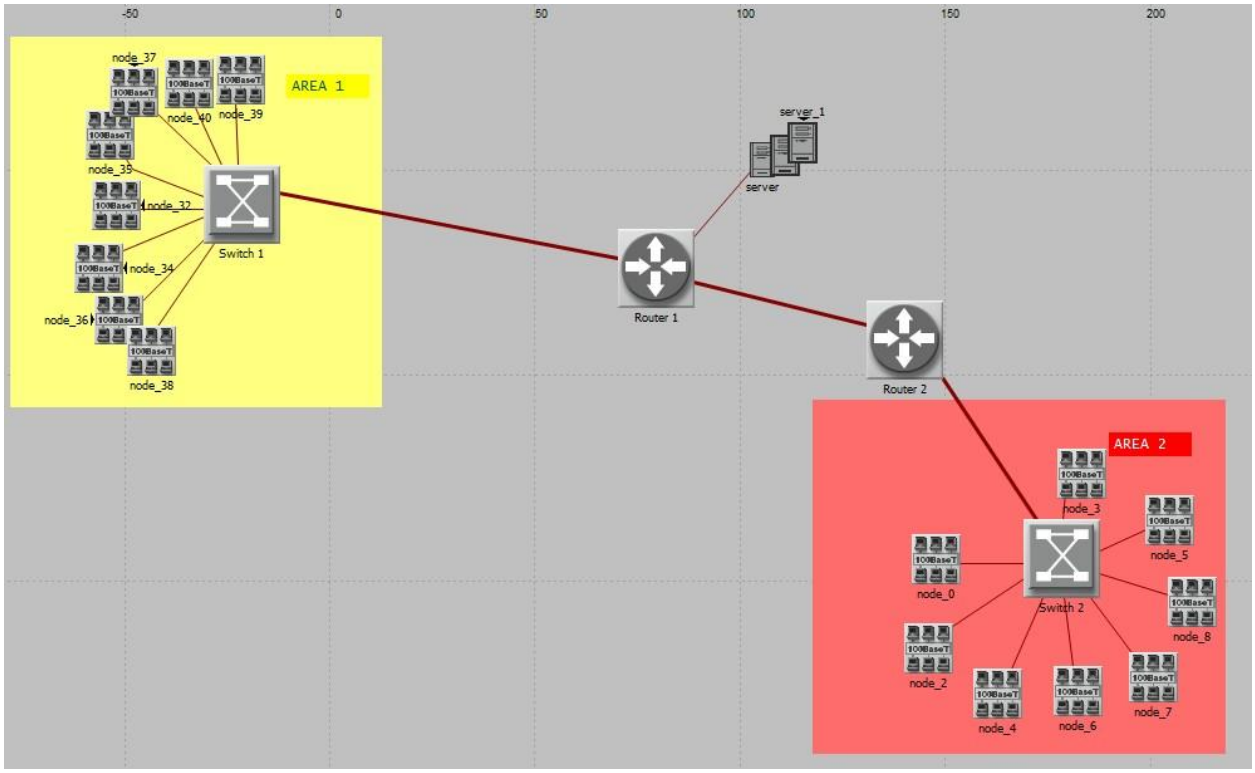

Рисунок 3.8 – Модель второй сети

Так же как и в первой сети проводились исследования и анализ работы сети, сначала настроенной на протокол четвертой, а затем протокол шестой версии, и получены данные, представленные на графиках ниже.

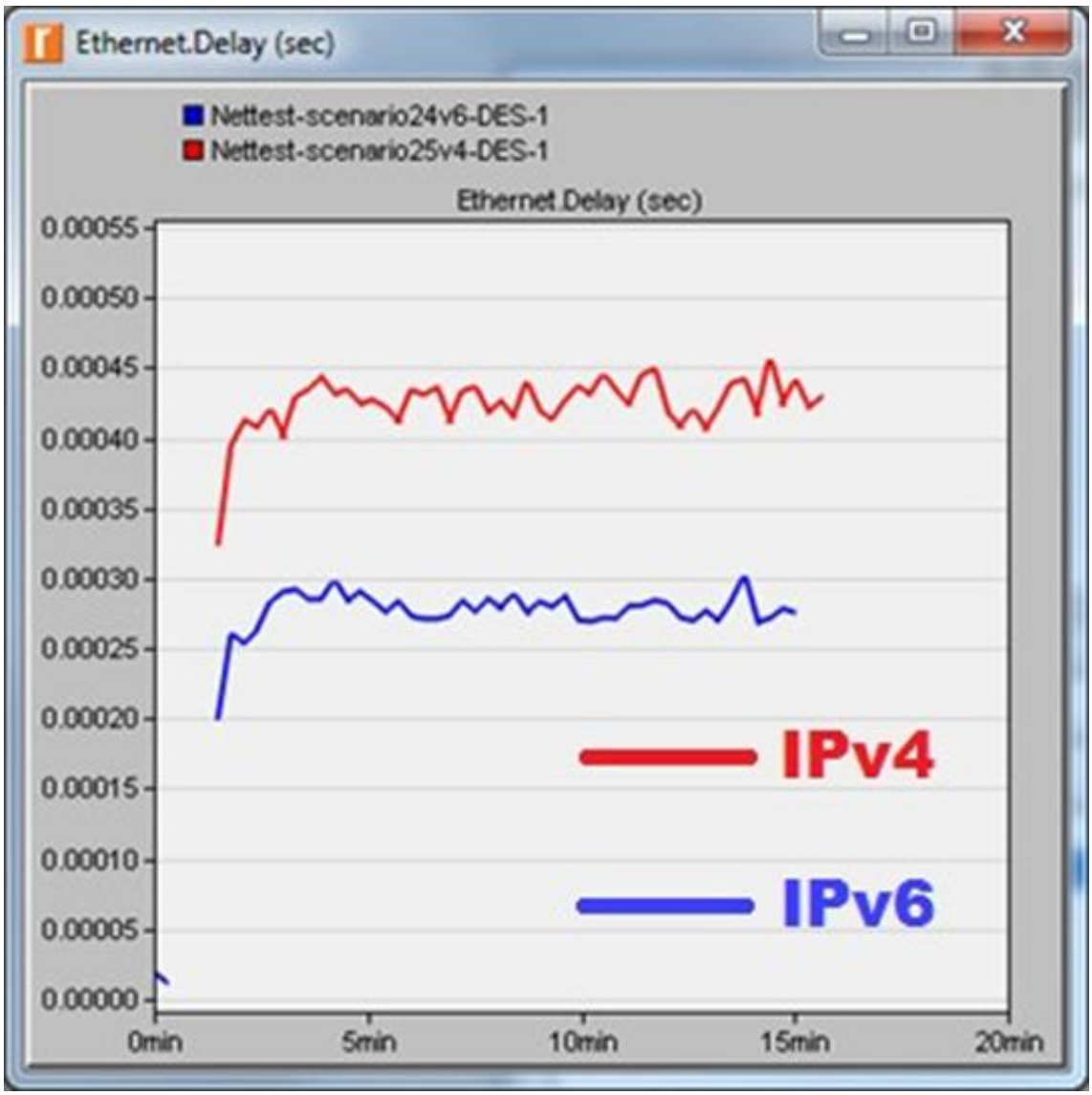

Рисунок 3.9 – Скорость прохождения второй сети пакетами IPv4 и IPv6

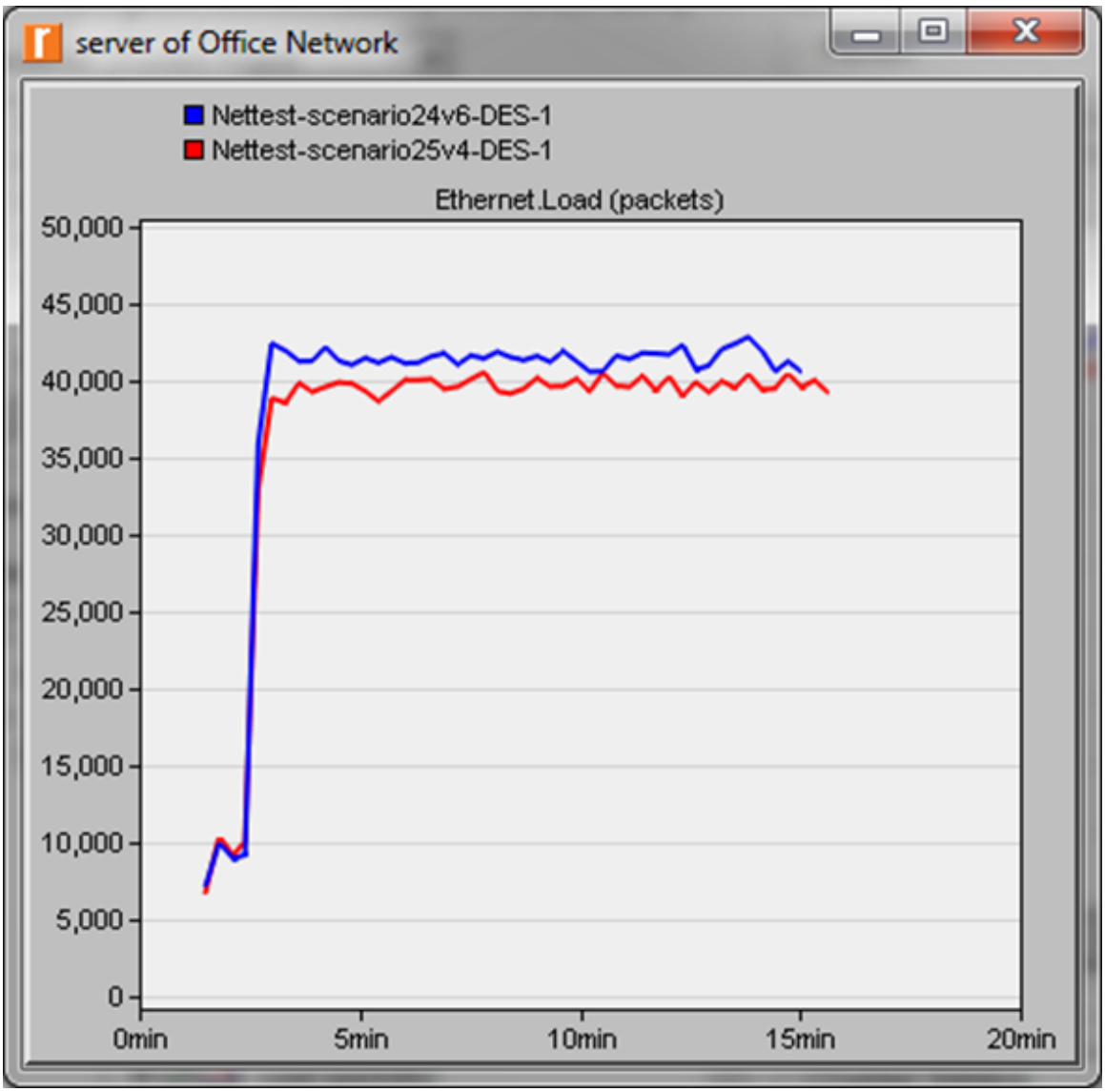

Рисунок 3.10 – Пакеты, обрабатываемые на сервере второй сети

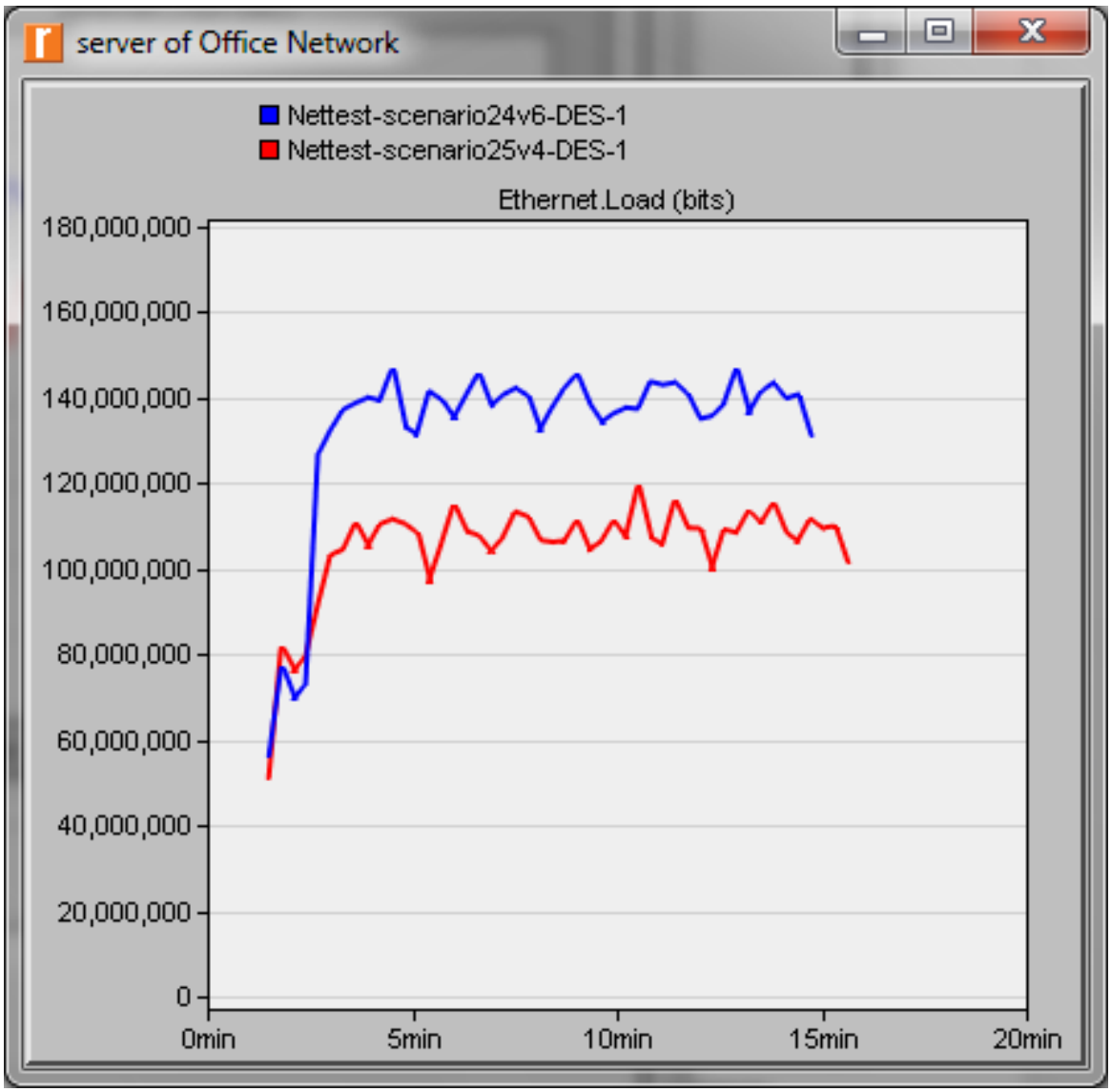

Рисунок 3.11 –Загрузка сервера второй сети в битах

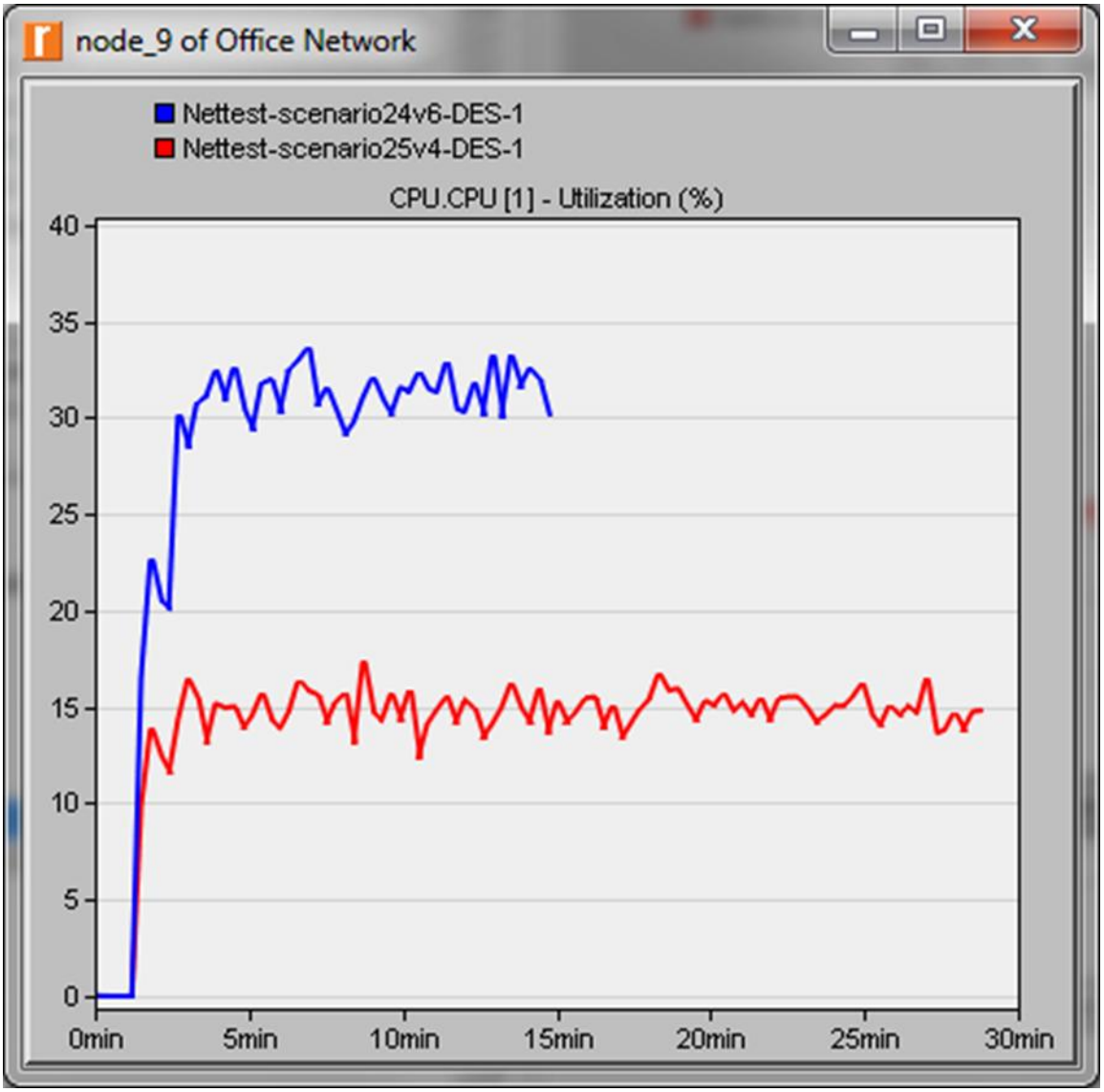

Рисунок 3.12 – Нагрузка на роутер 1 во второй сети

Как видно из рисунка 3.9 для протокола четвертого поколения значительно увеличилось время прохождения сети пакетом (с примерно 250 до 400-450 мкс). Это произошло из-за увеличения количества компьютеров в сети, а так же добавление второго роутера, обрабатывающего трафик. Но время, за которое пакет протокола шестой версии, доходит до адресата практически не увеличилось. В этой сети, сконфигурированной под протокол IPv6, трафик достигает цели практически в два раза быстрее, чем, если ее настроить на применение протокола четвертого поколения.

Это происходит, во первых, благодаря тому что в более современном протоколе интернета – в оптимизации заголовка пакета данных. В результате уменьшения числа полей, их количество сократилось до восьми, вместо четырнадцати у IPv4. Из заголовка пропали такие поля, как размер заголовка (потому что заголовок теперь имеет строгий размер в 40 байт), и поле контрольная сумма (которая теперь отсутствует в пакете, потому что протоколы более низких и более высоких уровней так же ведут расчет своих, поэтому в IPv6 ее убрали). Следовательно, роутеры не должны рассматривать пакет для нахождения длины заголовка или заново считать контрольную сумму когда изменяется время его жизни.

Все это ускоряет время, затрачиваемое процессором роутера на обработку одного пакета, что позволяет устройству пропустить через себя больший трафик за единицу времени.

В данной схеме при использовании протокола шестой версии происходит рост количества данных, которые проходят через процессор сервера. Сервисные серверы создают большие по размеру пакеты, что увеличивает количество полезных данных к их общему количеству.

Для дальнейших исследований была спроектирована третья модель, представленная на рис 3.13, которая включает в себя наибольшее возможное число устройств, которое допускает академическая версия приложения RiverbedModeler. Количество компьютеров удвоилось относительно второй схемы и выросло в четыре раза относительно первой. Так же добавился роутер номер 3, последовательно подключенный к первому. К первому роутеру по прежнему подключены несколько серверов, которые предоставляют абонентам доступ к разным сервисам.

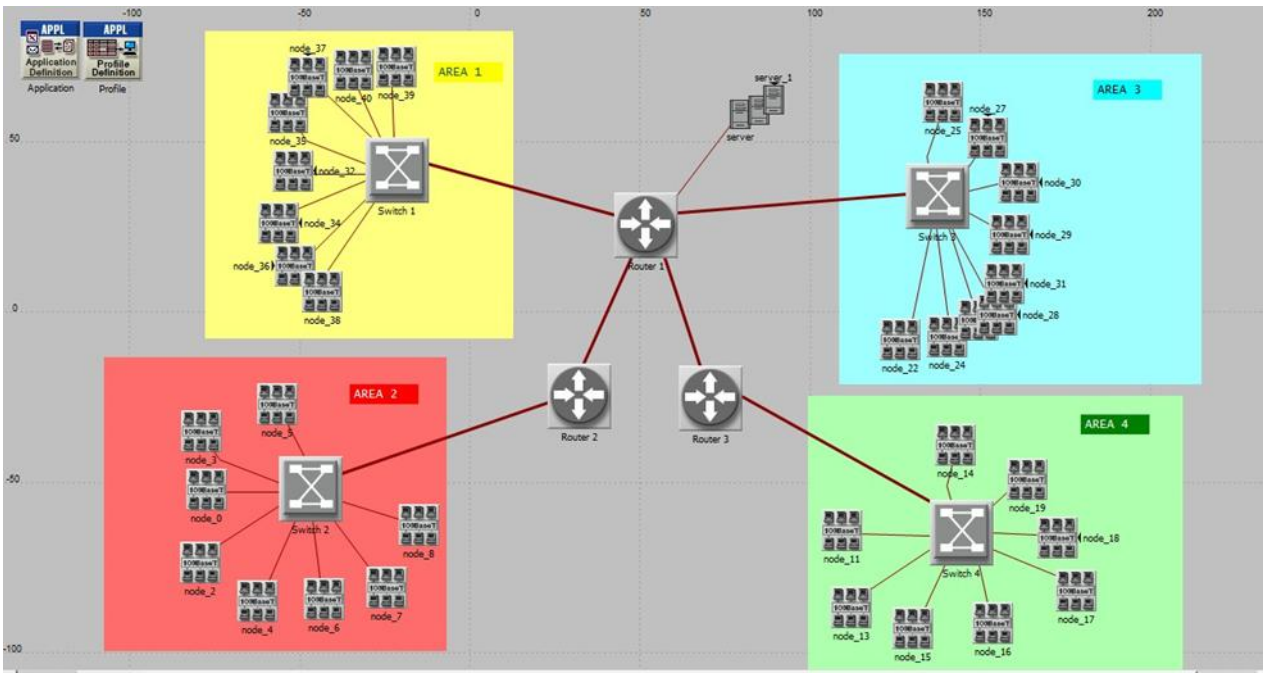

Рисунок 3.13 – Модель третьей сети

Увеличение числа абонентов приводит к значительному увеличению потребления ресурсов сети – времени обработки пакетов роутерами, нагрузку на процессоры серверов. Это приводит к появлению больших задержек в работе сети.

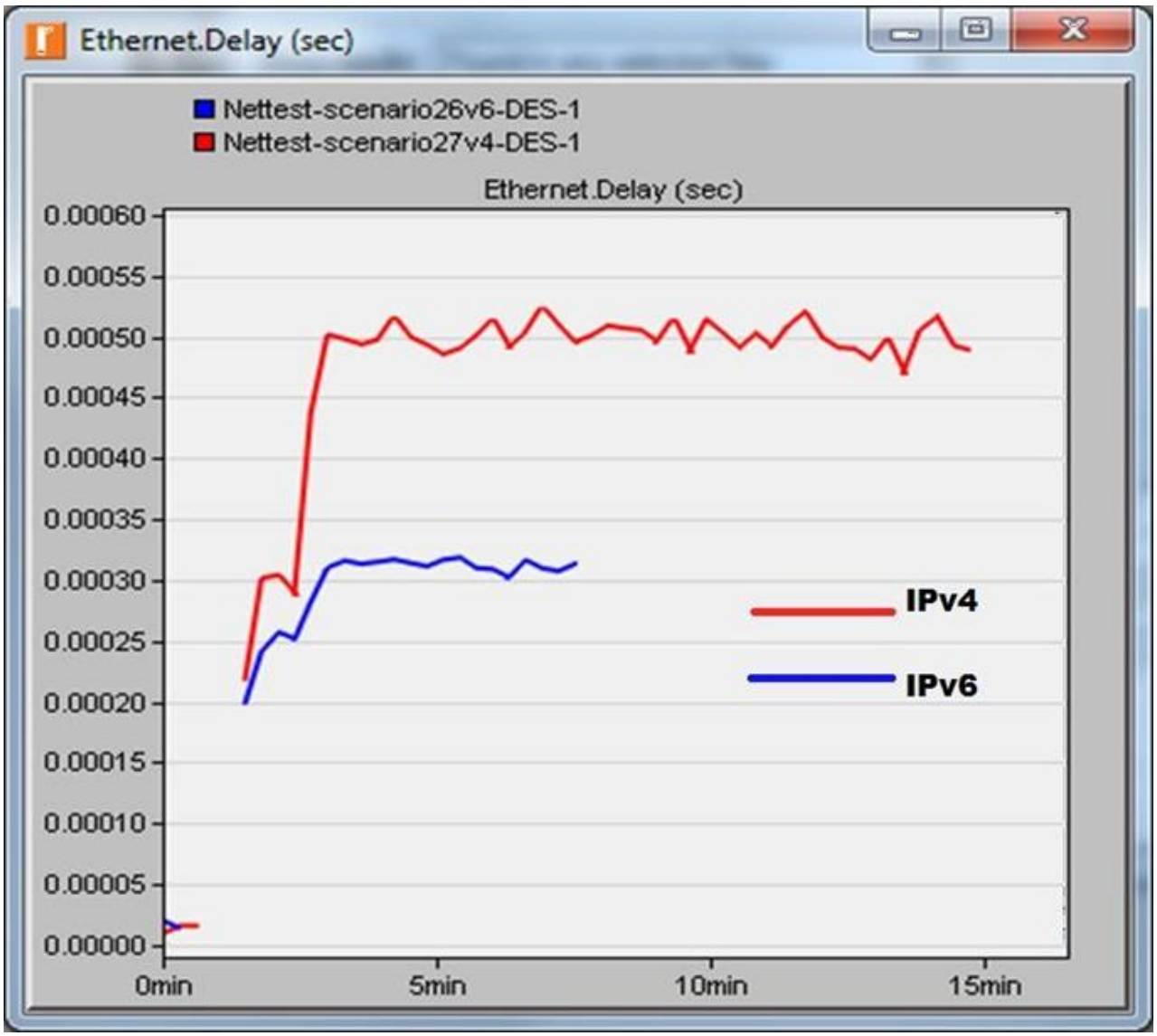

Рисунок 3.14 – Скорость прохождения второй сети пакетами IPv4 и IPv6

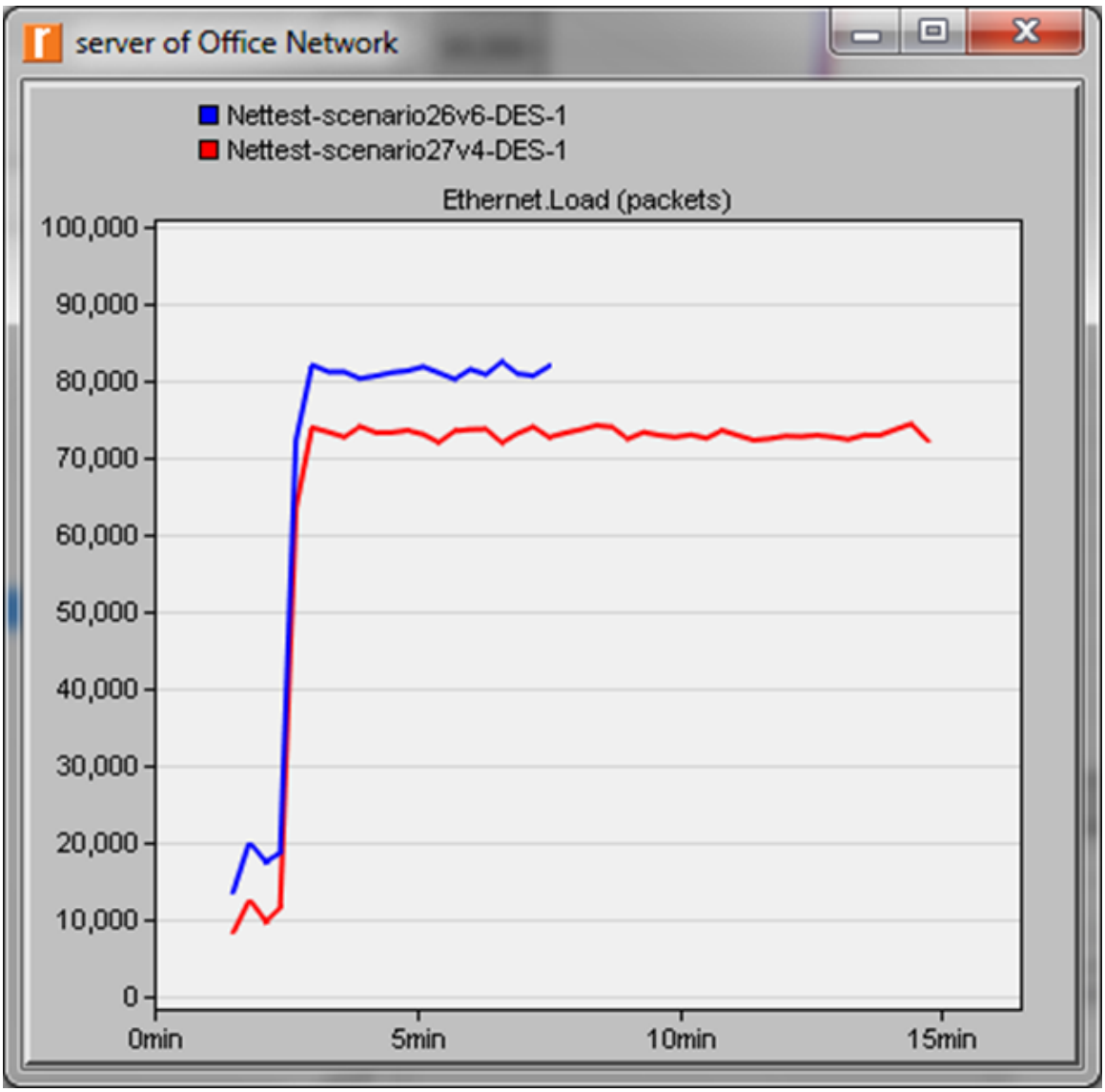

Рисунок 3.15 – Пакеты, обрабатываемые на сервере третьей сети

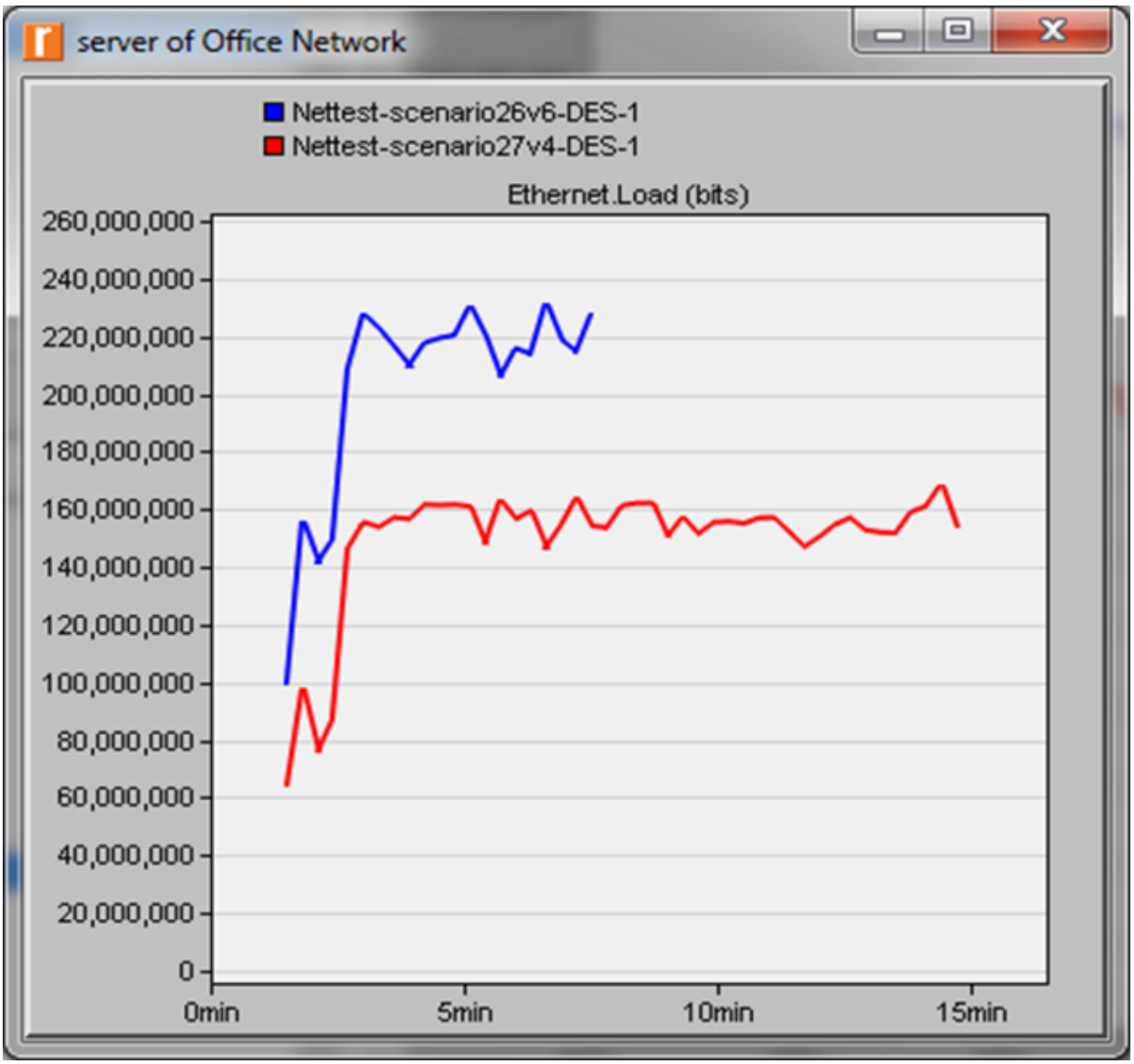

Рисунок 3.16 – Загрузка сервера третьей сети в битах

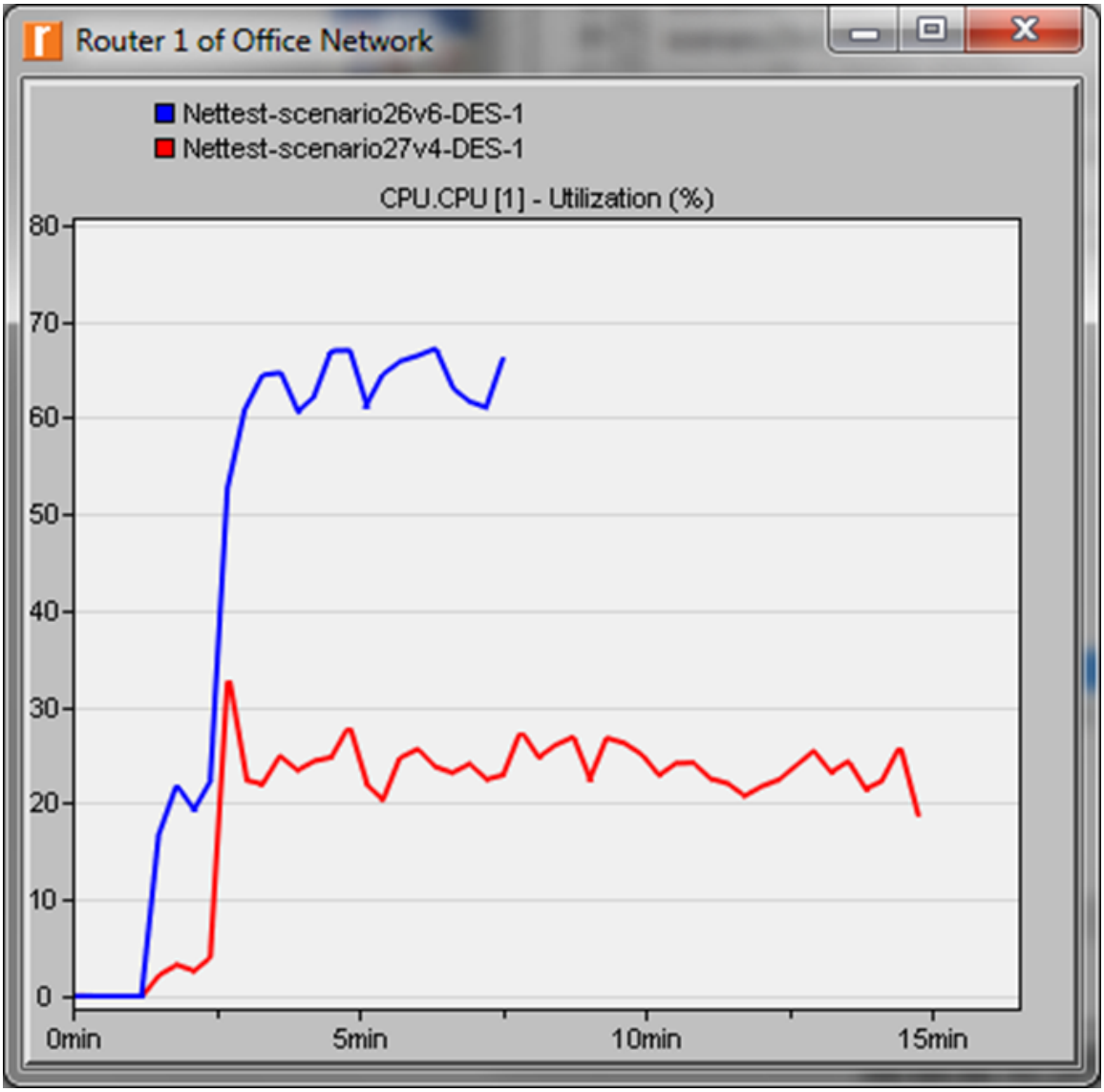

Рисунок 3.17 – Нагрузка на роутер 1 в третьей сети

Анализ работы этой модели сети дает четко понять, что при использовании протокола интернета четвертой версии в случае увеличения числа компьютеров в сети в несколько раз в разы увеличивается и задержка при прохождении информации через сеть. Протокол шестой версии в этом плане показывает гораздо лучшие показатели при тех же условиях. Однако, как видно из рисунка 3.17, при применении IPv6 существенную роль стала играть мощность роутера. На графике видно, что использование процессора первого роутера сети превысило 60 %. В случае еще одного удвоения количества абонентов, мощности процессора роутера будет уже недостаточно. IPv4 в этом плане выглядит значительно лучше.

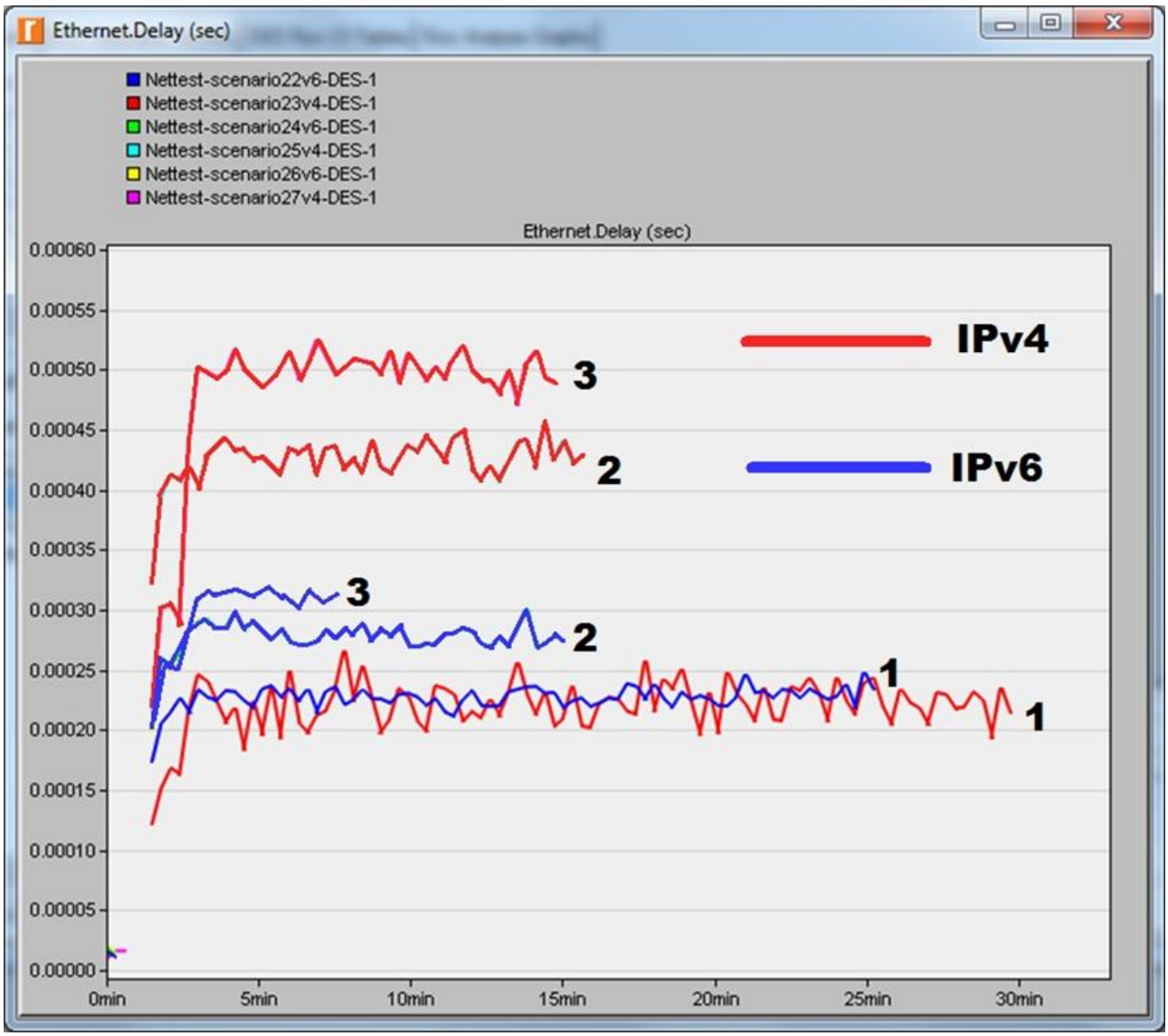

Рисунок 3.18 – Сравнение графиков времени прохождения пакетов трех сетей.

На рисунке 3.18 можно увидеть, как зависит время прохождения пакета через сеть от ее размера. По этим графиком можно сделать заключение, что использование более нового протокола дает большое преимущество при увеличении количества абонентов и размеров сети.

3.2 Исследование сети, разделенной на виртуальные каналы

В этой части работы будет произведен анализ работы сети, разделенной на виртуальные локальные сети для предоставления различных услуг.

В сети есть в наличии обычные потоки различных услуг:

– обычный трафик Интернета;
– сервисы голосовой и видео связи;
– широковещательное телевидение;
– VoD-сервисы;
– музыкальные каналы и пр.

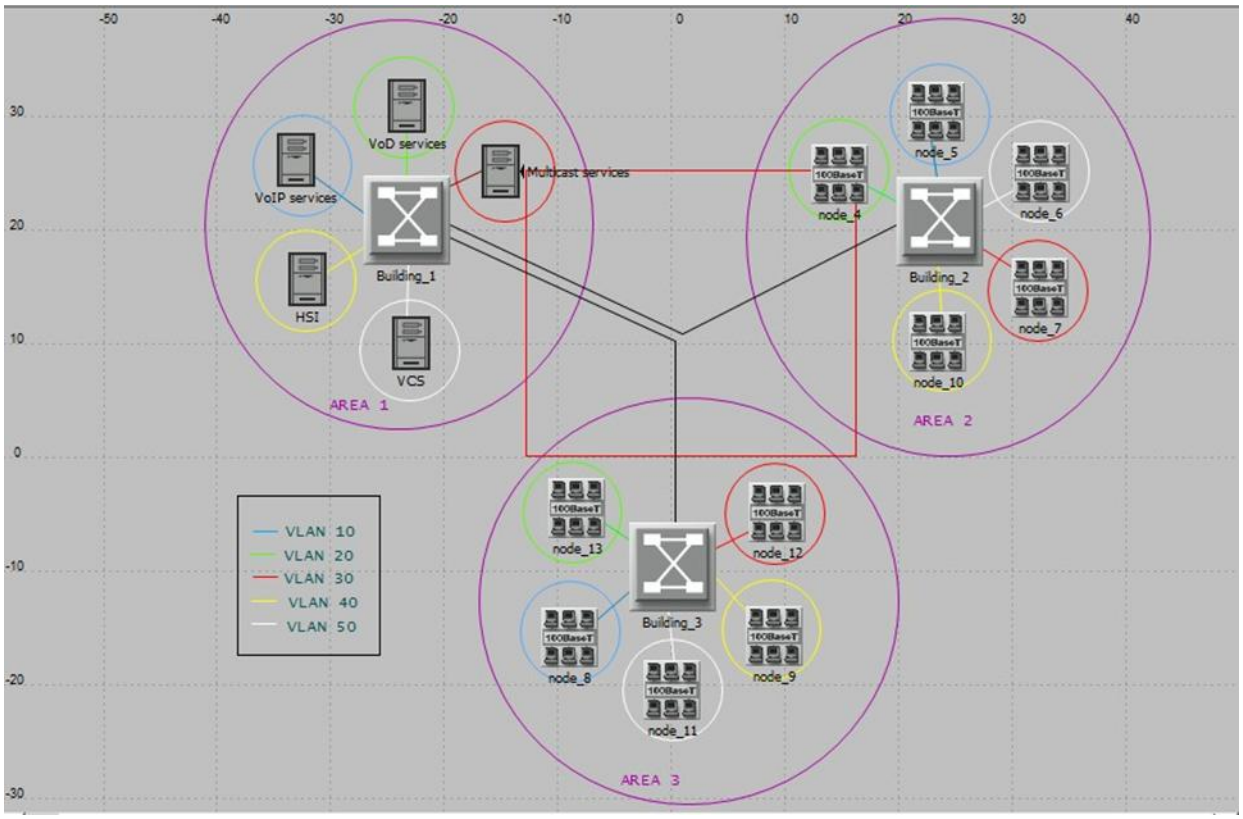

Рисунок 3.19 – Организация сети

В сети имеется три условных района, каждый из которых обслуживается своим роутером. В первом районе находятся сервера различных услуг, которыми пользуются абоненты двух других районов. На роутерах создаются каналы виртуальных сетей между абонентскими устройствами и серверами услуг. В

районах по тысяче пользователей, подключенных к различным услугам. Данный метод имеет большое преимущество по сравнению с передачей данных в общем потоке. Применение разных каналов виртуальных сетей для разных услуг позволяет немного уменьшить нагрузку на роутеры, снизив количество служебной информации, используемой при передаче данных.

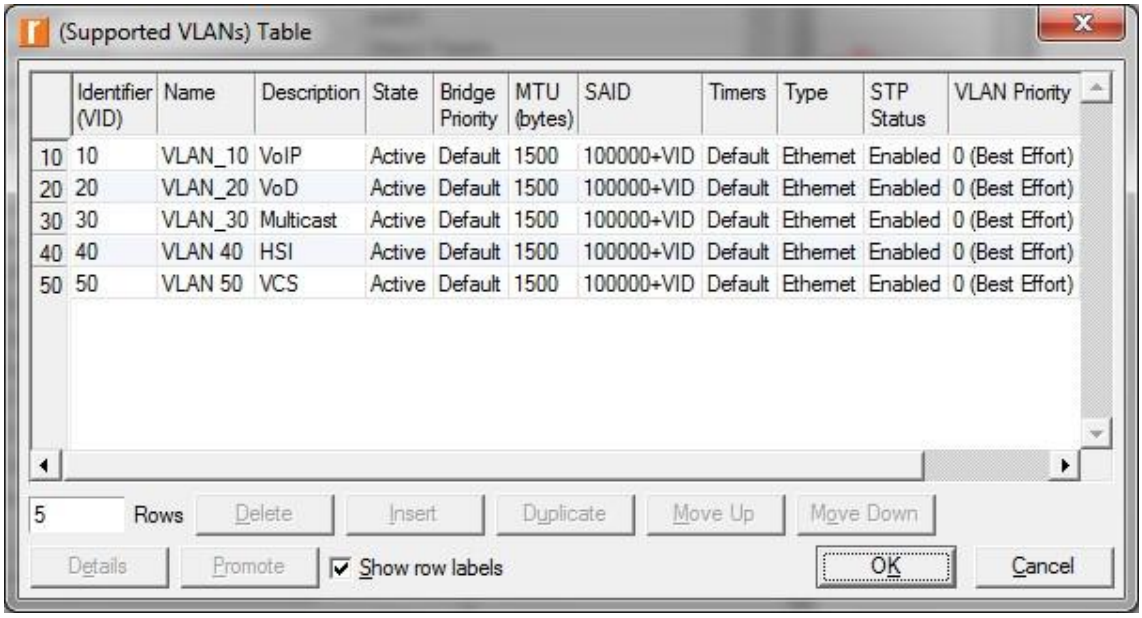

Рисунок 3.20 – Таблица настроек виртуальных сетей на первом роутере

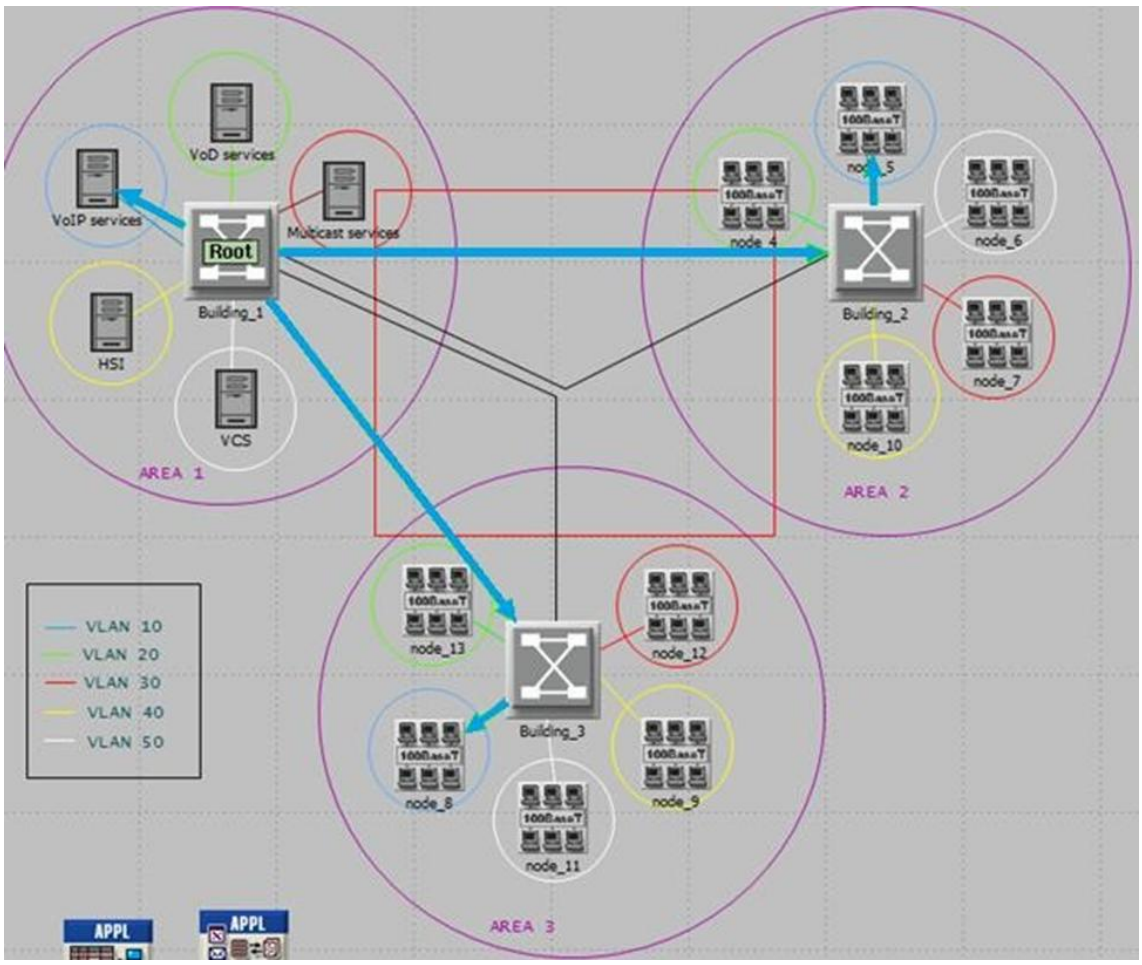

Рисунок 3.21 – Канал IP-телефонии между двумя абонентами

Для проведения анализа была построена модель сети с пятью виртуальными каналами услуг. Так же были созданы каналы точка-точка между роутерами. Моделирование продолжалось в течение минуты, сначала с использованием каналов виртуальных сетей, потом без них.

Ниже представлены полученные результаты – время пути пакета между двумя точками сети и нагрузка на роутерах в зависимости от принятых данных во время работы модели.

По графикам на рисунке 3.22 видна разница во времени прохождения пакетов. Можно увидеть что сеть с виртуальными каналами работает на 25% лучше, чем без них. Так же из рисунков 3.23, 3.24, 3.25, на которых изображены графики прохождения информации через роутеры, так же видно снижение нагрузки на оборудование при использовании каналов виртуальных сетей.

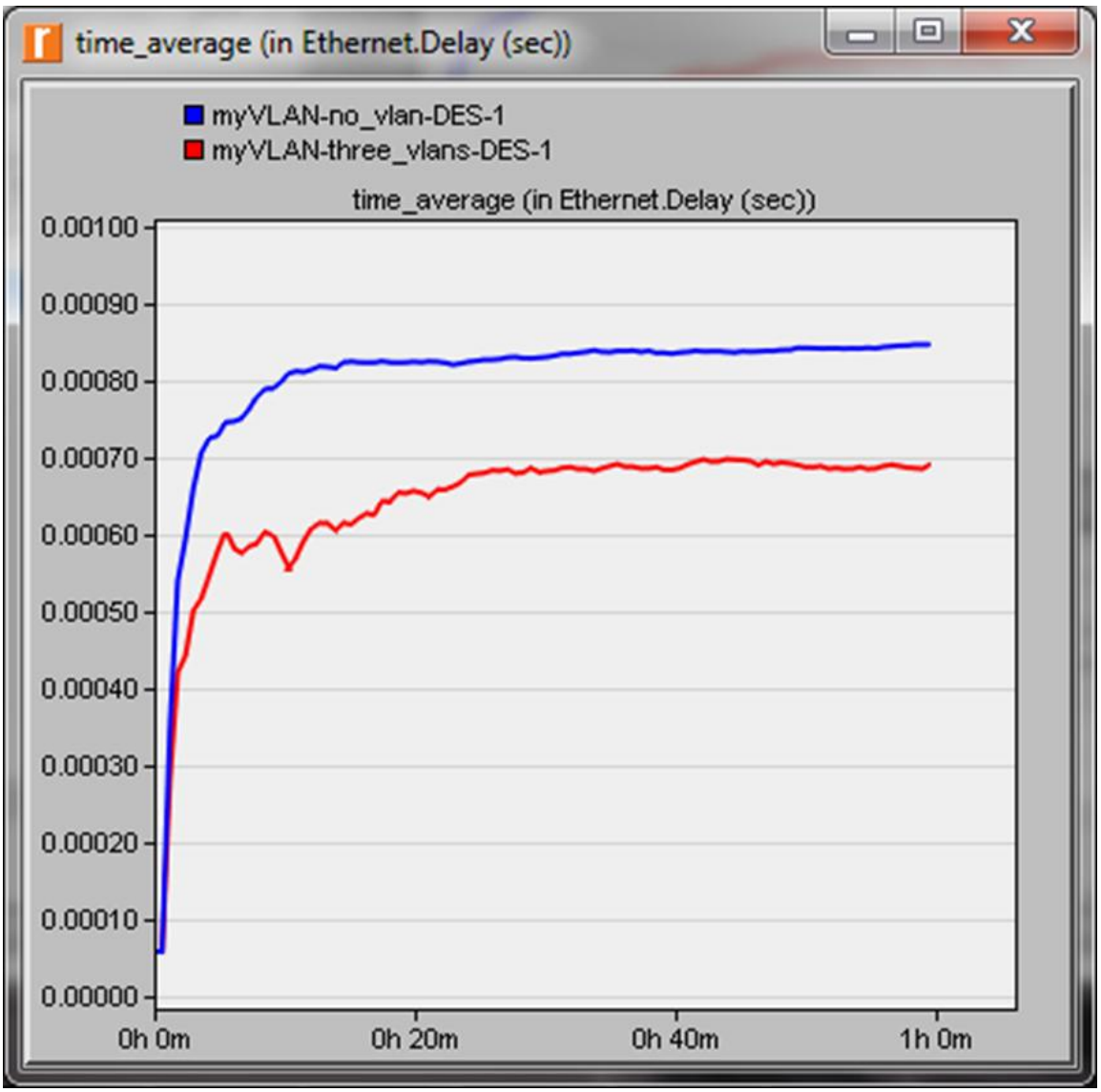

Рисунок 3.22 – Скорость прохождения пакетов
с виртуальными каналами и без них

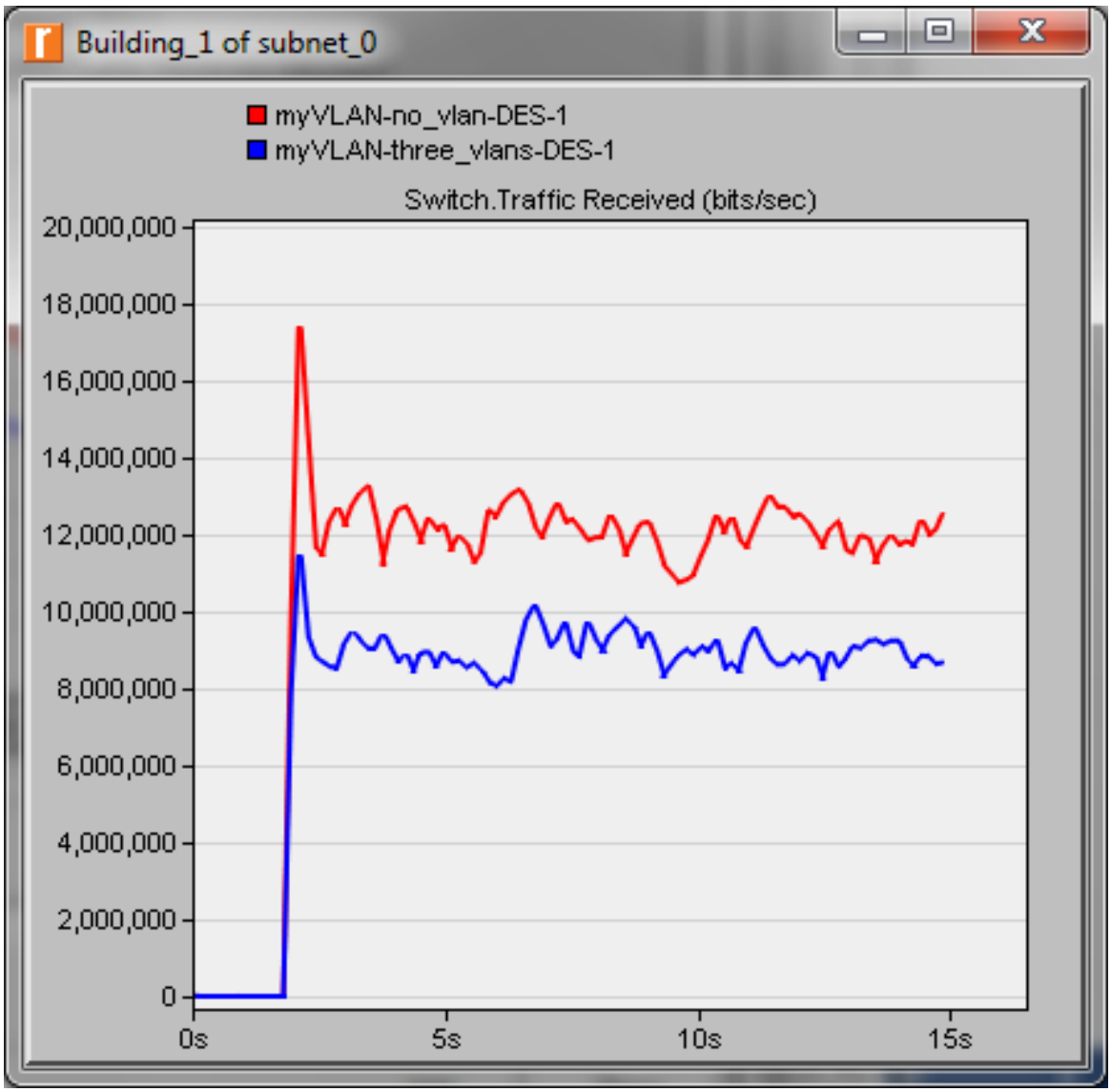

Рисунок 3.23 – Информация, прошедшая через роутер 1 с использованием виртуальных каналов и без них

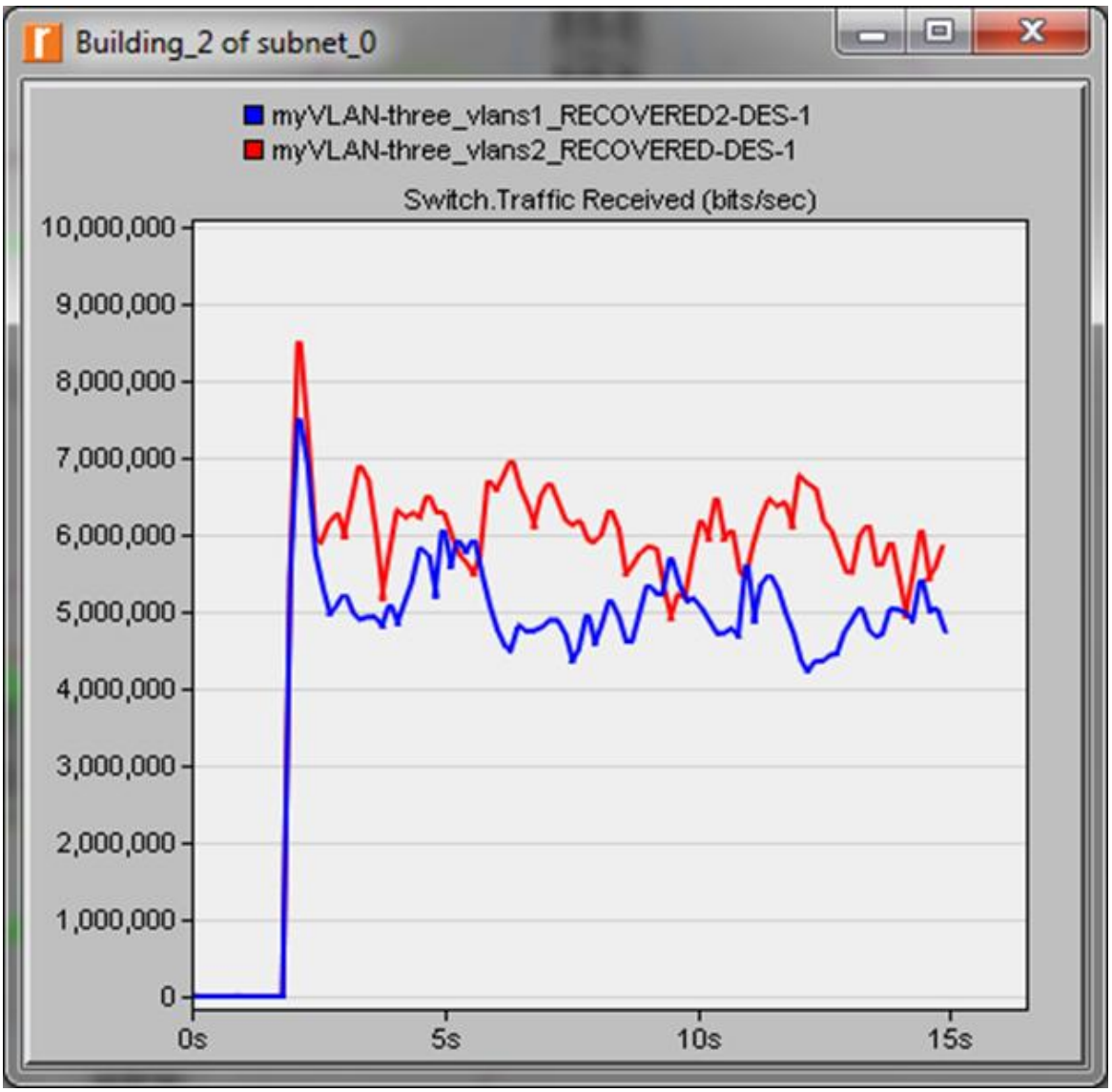

Рисунок 3.24 – Информация, прошедшая через роутер 2 с использованием виртуальных каналов и без них

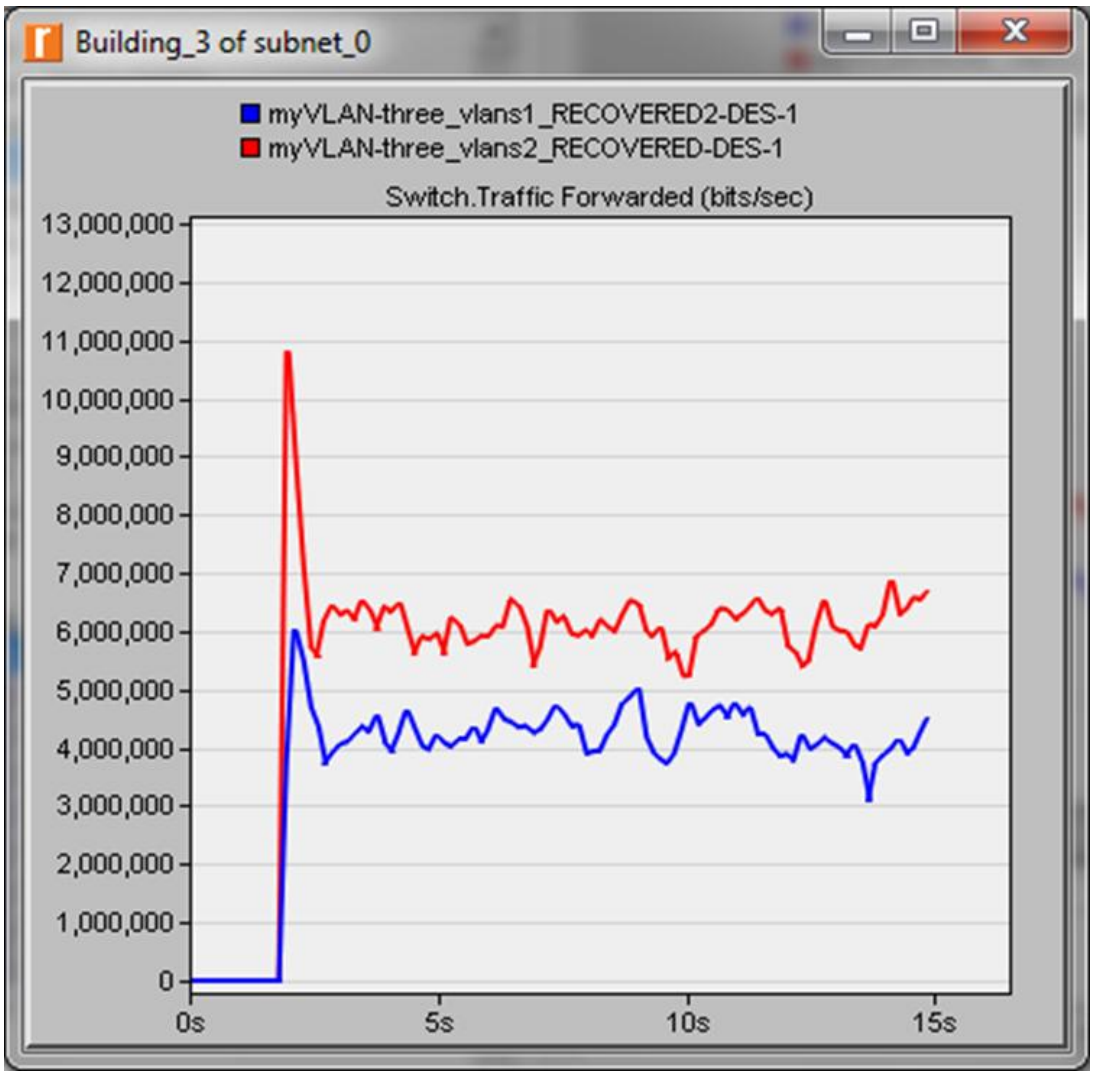

Рисунок 3.25 – Информация, прошедшая через роутер 3 с использованием виртуальных каналов и без них

Из рисунков выше мы можем видеть, что уменьшились нагрузка на роутеры и время прохождения пакетом сети. Это происходит потому что, в связи с отсутствием необходимости отправки широковещательных пакетов на все устройства, трафик в сети значительно уменьшается. Отправка широковещательных пакетов ограничена пределами одной виртуальной сети.

В результате работы моделей сетей мы можем видеть, что, при применении разделения реальной сети на виртуальные, сильно снижает количество данных, одновременно находящихся в сети, уменьшает время нахождения пакета в сети и его задержку. Все это положительно влияет на общую работу сети.

ЗАКЛЮЧЕНИЕ

При выполнении выпускной квалификационной работы в пакете программ RiverbedModeler были разработаны модели нескольких сетей связи условного жилого района, позволяющие симулировать поведение сетей связи при различных событиях, оценивать их характеристики (такие, как пропускная способность, задержки в прохождении пакета, нагрузка на роутеры и т.д.).

Используя созданные модели инфокоммуникационных сетей были проведены исследования и проанализированы полученные данные по оценке работы сетей, настроенных на использование протокола различных версий. Также была проанализирована работа сети (нагрузка, создаваемая на ее узлы), в которой применяется технология каналов виртуальных локальных сетей.

Получены следующие результаты выпускной квалификационной работы:

- проведены изучения работы сетей и получены их характеристики при использовании межсетевого протокола четвертой и шестой версий;
- сделан вывод, что протокол шестой версии имеет значительно меньшее время прохождения пакета, чем протокол четвертой версии;
- пакет шестой версии межсетевого протокола содержит большее информации, чем пакет четвертой версии;
- получены характеристики сети, использующей виртуальные каналы для различных услуг;
- результат моделирования показал, что применение технологии виртуальных каналов значительно снижает нагрузку на маршрутизаторы.

По результатам моделирования можно подытожить, что использование межсетевого протокола шестой версии увеличивает пропускную способность сети и ускоряет ее работу. IPv6 лучше IPv4 по многим показателям. Но нужно отметить, что в небольших сетях, настроенных по протоколу четвертой версии, нет отличий в скорости по сравнению с сетями, настроенными по протоколу

шестой версии, но в первых наблюдается гораздо меньшая загруженность сетевых коммутаторов. Применение виртуальных локальных услуг для передачиданных по виртуальным каналам снижает нагрузку на активные сетевые элементы и на всю сеть соответственно, позволяя передавать больше информации при тех же физических параметрах сети.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Камер, Д. Э. Сети TCP/IP, том 1. Принципы, протоколы и структура — М.:«Вильямс», 2003. — 880с.

2. Семенов, Ю. А. Протоколы Internet. — 2-е изд., стереотип.. — М.: Горячая линия - Телеком, 2005. — 1100с.

3. Общее описание RFC 793,1981

4. Общее описание RFC 791,1981

5. Новиков,Ю.В.,Основылокальныхсетей:курслекций:учеб.пособие : для студентов вузов, обучающихся по специальностям в обл. информ. технологий / Ю. В. Новиков, С. В. Кондратенко. — М.: Интернет — Ун-т Информ. Технологий, 2005. - 360с.

6. Олифер, В. Г., Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов / В. Г. Олифер, Н. А. Олифер. — 4-е изд. — СПб.:Питер, 2010. — 944 с.:ил.

7. Гольдштейн, Б. С. Протоколы сети доступа: Учеб.пособие / Б. С. Гольдштейн. – М.: Радио и связь, 2005. – 292с.

8. Олифер В.Г., Основы сетей передачи данных: Учеб. пособие / В.Г.Олифер, Олифер Н.А. - Интернет-университет информационныхтехнологий – ИНТУИТ.ру, 2005. –176с.

9. Ногл, М. TCP/IP. Иллюстрированный учебник М.: изд-во ДМК Пресс, 2001 — 480с.

10. Фейт, С. TCP/IP Архитектура, протоколы, реализация (включая IP версии 6 и IP Security) – Изд.: Лори, 2000 –424

11. Берлин,А.Н.ОсновныепротоколыИнтернет–Изд.:Бином,2013- 504

12. ОписаниепрограммногопродуктаRiverbedModelerwww.riverbed.com - официальный сайт компании Riverbedhttp://www.riverbed.com/gb/products/steelcentral/steelcentral-riverbed-modeler.html

13. Семенов,Ю.А.Алгоритмытелекоммуникационныхсетей.Часть1,и 3. - изд.: Национальный Открытый Университет "ИНТУИТ" 2016 - 832

14. Герасименко Сети и телекоммуникации. Учебное пособие / Б. В. Соболь, А. А. Манин – изд.: Феникс, 2015 г. –191

15. Хант К. TCP/IP. Сетевое администрирование – Изд.: Символ- Плюс, 2007 –816

16. Средства информационного взаимодействия в современных распределенных гетерогенных системах / Р.Э. Асратян, В. Н. Лебедев; Изд.: Ленанд, 2009 – 130стр.

17. www.overclockers.ru - информационныхсайт