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 ЭФФЕКТИВНОСТИ РАБОТЫ МУЛЬТИСЕРВИСНОЙ СЕТИ СВЯЗИ С ПОМОЩЬЮ СРЕДСТВ ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ

Магистерская диссертация
Золотарь Николая Ивановича

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

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

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

БЕЛГОРОД 2016

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Интенсивное развитие информационных технологий и сетей связи привело к созданию и внедрению современных инфокоммуникационных сетей связи поддерживающих широкий спектр услуг практически все сферы деятельности человека. Поэтому на сегодняшний день сети связи различных организаций, а также мультисервисные сети микрорайонов, могут достигать достаточно больших размеров, поддерживать широкий спектр услуг и иметь хорошую масштабируемость. Такая организация сетей не возможна без объединения большого количества активных сетевых устройств в отдельные сетевые сегменты, что в свою очередь приводит к появлению большого объема служебного трафика в сети, вызывающего дополнительные задержки трафика, увеличения времени пребывания пакетов в сети и сложности администрирования таких сетей. Зачастую стремления операторов связи к увеличению эффективности работы мультисервисных сетей сводиться к оптимизации таких параметров как пропускная способность, время задержки пакета в сети, загрузка серверов, скорости работы узлового сетевого оборудования. На сегодняшний день данная задача решается за счет применение новых технологий таких как организация виртуальных локальных сетей VLAN и использование протокола IPv6 позволяющие увеличить эффективность работы сети. Однако, не все новые подходы могут быть достаточно эффективными в том или ином случае. Таким образом, для того чтобы решить применять ту или иную технологию в инфокоммуникационных сетях в конкретном случае прибегают к имитационному моделированию, которое позволят на ранней стадии проектирования или сетевой

В данной работе поставлена цель, провести исследование эффективности работы мультисервисной сети связи с точки зрения времени задержки пакетов, пропускной способности, загрузке сетевых узлов, с помощью средств имитационного моделирования при внедрении технологий VLAN и IPv6.

Для решения поставленной цели необходимо решить ряд поставленных задач:

1. Провести анализ существующих средств имитационного моделирования сетей связи.

2. Осуществить оценка параметров мультисервисной сети с помощью средств имитационного моделирования.

3. Исследовать характеристики и значения параметров мультисервисной сети связи при различных конфигурациях сети и типов услуг при использовании технологии VLAN.

4. Исследовать характеристики и значения параметров мультисервисной сети связи при различных конфигурациях сети и типов услуг при использовании протокола IPv6.

Магистерская диссертация состоит из введения, трех глав, заключения, списка использованных источников. Текст магистерской диссертации изложен на 64 листах машинописного текста, включающий 38 рисунков, 6 таблиц и списка литературы из 63 названий.

Глава 1. ТЕХНОЛОГИИ ИСПОЛЬЗУЕМЫЕ В ОБЪЕКТЕ ИССЛЕДОВАНИЯ

1.1 Протокол IPv4

Протоколы, эквивалентные третьему уровню модели OSI, определяют то, как пакеты доставляются от компьютера, который их создал к компьютеру, который должен получить. В современных сетях единственным широко используемым протоколом третьего уровня является стек протоколов TCP/IP, а по большей части это протокол IP (Internet Protocol, межсетевой протокол). Неотъемлемой частью IP является IP-адрес. IP-адреса (Internet Protocol version 4, интернет протокол версии 4) – это наиболее распространенный тип адресов, который используется на сетевом уровне модели OSI, для осуществления передачи пакетов между сетями. IP-адреса состоят из четырех байт, к примеру 192.168.101.111 [1-3].

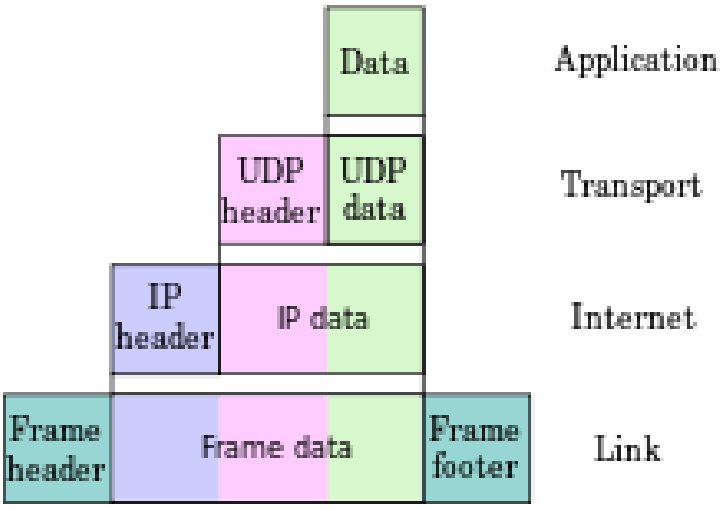

Рисунок 1.1 – Добавление частей заголовка пакета на каждом уровне OSI перед передачей его в сеть

IP-адреса присваиваются хостам двумя методами:

- вручную, настраивается системным администратором во время настройки вычислительной сети;

- автоматически, с использование специальных протоколов (в частности, с помощью протокола DHCP - Dynamic Host Configuration Protocol, протокол динамической настройки хостов).

Протокол IPv4 был разработан в сентябре 1981 года, как часть IP-протокола, с целью присвоить адрес каждому устройству в сети, чтобы передавать пакеты непосредственно адресату [4].

Основной задачей протокола IPv4 является осуществление передачи блоков данных (дейтаграмм) от хоста-отправителя, до хоста-назначения, где отправителями и получателями выступают вычислительные машины, однозначно идентифицируемые адресами фиксированной длины (IP-адресами). Также IP-протокол может выполнять, в случае необходимости, фрагментацию и сбор отправляемых дейтаграмм для передачи данных через другие сети с меньшим размером пакетов [5,7-9].

Недостатком протокола IP считают его ненадежность, из-за того, что при передаче не устанавливается соединение и не подтверждается доставка пакетов, не осуществляется контроль корректности полученных данных (с помощью контрольной суммы) и не выполняется операция квитирования (обмен служебными сообщения с узлом-назначения и его готовностью приема пакетов) [6].

Каждая дейтаграмма отправляется и обрабатывается протоколом IP отдельно, не учитывая другие дейтаграммы при передаче данных в сеть [7].

Отправитель не контролирует дальнейшие действия с дейтаграммой после того как она была отправлена протоколом IP. Если дейтаграмма, не достигнув адресата, не может быть передана дальше по сети по той или иной причине, она уничтожается. Узел, который уничтожил дейтаграмму, имеет возможность сообщить о причине сбоя отправителю, по обратному адресу (в частности с помощью протокола ICMP). Функция гарантированной доставки данных возложена на протоколы вышестоящего уровня (транспортный уровень), которые наделены для этого специальными механизмами (протокол TCP) [5-10].

Как известно, на сетевом уровне модели OSI работают маршрутизаторы. Поэтому, одной из самых основных задач протокола IP – это осуществление маршрутизации дейтаграмм, другими словами, определение оптимального пути следования дейтаграмм (с помощью алгоритмов маршрутизации) от узла-отправителя сети к любому другому узлу сети на основании IP адреса [1-10].

Алгоритм работы протокола IP на каком-либо узле сети принимающего дейтаграмму из сети выглядит следующим образом:

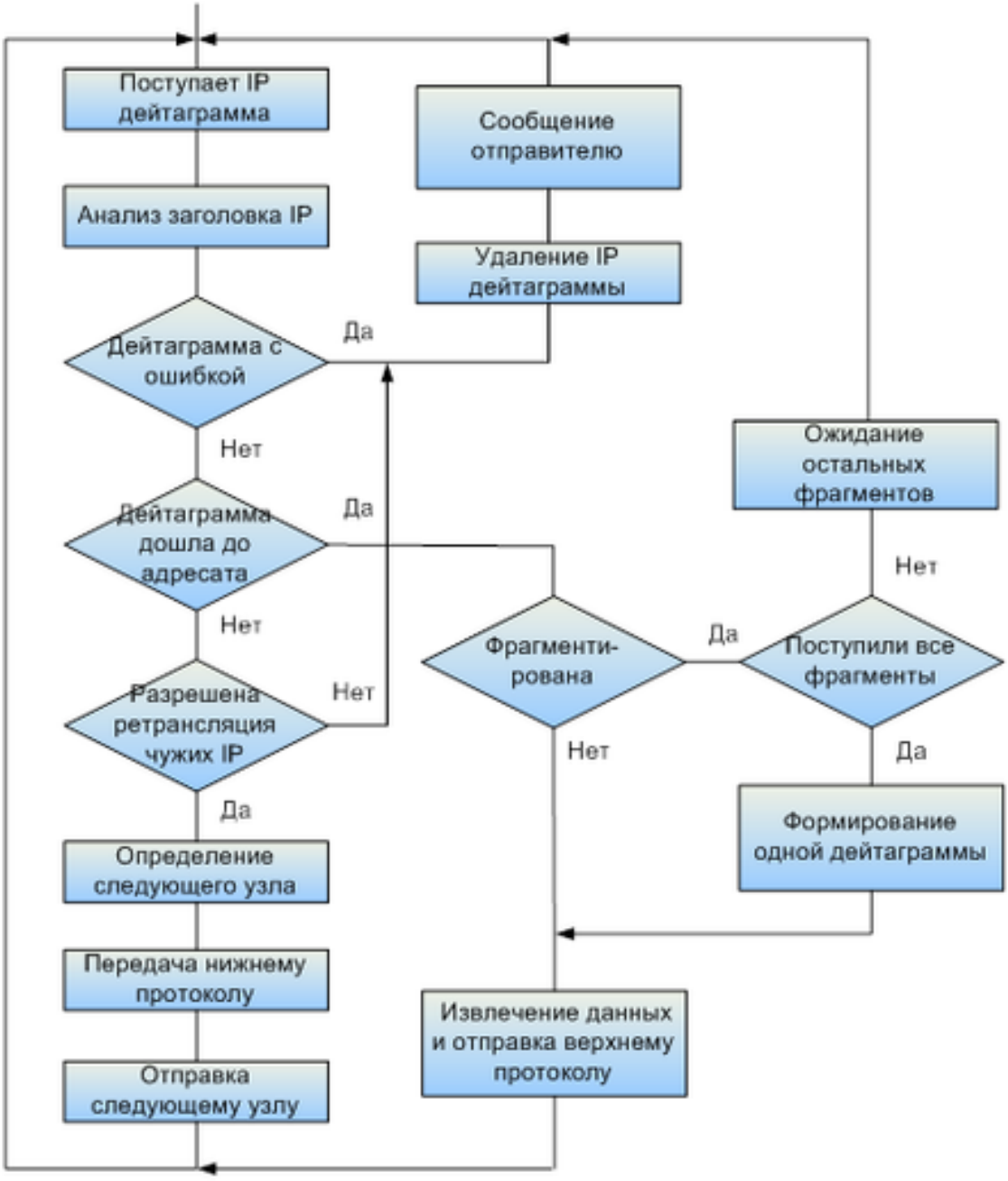

Рисунок 1.2 – Алгоритм работы протокола IPv4

1.1.1 Структура пакета IPv4

Структура IP пакетов версии 4 представлена на рисунке 1.3

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 – Структура пакета IPv4

- Версия — для IPv4 значение поля должно быть равно 4.
- Размер заголовка — (Internet Header Length) длина заголовка IP-пакета в 32-битных словах (dword). В этом поле указывается начало блока данных в пакете. Минимальное корректное значение для этого поля равно 5 (5×32=160 бит, 20 байт), максимальное — 15 (60 байт).
- Точка кода дифференцированных услуг (Differentiated Services Code Point, акроним DSCP) — 6 бит, используемые для указания класса обслуживания.
- УП (указатель перегрузки, Explicit Congestion Notification, ECN) — предупреждает о перегрузке сети без потери пакетов. Является необязательной функцией.
- Длина пакета — длина пакета в октетах, включая заголовок и данные. Минимальное корректное значение для этого поля равно 20, максимальное 65535.
- Идентификатор — значение, назначаемое отправителем пакета и предназначенное для определения корректной последовательности фрагментов при сборке пакета. Для фрагментированного пакета все фрагменты имеют одинаковый идентификатор.

- 3 бита флагов. Первый бит должен быть всегда равен нулю, второй бит DF (don’t fragment) определяет возможность фрагментации пакета и третий бит MF (more fragments) показывает, не является ли этот пакет последним в цепочке пакетов.
- Смещение фрагмента — значение, определяющее позицию фрагмента в потоке данных. Смещение задается количеством восьми байтовых блоков, поэтому это значение требует умножения на 8 для перевода в байты.
- Время жизни (TTL) — число маршрутизаторов, которые должен пройти этот пакет. При прохождении маршрутизатора это число уменьшатся на единицу. Если значения этого поля равно нулю то, пакет должен быть отброшен и отправителю пакета может быть послано сообщение Time Exceeded (ICMP код 11 тип 0).
- Протокол — идентификатор интернет-протокола следующего уровня указывает, данные какого протокола содержит пакет, например, TCP или ICMP.
- Контрольная сумма заголовка — вычисляется в соответствии с RFC 1071 [11]

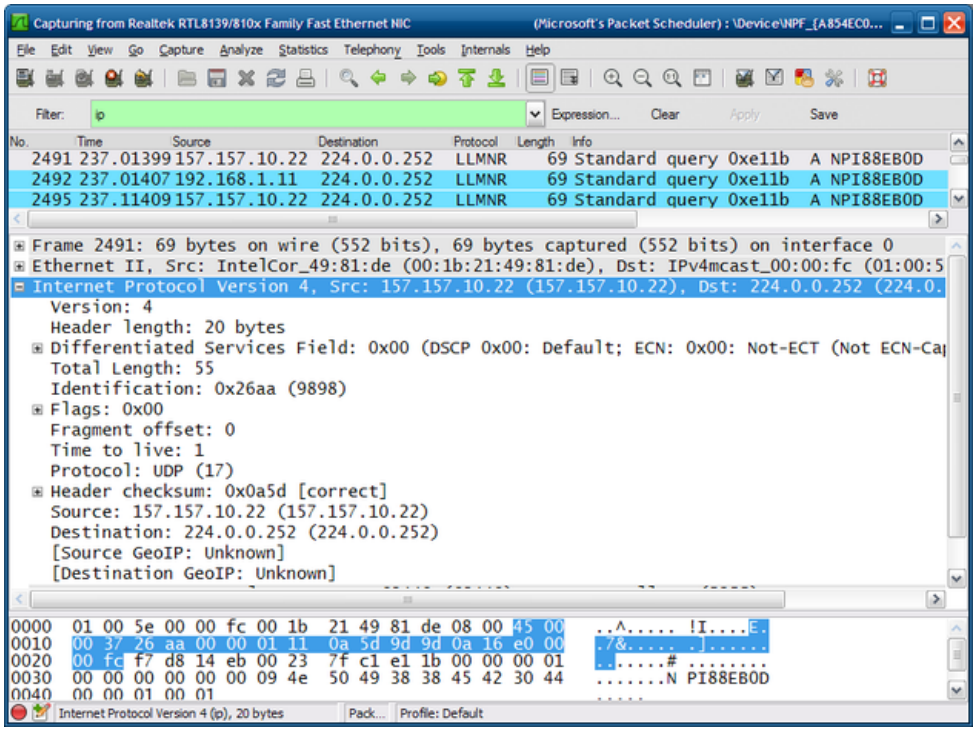

Рисунок 1.4 – Перехваченный IPv4 пакет с помощью сниффера Wireshark

1.1.2 Фрагментация IP пакетов

Способность протокола IP фрагментировать пакеты является важной особенностью в отличии от сетевого протокола IPX. Передача пакетов через локальные и глобальные сети разных типов приводит к проблеме разных допустимых размеров полей данных кадров канального уровня (Maximum Transfer Unit – MTU). Так, сети Ethernet могут передавать кадры, несущие до 1500 байт данных, для сетей X.25 характерен размер поля данных кадра в 128 байт, сети FDDI могут передавать кадры размером в 4500 байт, в других сетях действуют свои ограничения. Протокол IP умеет передавать дейтаграммы, прибегая к фрагментированию – разбиения “большого пакета” на некоторое количество частей (фрагментов), размер каждой из которых удовлетворяет MTU промежуточной сети. После передачи всех фрагментов пакета через промежуточную сеть, они будут собраны обратно в единый пакет. Отметим, что сборку пакета из фрагментов осуществляет только получатель, а не какой-либо из промежуточных маршрутизаторов. Маршрутизаторы могут только фрагментировать пакеты, но не собирать их. Это связано с тем, что разные фрагменты одного пакета не обязательно будут проходить через одни и те же маршрутизаторы [12].

С помощью поля Идентификация определяется принадлежность фрагмента к определенному пакету, для того что затем при сборе их не перепутать с фрагментами других пакетов. Значение этого поля должно быть одинаковым для всех фрагментов одного пакета и не повторяться для разных пакетов, пока у обоих пакетов не истекло время жизни. При делении данных пакета, размер всех фрагментов, кроме последнего, должен быть кратен 8 байтам. Это позволяет отвести меньше места в заголовке под поле Смещение фрагмента.

Второй бит поля Флаги (More fragments), при значении равной единице, указывает на то, что данный фрагмент – не последний в пакете. Пакет отправляется без фрагментации, если флаг “More fragments” устанавливается в 0, а поле Смещение фрагмента – заполняется нулевыми битами.

Первый бит поля Флаги (Don’t fragment) равный единице запрещает фрагментацию пакета. Если в данном случае пакет должен быть передан через сеть с недостаточным MTU, то маршрутизатор его отбросит (и сообщит об этом отправителю посредством протокола ICMP). Данный флаг применяется, если отправителю известно, что получатель не имеет возможности восстановить пакет на своей стороне [12-16, 35].

1.1.3 Классы IP адресов

IP-адреса имеют две логические части – номер сети и номер узла сети. Определить какая часть IP-адреса относится к номеру сети, а какая к номеру узла можно по значениям первых бит адреса. Значение этих бит также определяют к какому классу относится IP-адрес.

На рисунке 1.5 показана структура IP-адреса разных классов.

Рисунок 1.5 – Структура IP-адреса разных классов

Если адрес начинается с 0, то сеть относят к классу A и номер сети занимает один байт, остальные 3 байта интерпретируются как номер узла в сети. Сети класса A имеют номера в диапазоне от 1 до 126. (Номер 0 не используется, а номер 127 зарезервирован для специальных целей) Сетей класса A немного, зато количество узлов в них может достигать 2^{24}, то есть 16 777 216 узлов.

Если первые два бита адреса равны 10, то сеть относится к классу B. В сетях класса B под номер сети и под номер узла отводится по 16 бит, то есть по 2 байта. Это сети средних размеров с максимальным числом узлов 2^{16}, что составляет 65 536 узлов.

Если адрес имеет первые биты со значением 110, то это сеть класса C. Этот класс отводит 24 бита на номер сети, а под номер узла — 8 бит. Сети данного класса наиболее распространены, число узлов в них ограничено 2^8, то есть 256 узлами.

Адрес начинающийся с последовательности 1110, является адресом класса D и обозначает особый, групповой адрес — multicast. Пакеты с таким классом адреса должны получать все узлы, которым присвоен данный адрес.

Если адрес начинается с последовательности 11110, то этот адрес относится к классу E. Адреса этого класса зарезервированы для будущих применений [5,7,11, 26].

В таблице 1.1 приведены диапазоны номеров сетей и максимальное число узлов, соответствующих каждому классу сетей.

Таблица 1.1 - Диапазоны номеров сетей и максимальное число узлов

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

Большие сети получают адреса класса A, средние — класса B, а маленькие — класса C.

1.1.4 Использование масок в IP адресации

Ранее предприятия, чтобы получить тот или иной диапазон IP-адресов, заполняли регистрационную форму, где указывали текущее число ЭВМ и планируемое увеличение количества рабочих станций. Затем предприятию выдавался класс IP-адресов: A, B или C в зависимости от заявленных в форме параметров сети.

Такой механизм работал какое-то время исправно до тех пор, пока количество рабочих станций в организациях было небольшим. Но с развитием Интернета и сетевых технологий, количество рабочих станций во многих организациях уже исчислялось несколькими сотнями (например, больше 300), что вынуждало регистрировать сеть класса B, т.к. сеть класса C могла распределить адреса только между 254 компьютерами. В результате сетей класса B стало, просто на просто не хватать, но при этом большие диапазоны адресов были не задействованы.

Чтобы можно было гибко устанавливать границу между номером сети и номером узла, получил широкое распространение использование маски сети.

Маска — это число, которое используется в паре с IP-адресом; разряды, заполненные единицами в двоичной системе, интерпретируют номер сети в IP-адресе. Поскольку номер сети является цельной частью адреса, единицы в маске также должны представлять непрерывную последовательность.

Для стандартных классов сетей маски имеют следующие значения:

- 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).

Снабжая каждый IP-адрес маской, можно отказаться от понятий классов адресов и сделать более гибкой систему адресации. Например, если рассмотренный выше адрес 185.23.44.206 ассоциировать с маской 255.255.255.0, то номером сети будет 185.23.44.0, а не 185.23.0.0, как это определено системой классов.

В масках количество единиц в последовательности, определяющей границу номера сети, не обязательно должно быть кратным 8, чтобы повторять деление адреса на байты. Пусть, например, для IP-адреса 129.64.134.5 указана маска 255.255.128.0, то есть в двоичном виде:

- IP-адрес 129.64.134.5 - 10000001. 01000000.10000110. 00000101
- Маска 255.255.128.0 - 11111111.11111111.10000000. 00000000

Если игнорировать маску, то в соответствии с системой классов адрес 129.64.134.5 относится к классу B, а значит, номером сети являются первые 2 байта — 129.64.0.0, а номером узла — 0.0.134.5.

Если же использовать для определения границы номера сети маску, то 17 последовательных единиц в маске, «наложенные» (логическое умножение) на IP-адрес, определяют в качестве номера сети в двоичном выражении число:

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

или в десятичной форме записи — номер сети 129.64.128.0, а номер узла 0.0.6.5.

Существует также короткий вариант записи маски, называемый префиксом или короткой маской. В частности, сеть 80.255.147.32 с маской 255.255.255.252, можно записать в виде 80.255.147.32/30, где «/30» указывает на количество двоичных единиц в маске, то есть тридцать бинарных единиц (отсчет ведется слева направо) [10-20].

Для наглядности в таблице 1.2 отображается соответствие префикса с маской:

Таблица 1.2 – Соответствие префикса с маской сети

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

Механизм масок широко распространен в IP-маршрутизации причем маски могут использоваться для самых разных целей. С их помощью администратор может структурировать свою сеть, не требуя от поставщика услуг дополнительных номеров сетей. На основе этого же механизма поставщики услуг могут объединять адресные пространства нескольких сетей путем введения так называемых «префиксов» с целью уменьшения объема таблиц маршрутизации и повышения за счет этого производительности маршрутизаторов. Помимо этого, записывать маску в виде префикса значительно короче [19, 30].

1.1.5 Особые IP адреса

В протоколе IP существует несколько соглашений об особой интерпретации IP-адресов:

- 0.0.0.0 - представляет адрес шлюза по умолчанию, т.е. адрес компьютера, которому следует направлять информационные пакеты, если они не нашли адресата в локальной сети (таблице маршрутизации);
- 255.255.255.255 – широковещательный адрес. Сообщения, переданные по этому адресу, получают все узлы локальной сети, содержащей компьютер-источник сообщения (в другие локальные сети оно не передается);
- «Номер сети».«все нули» – адрес сети (например 192.168.10.0);
- «Все нули».«номер узла» – узел в данной сети (например 0.0.0.23). Может использоваться для передачи сообщений конкретному узлу внутри локальной сети;
- Если в поле номера узла назначения стоят только единицы, то пакет, имеющий такой адрес, рассылается всем узлам сети с заданным номером

сети. Например, пакет с адресом 192.190.21.255 доставляется всем узлам сети 192.190.21.0. Такая рассылка называется широковещательным сообщением (broadcast). При адресации необходимо учитывать те ограничения, которые вносятся особым назначением некоторых IP-адресов. Так, ни номер сети, ни номер узла не может состоять только из одних двоичных единиц или только из одних двоичных нулей. Отсюда следует, что максимальное количество узлов, приведенное в таблице для сетей каждого класса, на практике должно быть уменьшено на 2. Например, в сетях класса С под номер узла отводится 8 бит, которые позволяют задавать 256 номеров: от 0 до 255. Однако на практике максимальное число узлов в сети класса С не может превышать 254, так как адреса 0 и 255 имеют специальное назначение. Из этих же соображений следует, что конечный узел не может иметь адрес типа 98.255.255.255, поскольку номер узла в этом адресе класса А состоит из одних двоичных единиц [17].

- Особый смысл имеет IP-адрес, первый октет которого равен 127.x.x.x. Он используется для тестирования программ и взаимодействия процессов в пределах одной машины. Когда программа посылает данные по IP-адресу 127.0.0.1, то образуется как бы «петля». Данные не передаются по сети, а возвращаются модулям верхнего уровня как только что принятые. Поэтому в IP-сети запрещается присваивать машинам IP-адреса, начинающиеся со 127. Этот адрес имеет название loopback. Можно отнести адрес 127.0.0.0 ко внутренней сети модуля маршрутизации узла, а адрес 127.0.0.1 — к адресу этого модуля на внутренней сети. На самом деле любой адрес сети 127.0.0.0 служит для обозначения своего модуля маршрутизации, а не только 127.0.0.1, например 127.0.0.3.

В протоколе IP нет понятия широковещательности в том смысле, в котором оно используется в протоколах канального уровня локальных сетей, когда данные должны быть доставлены абсолютно всем узлам. Как ограниченный широковещательный IP-адрес, так и широковещательный IP-адрес имеют пределы распространения в интерсети — они ограничены либо сетью, к которой принадлежит узел-источник пакета, либо сетью, номер которой указан в

адресе назначения. Поэтому деление сети с помощью маршрутизаторов на части локализует широковещательный шторм пределами одной из составляющих общую сеть частей просто потому, что нет способа адресовать пакет одновременно всем узлам всех сетей составной сети [18].

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

1.1.6 IP-адреса, используемые в локальных сетях

Все используемые в Интернете адреса, должны регистрироваться, что гарантирует их уникальность в масштабе всей планеты. Такие адреса называются реальными или публичными IP-адресами.

Для локальных сетей, не подключенных к Интернету, регистрация IP-адресов, естественно, не требуется, так как, в принципе, здесь можно использовать любые возможные адреса. Однако, чтобы не допускать возможность

конфликтов при последующем подключении такой сети к интернету, рекомендуется применять в локальных сетях только следующие диапазоны так называемых частных IP-адресов (в интернете эти адреса не существуют и использовать их там нет возможности), представленных в таблице 1.4 [20].

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 Протокол IPv6

Во время разработки IPv4 состояние инфокоммуникационных технологий не предполагало столь большое число устройств, подключенных к глобальной сети Internet. Было представление, что около 4,23 миллиарда адресов вполне хватит, чтобы задействовать все устройства в мире в единую сеть на тот момент. Однако на 2015 год количество устройств, подключенных к сети Интернет составило примерно 15 миллиардов сетевых подключений и продолжает стремительно расти [21-23].

По сей день использование IPv4 проходит штатно, поскольку используются различные технологии экономии использования сетевых адресов, в частности технология NAT (Network Address Translation, преобразование сетевых адресов), но уже всем понятно, что дни эксплуатации IPv4 подходят к концу, поскольку в ближайшем будущем предусматривается наделять возможностью доступа к интернету всех бытовых приборов (холодильников, СВЧ-печей), для осуществления управления данными приборами удаленно, посредством сети с любой точки Земли.

В сложившейся ситуации переход на новый формат сетевого адреса становится крайне остро. Хотя многие специалисты предвидели проблему нехватки сетевых адресов еще в начале 1990 года, в то же время начала работать

группа проектирования Интернета IETF над новой версией сетевого протокола - IPv6 [22-27].

Основные решаемые задачи:

- Возможность доступа к глобальной сети миллиардов хостов даже при нерациональном использовании адресного пространства.
- Сокращение размера таблиц маршрутизации
- Упрощение протокола для ускорения обработки пакетов маршрутизации
- Повышение уровня безопасности протокола
- Упрощение работы многоадресных рассылок с помощью указания областей рассылки.
- Перспективы дальнейшего развития протокола в будущем
- Организация совместимости старого и нового протокола

Протокол IPv6 разработан в конце 1992 года.

Протокол IPv6 (Internet Protocol version 6) — это новая версия интернет протокола (IP), созданная с целью решения проблем, с которыми столкнулась предыдущая версия (IPv4) при её использовании в интернете, одна из которых – это использование длины адреса 128 бит вместо 32.

В наше время протокол IPv6 пока ещё не получил столь широкого распространения в Интернете, как IPv4, но постепенно доля в мировом масштабе растет и на начало 2016 года устройства использующие межсетевой протокол IP версии 6 составила 10% (рис.1.8) [28,29].

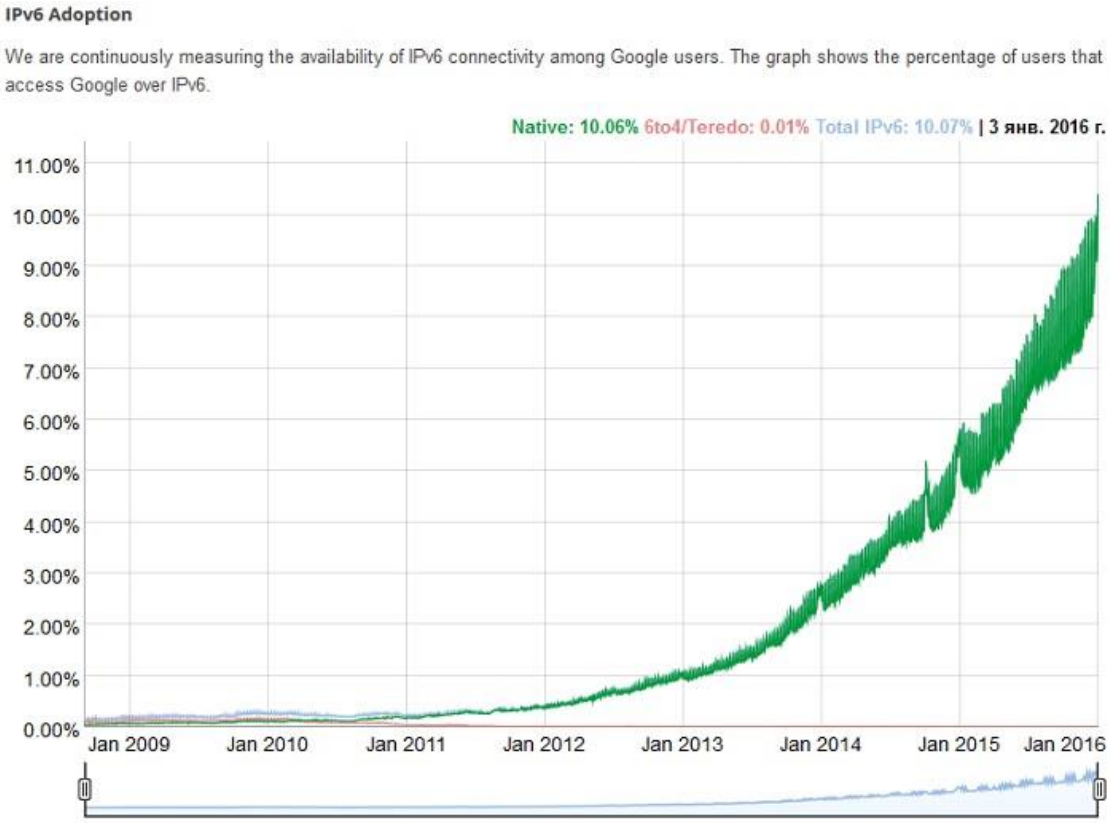

Рисунок 1.6 – График количества устройств использующих IPv6

Интернет протокол IPv6 хорошо справляется с основными поставленными задачами. Ему присущи достоинства интернет протокола IP и лишен некоторых недостатков, к тому же обладает некоторыми новыми возможностями. В общем случае протокол IPv6 несовместим с протоколом IPv4, но зато совместим со всеми остальными протоколами Интернета, включая TCP, UDP, ICMP, OSPF, DNS для чего иногда требуются небольшие изменения.

1.2.1 Особенности IPv6

- Протокол IPv6 имеет длину 16 байт, что решает основную проблему - обеспечить практически неограниченный запас интернет – адресов.
- Протокол IPv6 по сравнению с IPv4 имеет более простой заголовок пакета. Таким образом, маршрутизаторы могут быстрее обрабатывать пакеты, что повышает производительность.

- Улучшенная поддержка необязательных параметров. Подобное изменение действительно было существенным, так как в новом заголовке требуемые прежде поля стали необязательными.
- Повышен уровень безопасности, аутентификация и конфиденциальность являются ключевыми чертами нового IP-протокола
- Уделено больше внимание типу представляемых услуг. Для этой цели в заголовке пакета IPv4 было отведено 8-разрядное поле [30].

1.2.2 Заголовок IPv6

<table>
<tr><td>Октет</td><td colspan="32">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</td></tr>
<tr><td>0</td><td colspan="4">Версия</td><td colspan="4">Приоритет</td><td colspan="24">Метка потока</td></tr>
<tr><td>4</td><td colspan="20">Длина полезной нагрузки</td><td colspan="8">Следующий заголовок</td><td colspan="4">Макс. Число транзитных узлов</td></tr>
<tr><td>8-20</td><td colspan="32">IP-адрес отправителя</td></tr>
<tr><td>24-36</td><td colspan="32">IP-адрес получателя</td></tr>
<tr><td></td><td colspan="32">Дополнительны заголовок</td></tr>
<tr><td></td><td colspan="32">Данные</td></tr>
</table>

Рисунок 1.7 – Структура IP пакетов версии

- Версия — для IPv6 значение поля должно быть равно 6.
- Приоритет – используется для того, чтобы различать пакеты с разными требованиями к доставке в реальном времени.
- Метка потока – применяется для установки между отправителем и получателем псевдосоединения с определенными свойствами и требованиями. Например, поток пакетов между двумя процессами на разных хостах может обладать строгими требованиями к задержкам, что потребует резервирование пропускной способности.
- Длина полезной нагрузки – сообщает, сколько байт следует за 40-байтовым заголовком.
- Следующий заголовок – сообщает, какой из дополнительных заголовков следует за основным.

- Max число транзитных узлов – аналог времени жизни (TTL).
- Дополнительные заголовки:
- Параметры маршрутизации – разнообразная информация для маршрутизаторов;
- Параметры получения – дополнительная информация для получателя
- Маршрутизация – частичный список транзитных маршрутизаторов на пути пакета;
- Фрагментация – управление фрагментами дейтаграмм;
- Аутентификация – проверка подлинности отправителя;
- Шифрованные данные – информация о зашифрованном содержимом [31-34].

1.2.3 Типы адресов в IPv6

Unicast - Идентификатор одиночного интерфейса. Пакет, посланный по уникастному адресу, доставляется интерфейсу, указанному в адресе.

Anycast - Идентификатор набора интерфейсов (принадлежащих разным узлам). Пакет, посланный по эникастному адресу, доставляется одному из интерфейсов, указанному в адресе (ближайший, в соответствии с мерой, определенной протоколом маршрутизации).

Multicast - Идентификатор набора интерфейсов (обычно принадлежащих разным узлам). Пакет, посланный по мультикастинг-адресу, доставляется всем интерфейсам, заданным этим адресом.

В IPv6 не существует широковещательных адресов, их функции переданы мультикастинг-адресам.

В IPv6, все нули и все единицы являются допустимыми кодами для любых полей, если не оговорено исключение [35].

1.2.4 Модель адресации в IPv6

IPv6 адреса всех типов ассоциируются с интерфейсами, а не узлами. Так как каждый интерфейс принадлежит только одному узлу, уникастный адрес интерфейса может идентифицировать узел.

IPv6 уникастный адрес соотносится только с одним интерфейсом. Одному интерфейсу могут соответствовать много IPv6 адресов различного типа (уникастные, эникастные и мультикстные). Существует два исключения из этого правила:

- Одиночный адрес может приписываться нескольким физическим интерфейсам, если приложение рассматривает эти несколько интерфейсов как единое целое при представлении его на уровне Интернет.
- Маршрутизаторы могут иметь ненумерованные интерфейсы (например, интерфейсу не присваивается никакого IPv6 адреса) для соединений точка-точка, чтобы исключить необходимость вручную конфигурировать и объявлять (advertise) эти адреса. Адреса не нужны для соединений точка-точка маршрутизаторов, если эти интерфейсы не используются в качестве точки отправления или назначения при посылке IPv6 дейтограмм. Маршрутизация здесь осуществляется по схеме близкой к используемой протоколом CIDR в IPv4.

IPv6 соответствует модели IPv4, где субсеть ассоциируется с каналом. Одному каналу могут соответствовать несколько субсетей [36].

1.2.5 Формы представления IPv6

- **Форма шестнадцатеричных чисел и двоеточий**

Эта форма является предпочтительной и имеет вид n:n:n:n:n:n:n:n. Каждый знак n соответствует 4-хзначному шестнадцатеричному числу (всего 8 шестнадцатеричных чисел, для каждого числа отводится 16 бит). Например: 1FA9:FFFF:2621:ACDA:2245:BF98:3412:4167.

- **Сжатая форма**

По причине большой длины адрес обычно содержит много нулей подряд. Для упрощения записи адресов используется сжатая форма, в которой смежные последовательности нулевых блоков заменяются парами символов двоеточий (::).Однако такой символ может встречаться в адресе только один раз.

Например:

- адрес групповой рассылки FFEA:0:0:0:0:CA28:1210:4362 имеет сжатую форму FFEA::CA28:1210:4362.
- Адрес одноадресной рассылки 3FFE:FFFF:0:0:8:800:02A1:0 в сжатой форме имеет вид: 3FFE:FFFF::8:800:02A1:0.
- Шлейфовый адрес 0:0:0:0:0:0:0:1 в сжатой форме вы-глядит так ::1.
- Неопределенный адрес 0:0:0:0:0:0:0:0 превращается в :: .

- **Смешанная форма**

Эта форма представляет собой сочетание адресов протоколов IPv4 и IPv6. В этом случае адрес имеет формат n:n:n:n:n:n:d.d.d.d, где каждый символ n соответствует 4-х значному шестнадцатеричному числу (6 шестнадцатеричных чисел, для каждого числа отводится 16 бит), ad.d.d.d -часть адреса, записанная в формате IPv4 (32 бита) [36-39].

Например:

- 0:0:0:0:0:0:19.8.62.32
- 0:0:0:0:0:FFFF:111.214.2.34
- или в сжатом виде:
- ::73.3.68.45
- ::F2F3:129.131.32.31

Таблица 1.5 – 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

1.3 Сети Virtual Local Area Network (VLAN)

На данный момент многие современные организации и предприятия практически не используют такую весьма полезную, а часто и необходимую, возможность, как организация виртуальной локальной сети (VLAN) в рамках цельной инфраструктуры, которая предоставляется большинством современных коммутаторов. Связано это со многими факторами, поэтому стоит рассмотреть данную технологию с позиции возможности ее использования в таких целях [40-42].

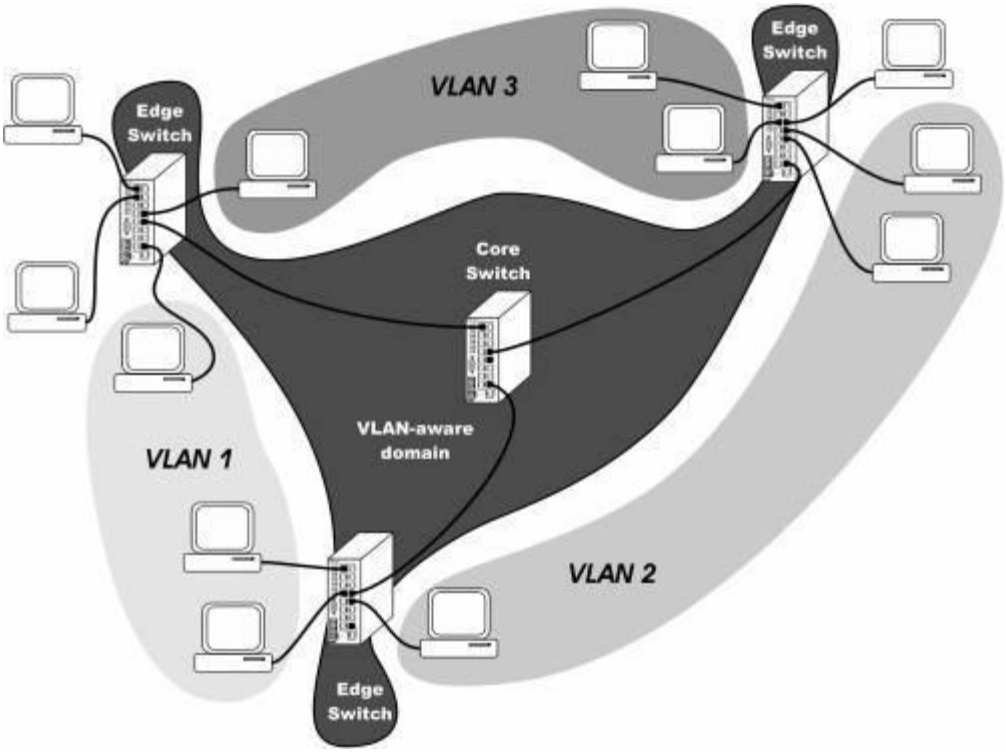

Рисунок 1.8 – Пример разделение локальной сети по VLAN

1.3.1 VLAN. Общее описание

Для начала стоит определиться с тем, что такое VLANs. Под этим подразумевается группа компьютеров, подключенных к сети, которые логически объединены в домен рассылки сообщений широкого вещания по определенному признаку. К примеру, группы могут быть выделены в зависимости от структуры предприятия либо по видам работы над проектом или задачей совместно. Сети VLAN дают несколько преимуществ. Для начала речь идет о значительно более эффективном использовании пропускной способности (в сравнении с традиционными локальными сетями), повышенной степени защиты информации, которая передается, а также упрощенной схеме администрирования.

Так как при использовании VLAN происходит разбитие всей сети на широковещательные домены, информация внутри такой структуры передается только между ее членами, а не всем компьютерам в физической сети. Получа-

ется, что широковещательный трафик, который генерируется серверами, ограничен предопределенным доменом, то есть не транслируется всем станциям в этой сети. Так удается достичь оптимального распределения пропускной способности сети между выделенными группами компьютеров: серверы и рабочие станции из разных VLAN просто не видят друг друга [40-45].

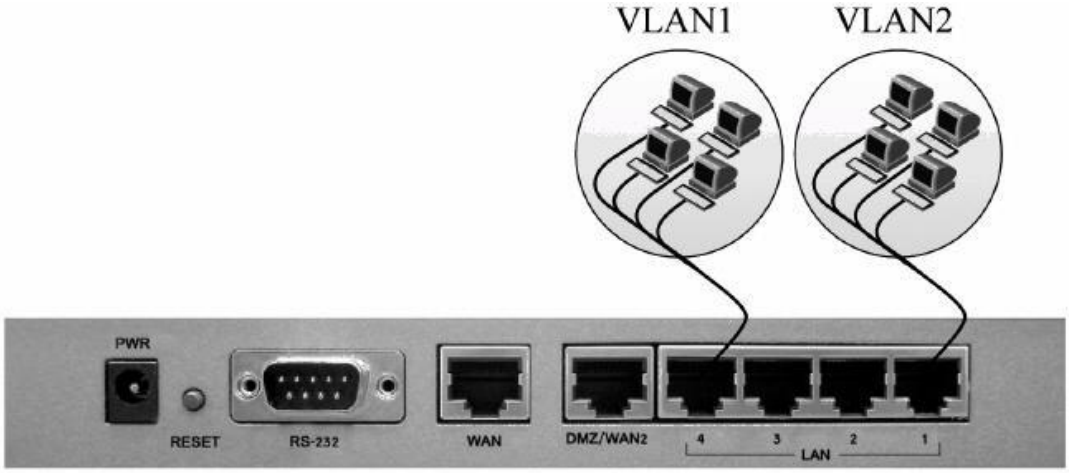

Рисунок 1.9 – Схематичный вид разделения сети на VLANs на коммутаторе

1.3.2 Процессы при использовании VLAN

В такой сети информация довольно хорошо защищена от несанкционированного доступа, ведь обмен данными осуществляется внутри одной конкретной группы компьютеров, то есть они не могут получить трафик, генерируемой в какой-то другой аналогичной структуре. Если говорить о том, что такое VLANs, то тут уместно отметить такое достоинство этого способа организации, как упрощенное сетевое администрирование. Это затрагивает такие задачи, как добавление новых элементов к сети, их перемещение, а также удаление. К примеру, если какой-то пользователь VLAN переезжает в другое помещение, сетевому администратору не потребуется перекоммутировать кабели. Он должен просто произвести настройку сетевого оборудования со своего рабочего места. В некоторых реализациях таких сетей контроль перемещения членов группы может производиться в автоматическом режиме, даже не

нуждаясь во вмешательстве администратора. Ему только необходимо знать о том, как настроить VLAN, чтобы производить все необходимые операции. Он может создавать новые логические группы пользователей, даже не вставая с места. Это все очень сильно экономит рабочее время, которое может пригодиться для решения задач не меньшей важности [42-45,47].

1.3.3 Способы организации VLAN

Существует три различных варианта: на базе портов, протоколов третьего уровня или MAC-адресов. Каждый способ соответствует одному из трех нижних уровней модели OSI: физическому, сетевому и канальному соответственно. Если говорить о том, что такое VLANs, то стоит отметить и наличие четвертого способа организации – на базе правил. Сейчас он используется крайне редко, хотя с его помощью обеспечивается большая гибкость. Можно рассмотреть более подробно каждый из перечисленных способов, чтобы понять, какими особенностями они обладают [47].

1.3.4 VLAN на базе портов

Здесь предполагается логическое объединение определенных физических портов коммутатора, выбранных для взаимодействия. К примеру, сетевой администратор может определить, что определенные порты, к примеру, 1, 2, и 5 формируют VLAN1, а номера 3, 4 и 6 используются для VLAN2 и так далее. Один порт коммутатора вполне может использоваться для подключения нескольких компьютеров, для чего применяют, к примеру, хаб. Все они будут определены в качестве участников одной виртуальной сети, к которой прописан обслуживающий порт коммутатора. Подобная жесткая привязка членства виртуальной сети является основным недостатком подобной схемы организации [43].

1.3.5 VLAN на базе MAC-адресов

В основу этого способа заложено использование уникальных шестнадцатеричных адресов канального уровня, имеющихся у каждого сетевого адаптера сервера либо рабочей станции сети. Если говорить о том, что такое VLANs, то стоит отметить, что этот способ принято считать более гибким в сравнении с предыдущим, так как к одному порту коммутатора вполне допускается подключение компьютеров, принадлежащих к разным виртуальным сетям. Помимо этого, он автоматически отслеживает перемещение компьютеров с одного порта на другой, что позволяет сохранить принадлежность клиента к конкретной сети без вмешательства администратора. Принцип работы тут весьма прост: коммутатором поддерживается таблица соответствия MAC-адресов рабочих станций виртуальным сетям. Как только происходит переключение компьютера на какой-то другой порт, происходит сравнение поля MAC-адреса с данными таблицы, после чего делается правильный вывод о принадлежности компьютера к определенной сети. В качестве недостатки подобного способа называется сложность конфигурирования VLAN, которая может изначально стать причиной появления ошибок. При том, что коммутатор самостоятельно строит таблицы адресов, сетевой администратор должен просмотреть ее всю, чтобы определить, какие адреса каким виртуальным группам соответствуют, после чего он прописывает его к соответствующим VLANs. И именно тут есть место ошибкам, что иногда случается в Cisco VLAN, настройка которых довольно проста, но последующее перераспределение будет сложнее, чем в случае с использованием портов. VLAN на базе протоколов третьего уровня Этот, метод довольно редко используется в коммутаторах на уровне рабочей группы или отдела. Он характерен для магистральных, оснащенных встроенными средствами маршрутизации основных протоколов локальных сетей - IP, IPX и AppleTalk. Этот способ предполагает, что группа портов коммутатора, которые принадлежат к определенной VLAN, будут ассоциироваться с какой-то подсетью IP или IPX. В данном случае гибкость

обеспечивается тем, что перемещение пользователя на другой порт, который принадлежит той же виртуальной сети, отслеживается коммутатором и не нуждается в переконфигурации. Маршрутизация VLAN в данном случае довольно проста, ведь коммутатор в данном случае анализирует сетевые адреса компьютеров, которые определены для каждой из сетей. Данный способ поддерживает и взаимодействие между различными VLAN без применения дополнительных средств. Есть и один недостаток у данного способа – высокая стоимость коммутаторов, в которых он реализован. VLAN Ростелеком поддерживают работу на этом уровне [45].

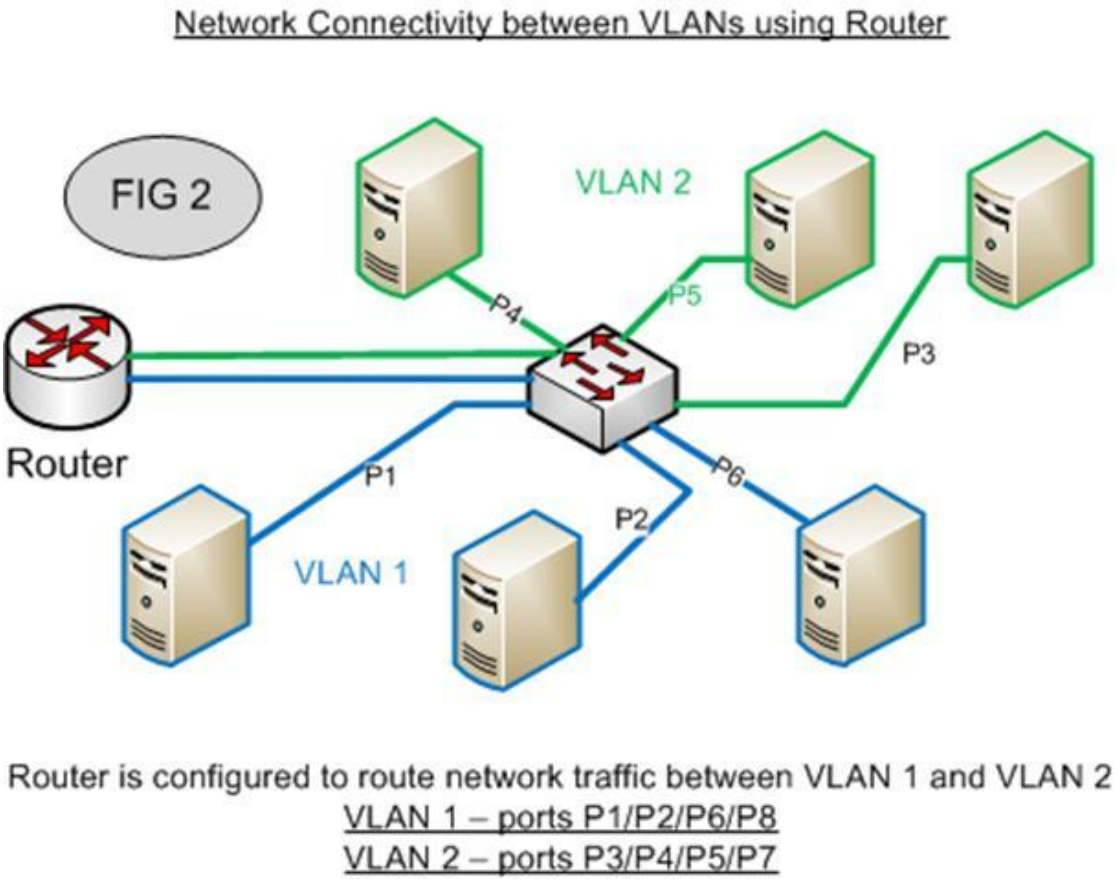

Рисунок 1.10 – Формирование VLANs на базе MAC-адресов

ГЛАВА 2. СХЕМА ОРГАНИЗАЦИИ СВЯЗИ МУЛЬТИСЕРВСИНОЙ СЕТИ СВЯЗИ МИКРОРАЙОНА

2.1 Описание типовой схемы, исследуемой мультисервисной сети связи микрорайона

Одна из целей исследования было определить эффективность работы мультисервисной сети по времени задержки прохождения пакетов в сети и загрузке сервера обрабатываемыми пакетами данных при различных конфигурациях. Основной интерес в данной работе уделена исследованию характеристик мультисервисной сети при использовании сетевого протокола IP версии 4, а также IP версии 6 и сравнить их. IP протокол является одним из самых важных на сегодняшний день в организации какой-либо сети. Этот протокол, объединяя сегменты сети, обеспечивает доставку пакетов между любыми узлами сети через произвольное число промежуточных узлов. Информационная часть пакетов с данными существенно влияет на работу сети. В зависимости от информации, содержащейся в заголовках IP пакета будет зависеть доставка данных по назначению, как можно быстрее и эффективнее. Чем быстрее IP-пакет будет обрабатываться на узлах (маршрутизаторах) тем быстрее будет работать и вся сеть. IP протокол версии 6 способствует эффективной работе сети за счет нескольких особенностей в сравнении с IPv4 [48-50].

В качестве эксперимента была взята типовая схема мультисервисной сети жилого микрорайона. В этой сети находится 4000 абонентов, подсоединённых к различным Web, VoIP, видео, аудио сервисам через коммутаторы и маршрутизаторы по древовидной топологии. Маршрутизаторы между собой соединены оптоволоконным кабелем, а также с коммутаторами доступа, от которых используя UTP кабель по технологии FastEhternet передается трафик к каждому абоненту. Для того чтобы проследить, как влияет количество абонентов и узлов (маршрутизаторов) в сети при использовании двух исследуемых

протоколов, было решено построить 3 модели различного масштаба и емкости. Первая модель включает в себя 1000 абонентов, подключенных к коммутатору, и далее через маршрутизатор получают услуги от группы серверов. Вторая модель имеет в два раза больше абонентов и на один больше маршрутизатор, чем в первой. Также весь трафик проходит через маршрутизаторы к группе серверов предоставляющие услуги подключенным абонентам. Третья модель имеет в 4 раза больший размер подключенных клиентов, получающих услуги и объединены между собой с доступом к серверам через три маршрутизатора.

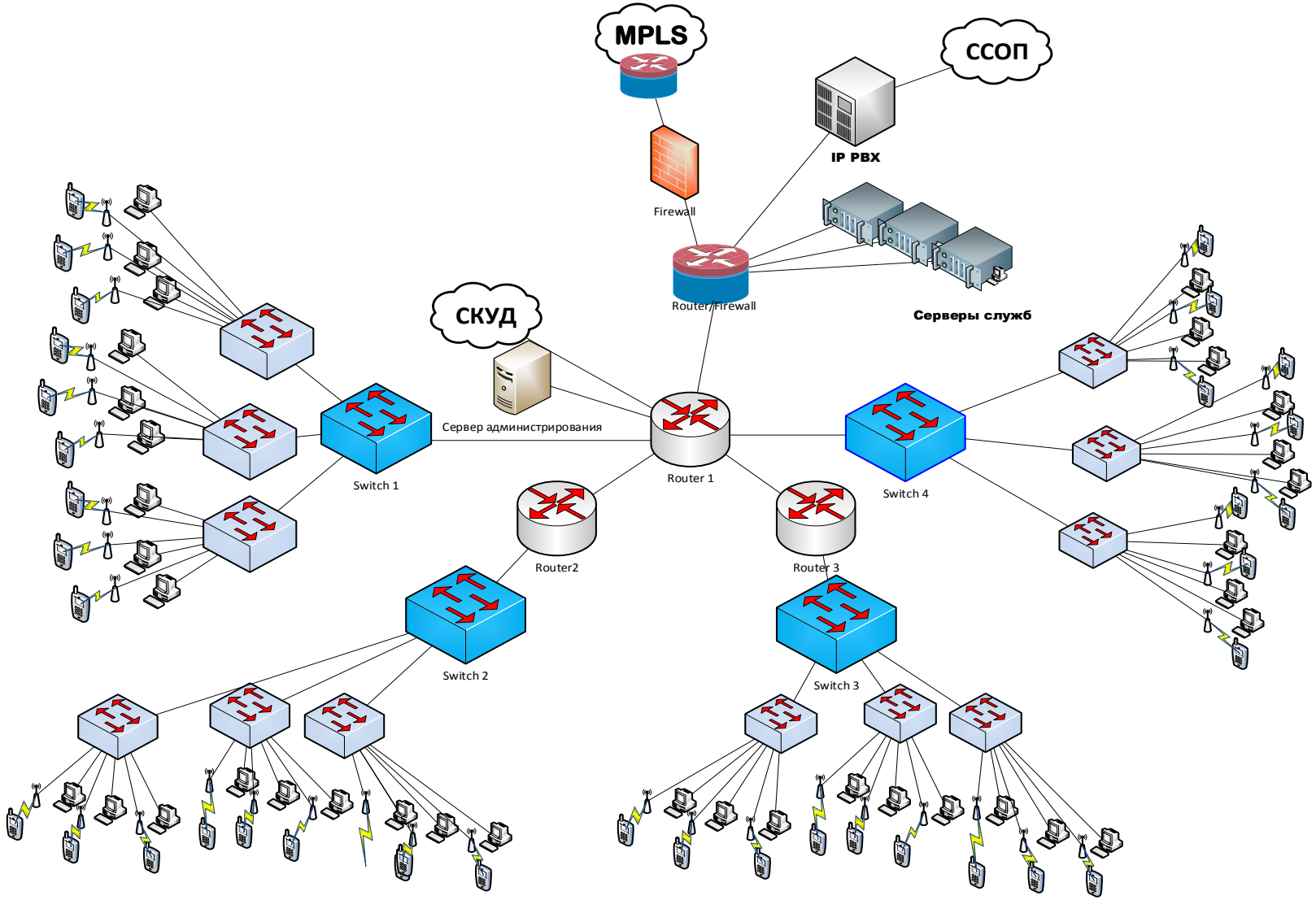

Рисунок 2.1 – Типовая схема мультисервисной сети микрорайона

2.2 Технология Riverbed Modeler

Под технологией Riverbed Modeler подразумевают совокупность действий для создания модели сети и проведение на ней имитационных экспериментов. Программный пакет Riverbed Modeler предоставляет широкие возможности для построения моделей сети, позволяющие уделять внимание вплоть до мелочей в создании какого-либо проекта сетевой инфраструктуры. Выбор требуемой статистики, собираемая с каждого объекта сети или со всей сети, запуская процесс моделирования на задаваемые время симуляции работы сети и затем осуществляться просмотр результатов – все эти возможности, предоставляемые данным продуктом, несут огромный потенциал в решении различных вопросов по организации ИВС (информационно-вычислительных сетей).

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

Рисунок 2.2 – 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. Также можно учитывать размеры модели сети, создавая проекты на шаблоне глобального масштаба, районного, кампусного или размером офиса, учитывая расстояния между узлами. Или использовать схему здания, где размещается или планируется разместить вычислительную сеть, получая готовый план-проект, который можно изменять только в рамках ограниченных средой размещения сети.

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.

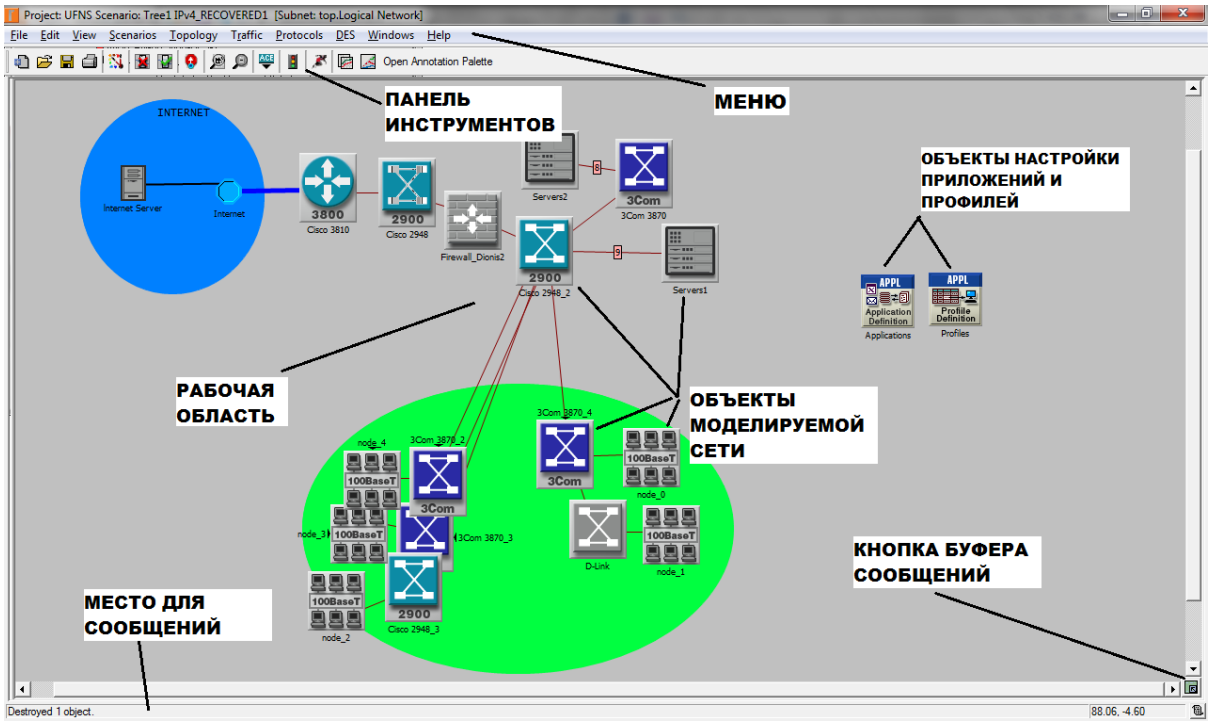

Рисунок 2.3 – Интерфейс программы Riverbed Modeler

Riverbed Modeler предоставляет собой виртуальную сетевую среду, которая моделирует поведение сетей, включая маршрутизаторы, коммутаторы, рабочие станции, серверы, протоколы и конкретные приложения. Дружественный интерфейс Modeler 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. Создание самостоятельно уникальных всевозможных сетевых устройств, которых нет в большой базе Modeler, предоставляет возможность наиболее точно спроектировать сеть, добиваясь необходимых результатов.

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 Modeler проектом), необходимо определиться с узлами сети: с компьютерами, коммутаторами, маршрутизаторами и так далее), соединениями между узлами и приложениями, которые будут работать на том или ином узле. Также можно сгенерировать определенный трафик со спецификой, которые имеются в реальной работающей сети, или даже загрузить файл с характеристикой трафика работы реальной сетевой инфраструктуры. [58-60]

ГЛАВА 3. ИССЛЕДОВАНИЕ ЭФФЕКТИВНОСТИ РАБОТЫ МЕЖСЕТЕВЫХ ПРОТОКОЛОВ И VLAN-КАНАЛОВ ПО УСЛУГАМ

3.1 Сравнение эффективности работы протоколов IPv4 и IPv6

Для моделирования сетей была использована программа Riverbed Modeler, позволяющая создавать модели сетей и получения характеристик в виде графиков тех или иных параметров: время задержки прохождения пакета, пропускная способность на узле, загрузка серверов и т.д.

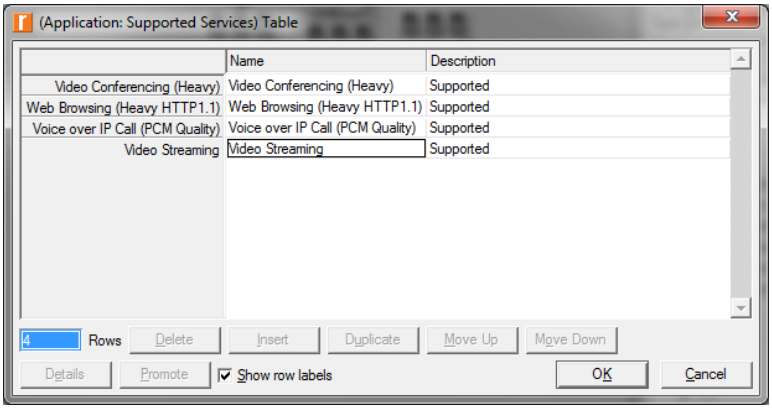

Рисунок 3.1 – Настройка различных видов трафика

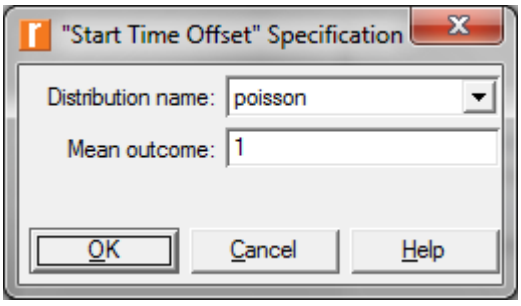

Рисунок 3.2 – Настройка закона генерации трафика

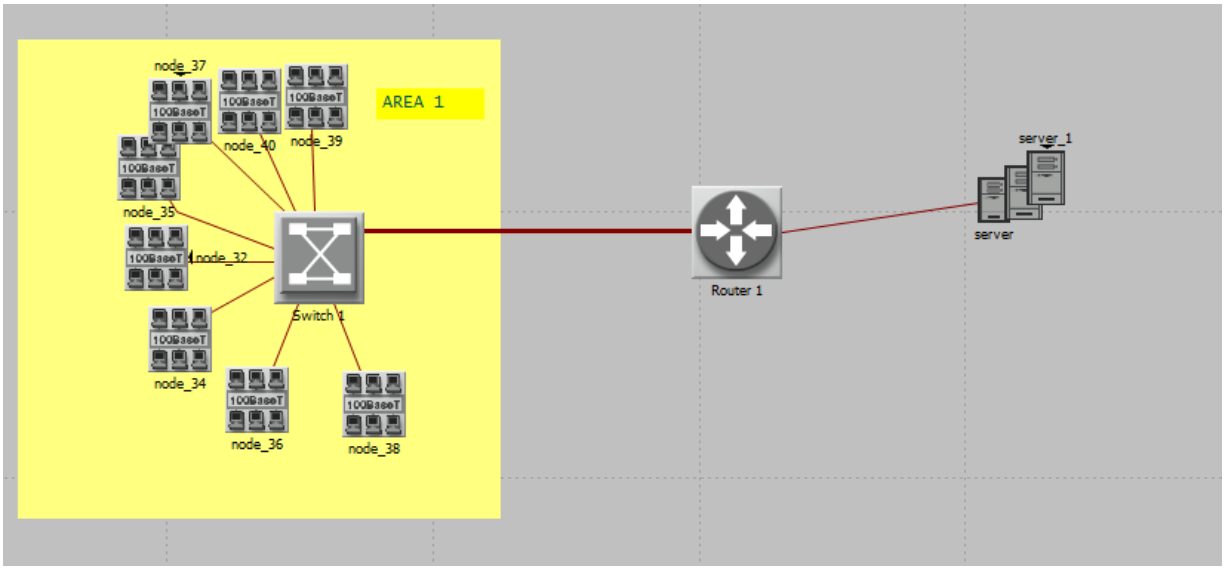

Рисунок 3.3 – Схема модели первого сценария

Первая модель имеет до 1000 абонентов и один маршрутизатор через который проходит трафик к серверам, обслуживающие клиентов предоставляя различные услуги: Web, VoIP, видео, аудио трансляции и другое. Были заданы спецификации генерации трафика по определенному закону и с интенсивностью 100 пакетов в секунду от подключенного устройства. На каждом элементе сети был присвоен индивидуальный IP-адрес. Изначально сеть была сконфигурирована по протоколу IPv4, затем рабочие станции и маршрутизаторы были перенастроены на работу по протоколу IPv6.

Запустив симуляцию работы сети продолжительностью 15 минут, были получены результаты, исследуемых характеристик. В качестве критерия оценки производительности сети используется средняя время пребывания пакета в сети с несколькими узлами коммутации, соединенными между собой дуплексными линиями связи с пропускной способностью $d_{k,l}$ байт/с между k и l узлами [44].

Каждый узел коммутации имеет буфер неограниченной емкости, средняя длина пакета равна $L_p=1/\mu$ байт. Поток данных, возникающей в узле i и предназначенный узлу j, является простейшим со средней интенсивностью $\lambda_{i,j}$ пакетов/с. Полная средняя интенсивность сети определяется по формуле:

$$\lambda = \sum_{i=1}^{N} \sum_{j=1}^{N} \lambda_{ij} \quad (1)$$

где *N:* – общее число узловых коммутаторов.

Выражение для средней задержки пакета выглядит следующим образом:

$$T = \frac{1}{\lambda} \sum_{k=1}^{N} \sum_{j=1}^{N} \gamma_{kl} t_{kl} \quad (2)$$

где t_{kl}:– среднее время пребывания сообщений в линии,

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

где $x_{kl}^{(i,j)}$: – доля потока, проходящая по линии (*k*,*l*) [61-63].

Помимо времени задержки сравнение производится по результатам загрузки серверов услуг пакетами и количеством бит, которые обрабатываются.

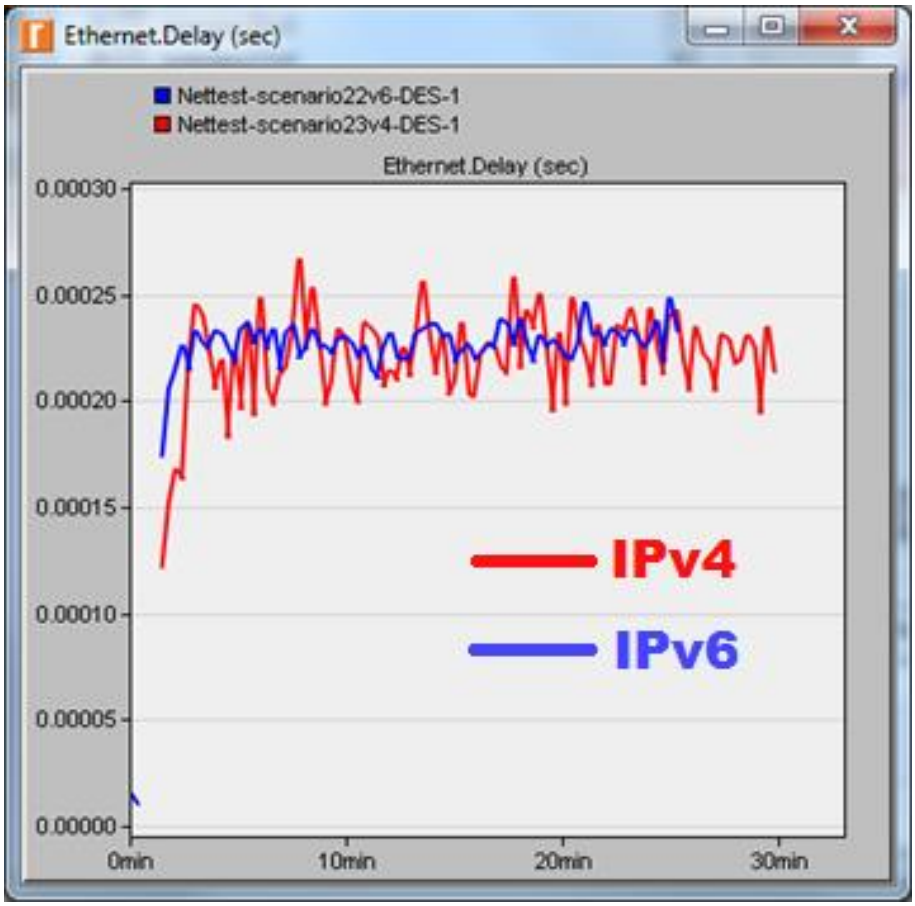

Рисунок 3.4 – Время задержки пакетов в первом сценарии

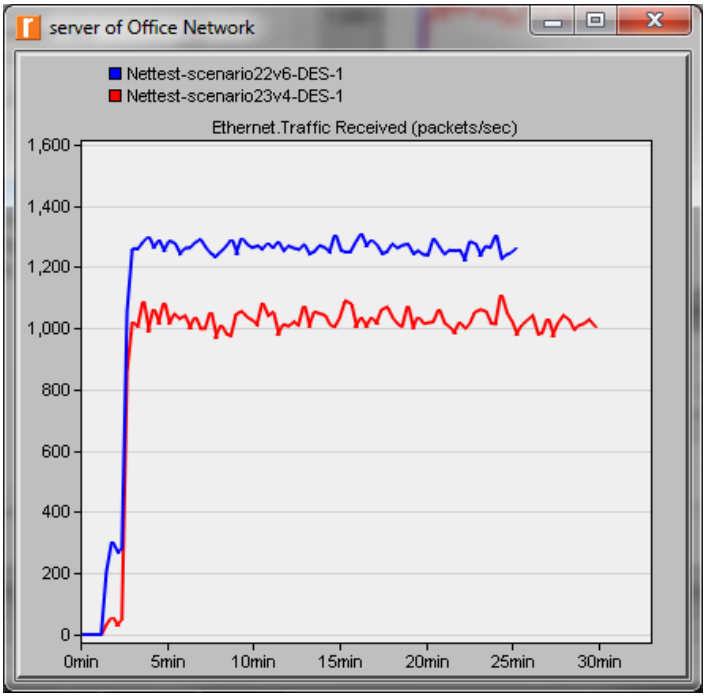

Рисунок 3.5 –Количество обрабатываемых пакетов на сервере в первом сценарии

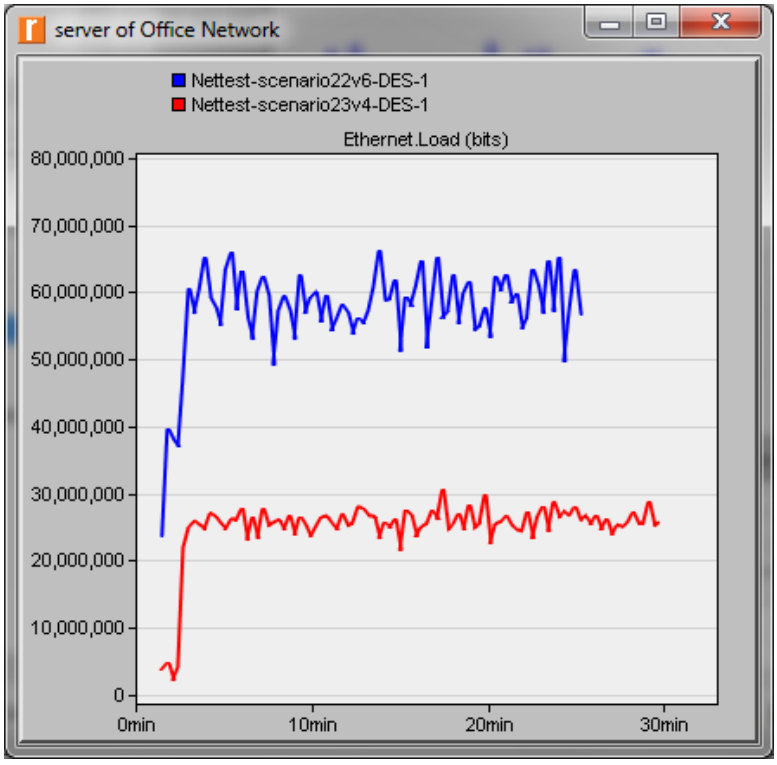

Рисунок 3.6 –Количество байт обрабатываемая сервером в первом сценарии

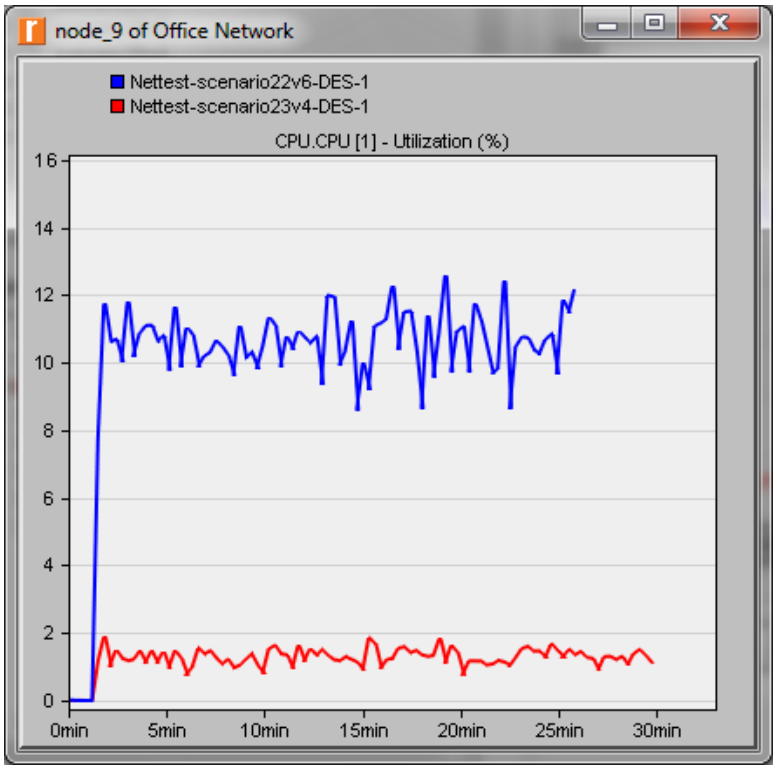

Рисунок 3.7 –Загрузка процессора маршрутизатора в первом сценарии

На полученном графике можно пронаблюдать какое время (в секундах) затрачивается пакетом при прохождении всего пути. Видно, что разница в использовании IP протоколов разных версий несильно влияет на время задержки прохождения пакета в малых сетях. В некоторые моменты времени работы сети, сетевая модель, сконфигурированная по протоколу IPv4, работает быстрее IPv6. Маршрутизатор в состоянии обработать требуемое количество пакетов, не внося существенное время на задерживании пакетов в очереди, держа их в памяти. Однако на графике, описывающем загрузку сервера на обработку запросов и передачу услуг, видно, что протокол IPv6 более нагружает сервер по количеству обрабатываемой бит информации, чем IPv4. При этом на графике, показывающем обрабатываемые пакеты данных, количество одинаковы у двух исследуемых протоколах.

Это объясняется тем что протокол IPv6 спроектирован разработчиками, учитывая современное развитие технологий передачи данных, с возможностью формирования пакетов с большим количеством данных. Это сокращает

количество пакетов в сети, что в соответствии сокращает количество бит технической передаваемой информации, разгружая канал передачи данных. При этом увеличивается нагрузка на маршрутизаторы, что можно пронаблюдать на графике загрузки процессора. Также требуется большая емкость буфера маршрутизатора, чтобы хранить большие пакеты, ожидающие в очереди на обработку.

Вторая модель более нагружена абонентами и промежуточными узлами. Она имеет в два раза больше абонентов, плюс ещё один маршрутизатор. Расширение сети должно увеличить время задержки в сети, загрузку маршрутизатора и загруженность серверов.

Как и с первой моделью, также была проведена симуляция работы сети продолжительностью 15 минут, сначала с сетью, сконфигурированной по протоколу IPv4, а затем по протоколу IPv6. Были получены исследуемые характеристики.

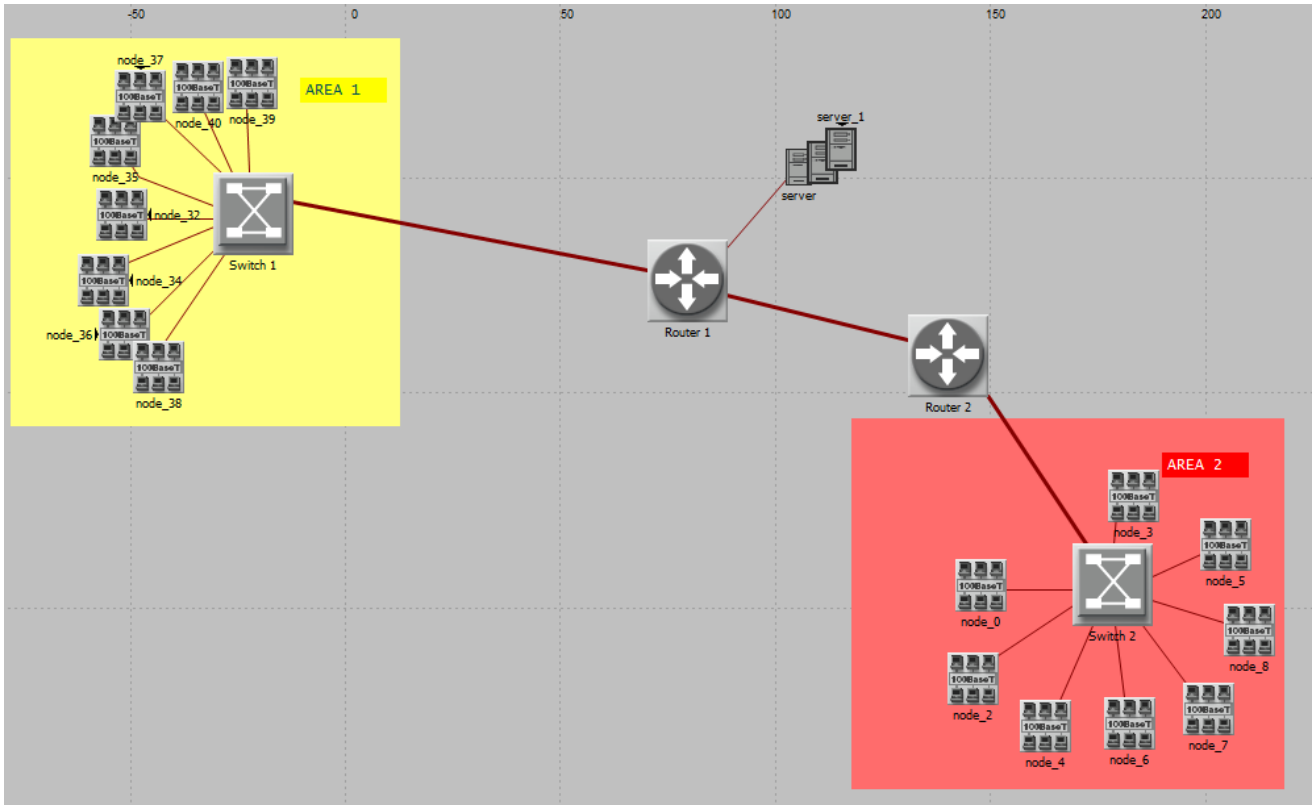

Рисунок 3.8 – Схема модели второго сценария

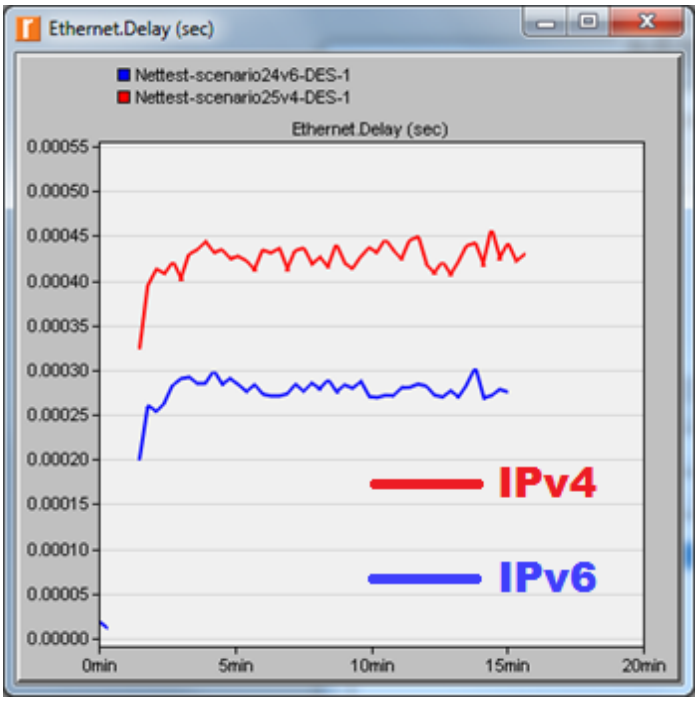

Рисунок 3.9 – Время задержки пакетов второго сценария

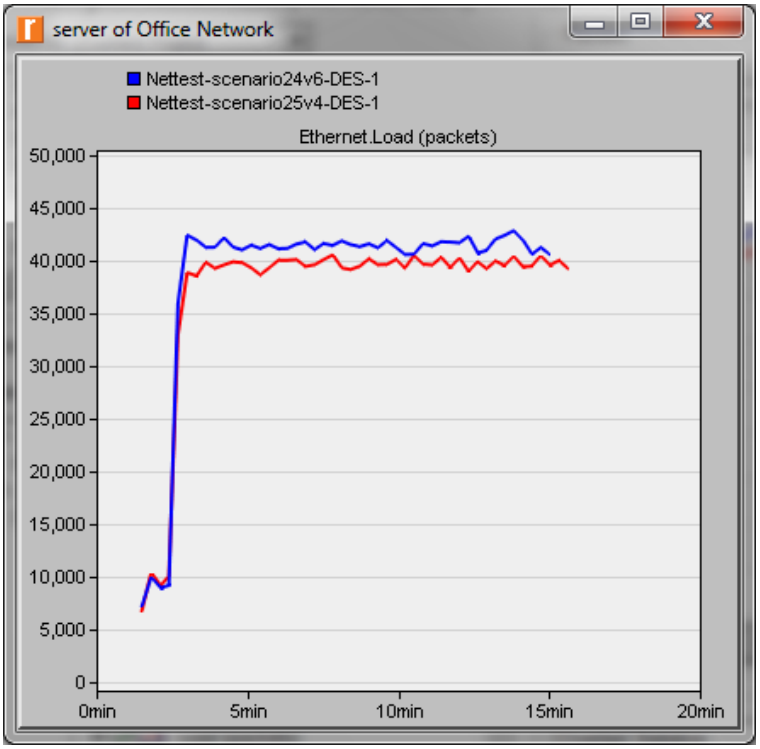

Рисунок 3.10 – Количество обрабатываемых пакетов сервером второго сценария

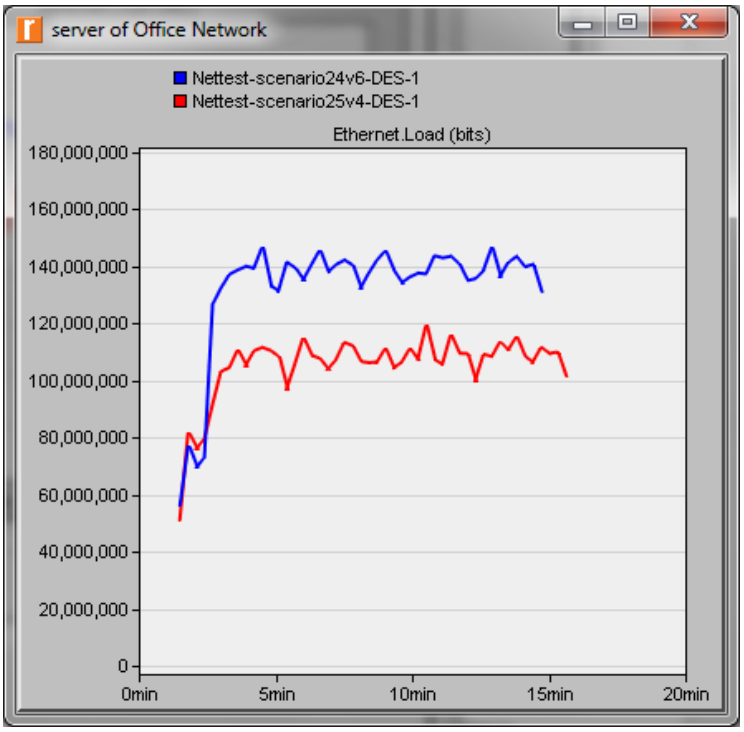

Рисунок 3.11 –Количество бит обрабатываемая сервером второго сценария

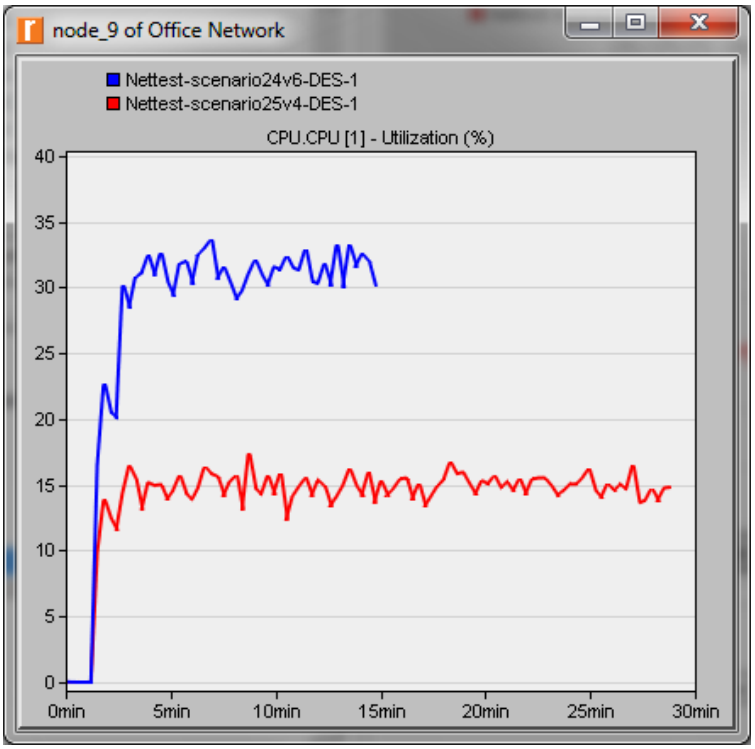

Рисунок 3.12 – Загрузка процессора маршрутизатора Router 1 во втором сценарии

По графикам задержки прохождения пакета наблюдается увеличение времени, т.к. на это влияет большее количество абонентов. Увеличилось и количество маршрутизаторов обрабатывающие пакеты. Время, за которое проходит пакет от точки до точки, используя межсетевой протокол IP версии 6 существенно меньше, чем у IPv4. Пакет в нагруженной абонентами и маршрутизаторами проходит на 40-50% быстрее при использовании IPv6, нежели, если сеть сконфигурирована по протоколу IPv4. Одна из причин увеличения скорости передачи, при использовании межсетевого протокола IP версии 6 в сравнении с IPv4, это упрощение заголовка. В результате оптимизации заголовка число полей сократилось с 14 до 8. Из него были изъяты поля «размер» — он теперь фиксированного размера и «контрольная сумма» — ее больше нет в IP пакете, т.к. более высокоуровневые протоколы (например TCP, UDP) ведут свои контрольные суммы, низкоуровневые (например Ethernet) свои. Смысла в еще одной контрольной сумме нет, поэтому ее изъяли. Поэтому маршрутизаторам не нужно анализировать пакет на предмет вычисления длины заголовка или пересчитывать контрольную сумму при изменении TTL пакета, что в свою очередь сокращает время обработки IP пакета в маршрутизаторе, позволяя передавать большее количество пакетов за то же время.

В этом сценарии также наблюдается увеличение обрабатываемой информации сервером. Сервера услуг формируют пакеты данных большего объема по протоколу IPv6, загружая канал передачи полезной нагрузкой. При этом на другом графике видно, что большие пакеты данных оказывают большую нагрузку на маршрутизаторы относительно IPv4.

Третья модель построена с максимальным количеством подключенных оконечных устройств, связанная с ограничением академической версией программы Riverbed Modeler. В данной модели в 4 раза больше абонентов, чем в первой и в 2 раза соответственно, чем во второй, а также сеть объединяют три маршрутизатора подсоединённых между собой последовательно, предостав-

ляя доступ к услугам подключенных абонентов. Большое количество подключенных рабочих станций вносит существенную нагрузку на работу сети, обработку пакетов маршрутизаторами, загрузку серверов. Все это влияет на задержки в сети, а также на пропускную способность маршрутизаторов.

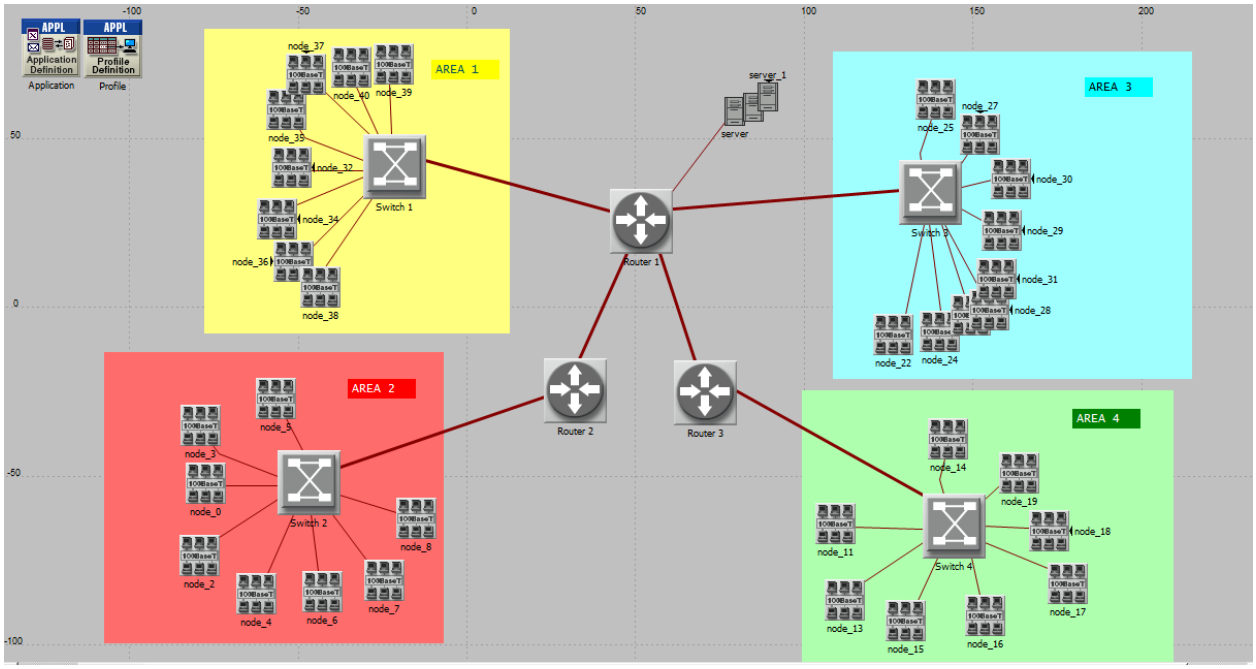

Рисунок 3.13 –Схема модели третьего сценария

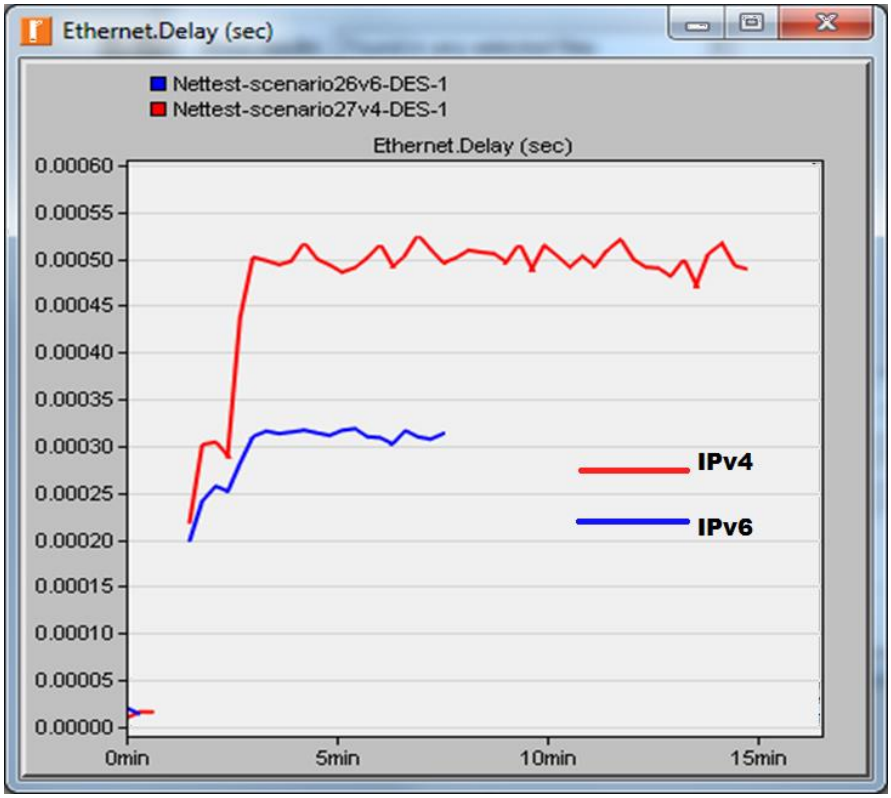

Рисунок 3.14 – Время задержки пакетов третьего сценария

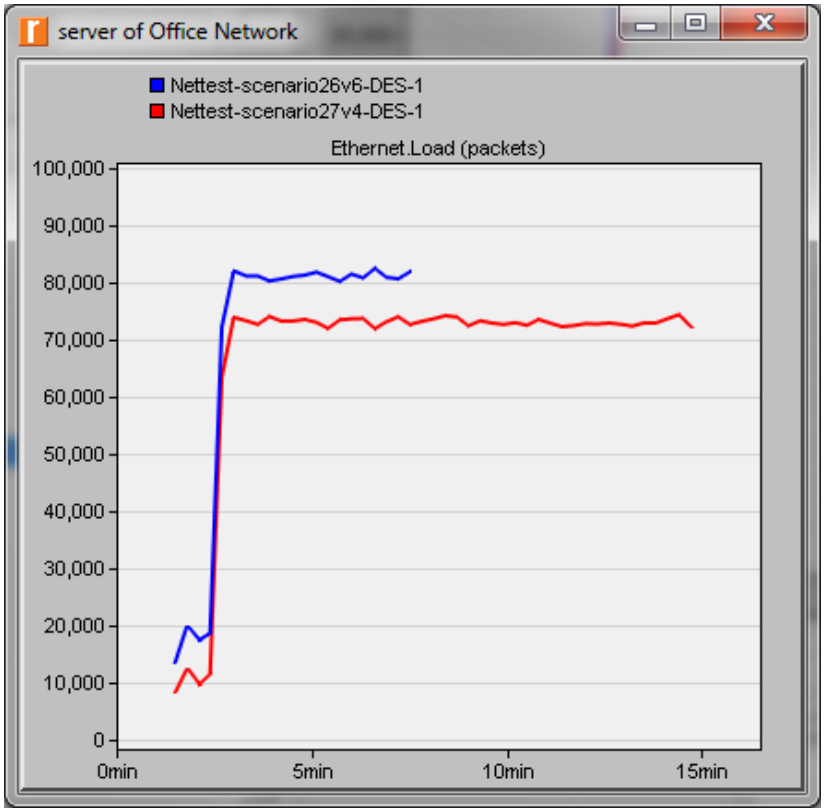

Рисунок 3.15 – Количество обрабатываемых пакетов сервером третьего сценария

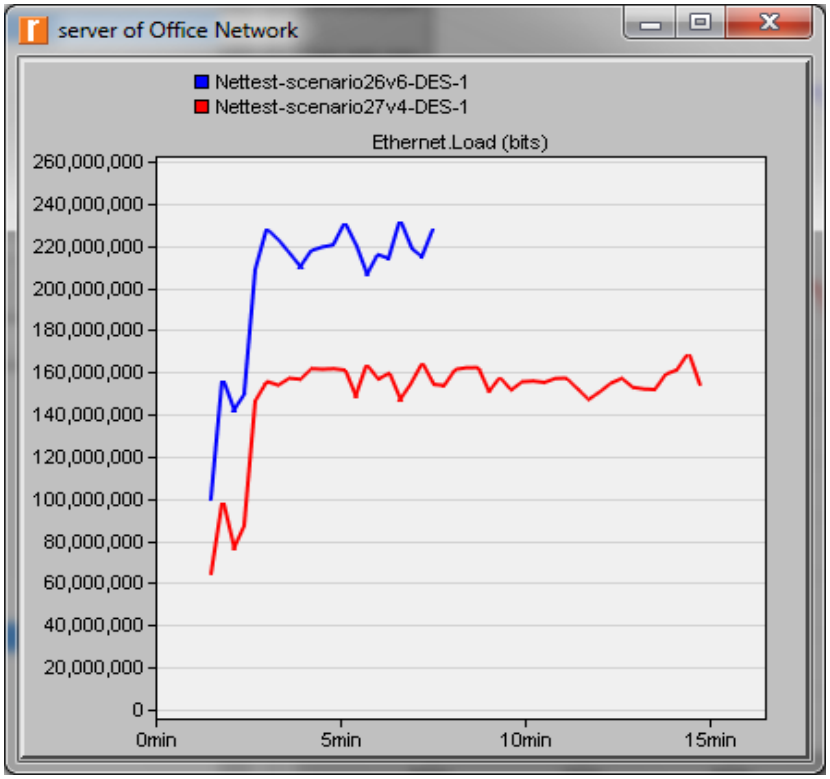

Рисунок 3.16 –Количество бит обрабатываемая сервером третьего сценария

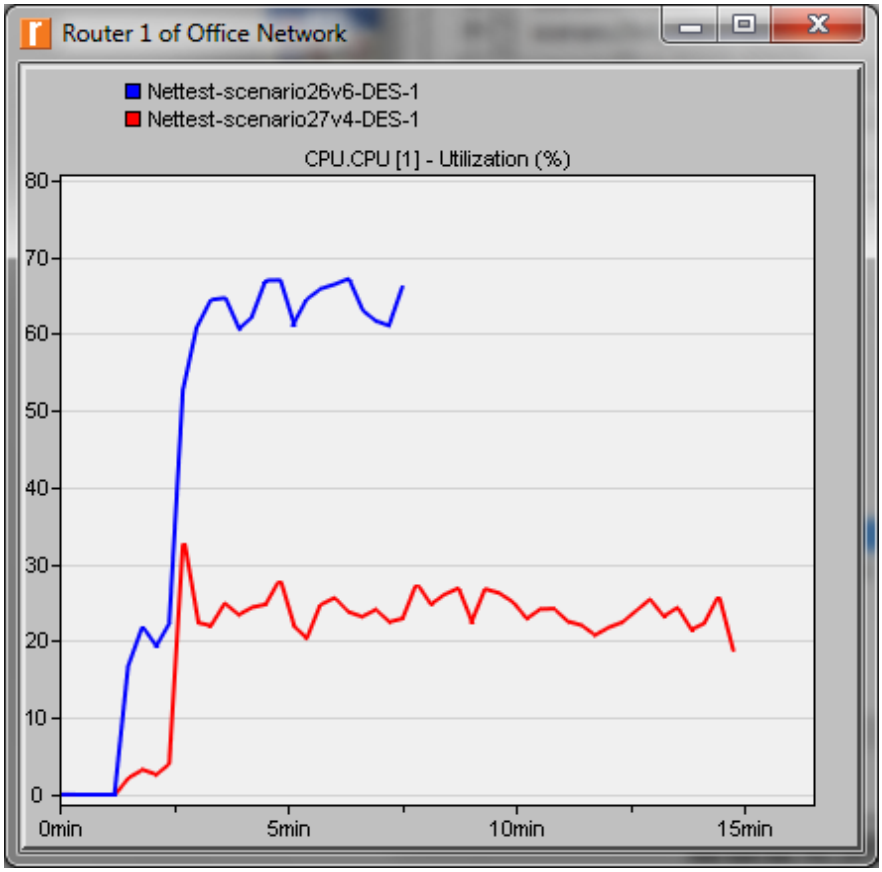

Рисунок 3.17 – Загрузка процессора маршрутизатора в третьем сценарии

Результат симуляции работы сети третьей модели показывает, что возрастание времени задержки прохождения пакетов при использовании межсетевого протокола IPv4 увеличивается кратно, с увеличением количества абонентов и числа узлов маршрутизации. В той же ситуации протокол IPv6 увеличивает время задержки намного меньше при том же количестве абонентов и маршрутизаторов. В третьей модели разница исследуемого параметра времени задержки прохождения пакета от точки до точки с конфигурацией сети IPv6 уже выше 50%, чем с конфигурацией IPv4, что существенно при работе сети.

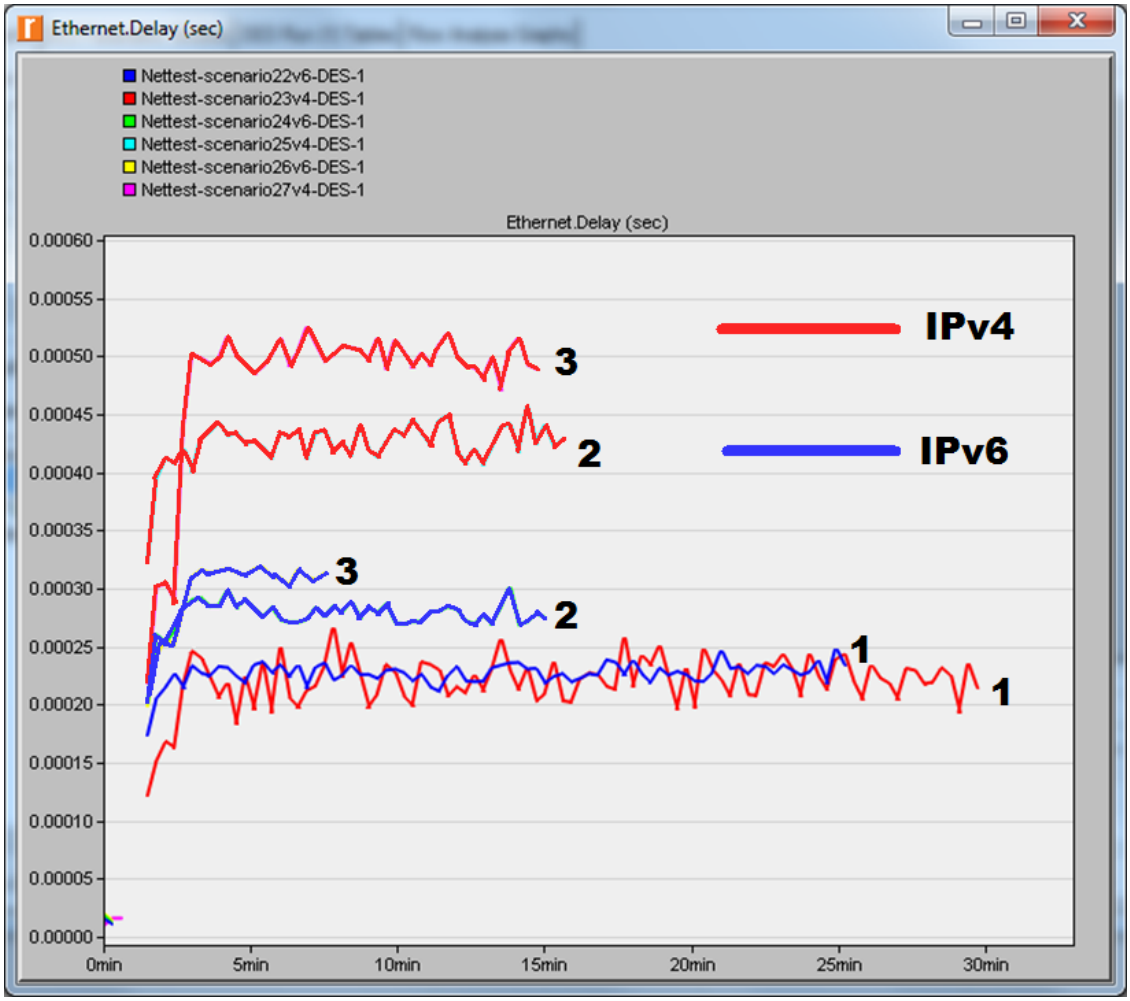

Рисунок 3.18 – Обобщенный график сравнения времени задержки пакетов всех 3 моделей

На сравнительном графике протоколов IPv4 и IPv6 отображена зависимость времени задержки прохождения пакетов от размеров сети. По данной сравнительной характеристике можно сделать вывод, что использование протокола IPv6 с увеличением размеров сети дает преимущество перед IPv4.

3.2 VLAN-каналы по услугам

В данной части исследуется характеристики мультисервисной сети при использовании технологии VLAN для предоставления услуг клиентам. Для эксперимента взята та же типовая схема мультисервисной сети связи микрорайона.

В сети имеются классические услуги различных unicast-потоков

• Internet-трафик (HSI – High Speed Internet);

• IP-телефония (VoIP);

• VoD-сервисы (VoD);

• Видеоконференсвязь-сервисы ();

И Multicast-сервисы:

• широковещательное телевидение (BTV);

• музыкальные каналы и др.

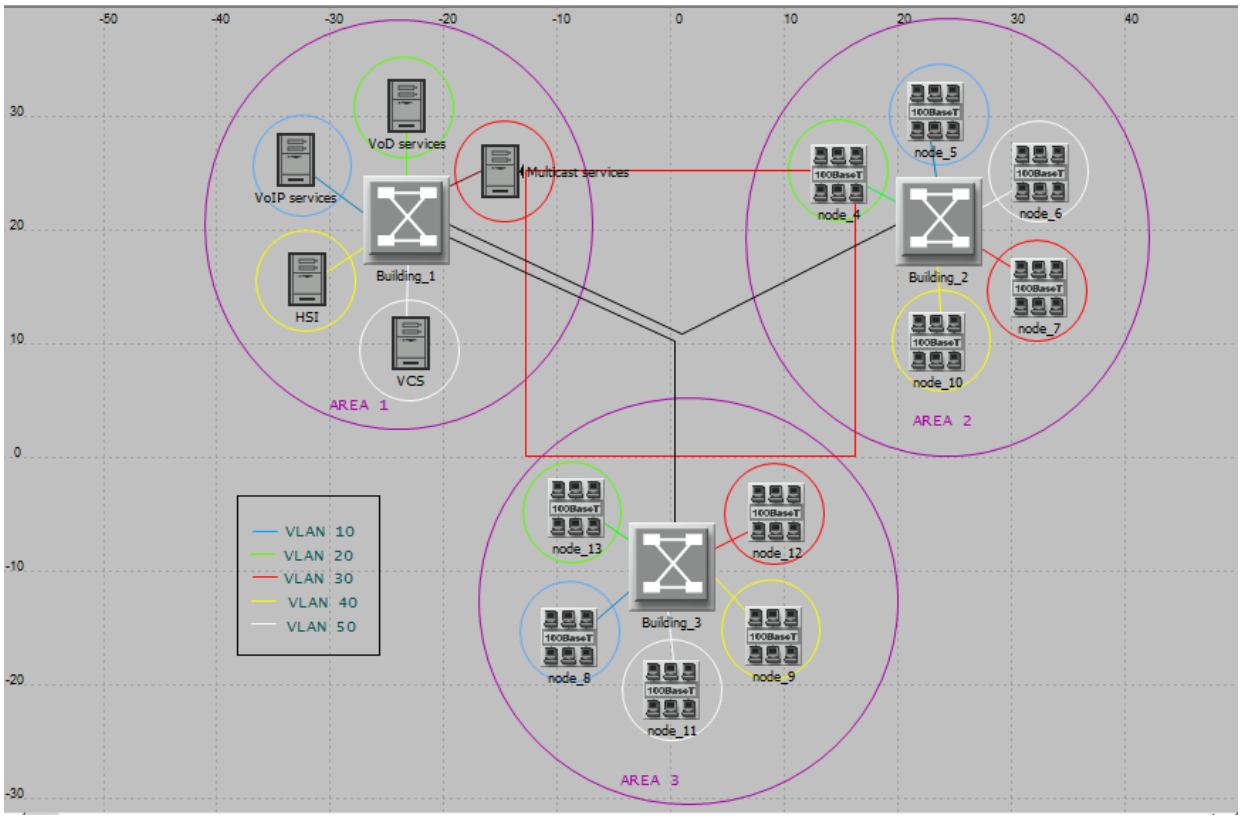

Рисунок 3.19 – Схема модели с VLAN

Модель состоит из трех районов, объединенных тремя коммутаторами. В одном районе сосредоточены системы формирования услуг, которые распространяются по созданным на коммутаторах VLAN-каналы до абонентов в два других района. В каждом районе по 1000 пользователей, подключенные к тем или иным услугам. Данная технология (имеющая название Triple Play) имеет некоторые преимущества перед распространением услуг в общем потоке данных. Использование VLAN каналов по услугам позволяет в некоторой мере разгрузить коммутаторы, уменьшив количество технической информации при передаче пакетов.

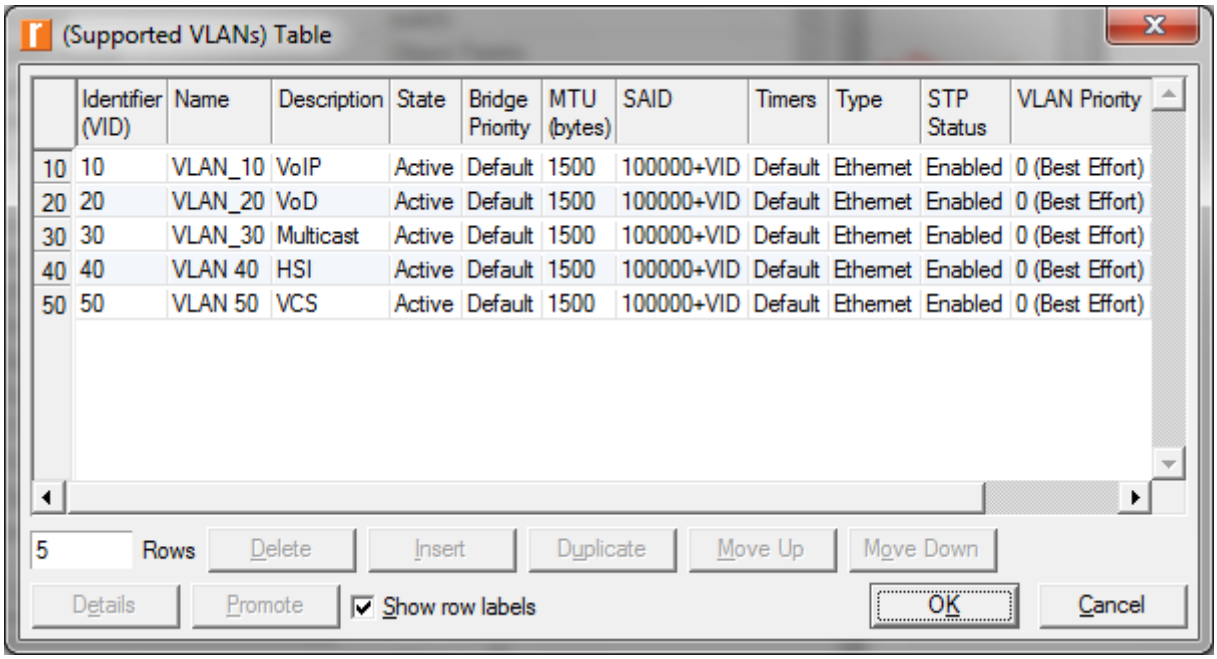

Рисунок 3.20 – Настройка VLAN на коммутаторе 1

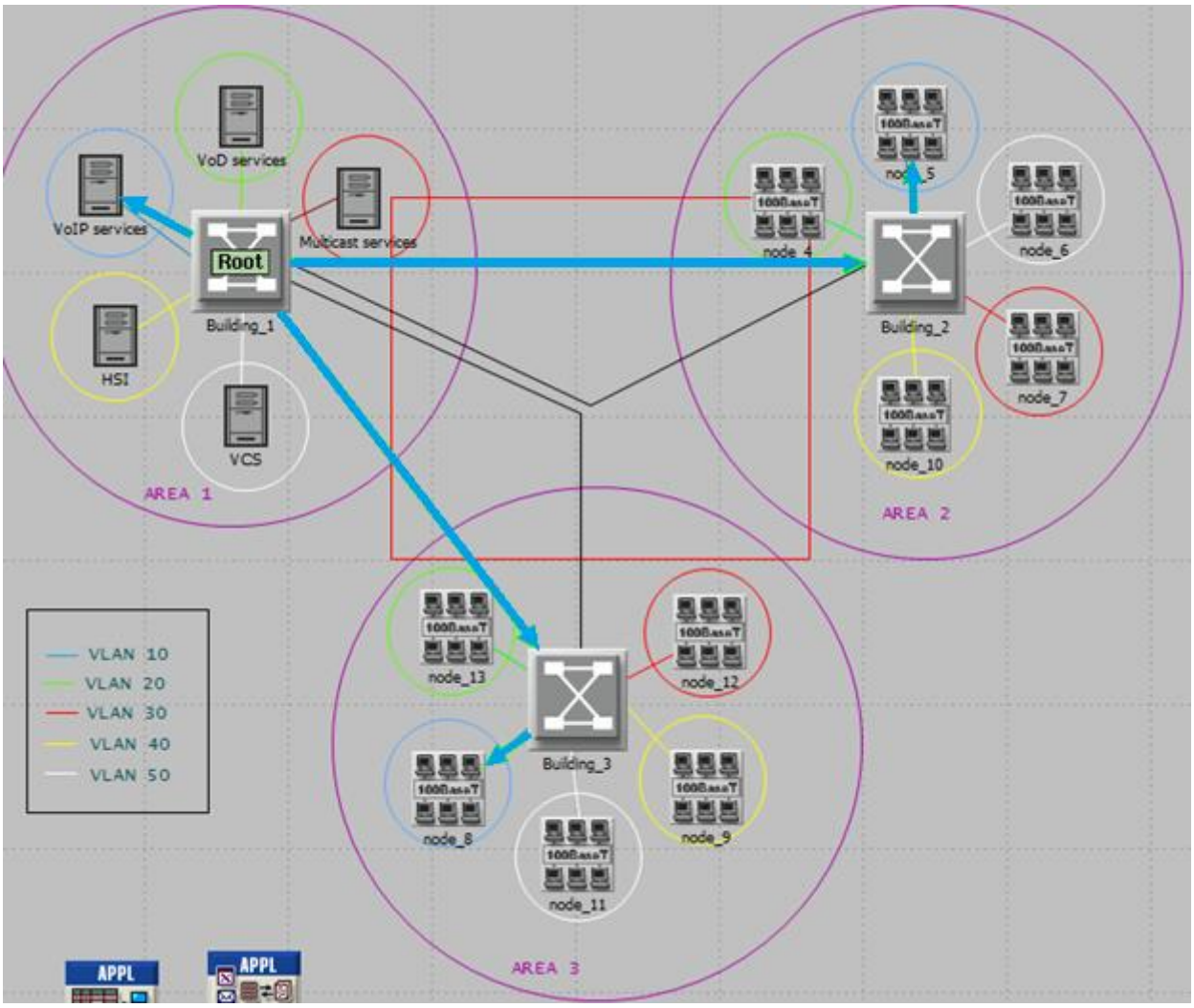

Рисунок 3.21 – Рисунок показывающий VLAN-канал VoIP

Таблица 3.1 - План организации VLANs

Отделы организации	VoIP	VoD	Multicast-сервисы	HSI	Видеоконференцсвязь
Номера VLAN	10	20	30	40	50

В программе Riverbed Modeler была построена модель и сконфигурированы 5 VLAN каналов по услугам. Также созданы Trunk-каналы между коммутаторами. Имитация работы модели была проведена продолжительностью 60 секунд с использованием VLAN каналов, а затем без них. Были получены результаты времени задержки прохождения пакетов от точки до точки и загруженность коммутаторов в зависимости от принятой информации в байтах в

каждый момент работы сети. По графику время задержки пакетов наблюдается разница, где сеть с использованием VLAN работает на четверть быстрее. Также на другом графике, описывающем загруженность коммутатора принятыми байтами информации, сеть с VLAN загружает коммутаторы на четверть меньше, чем в сети, где все услуги передаются в общем канале передачи данных.

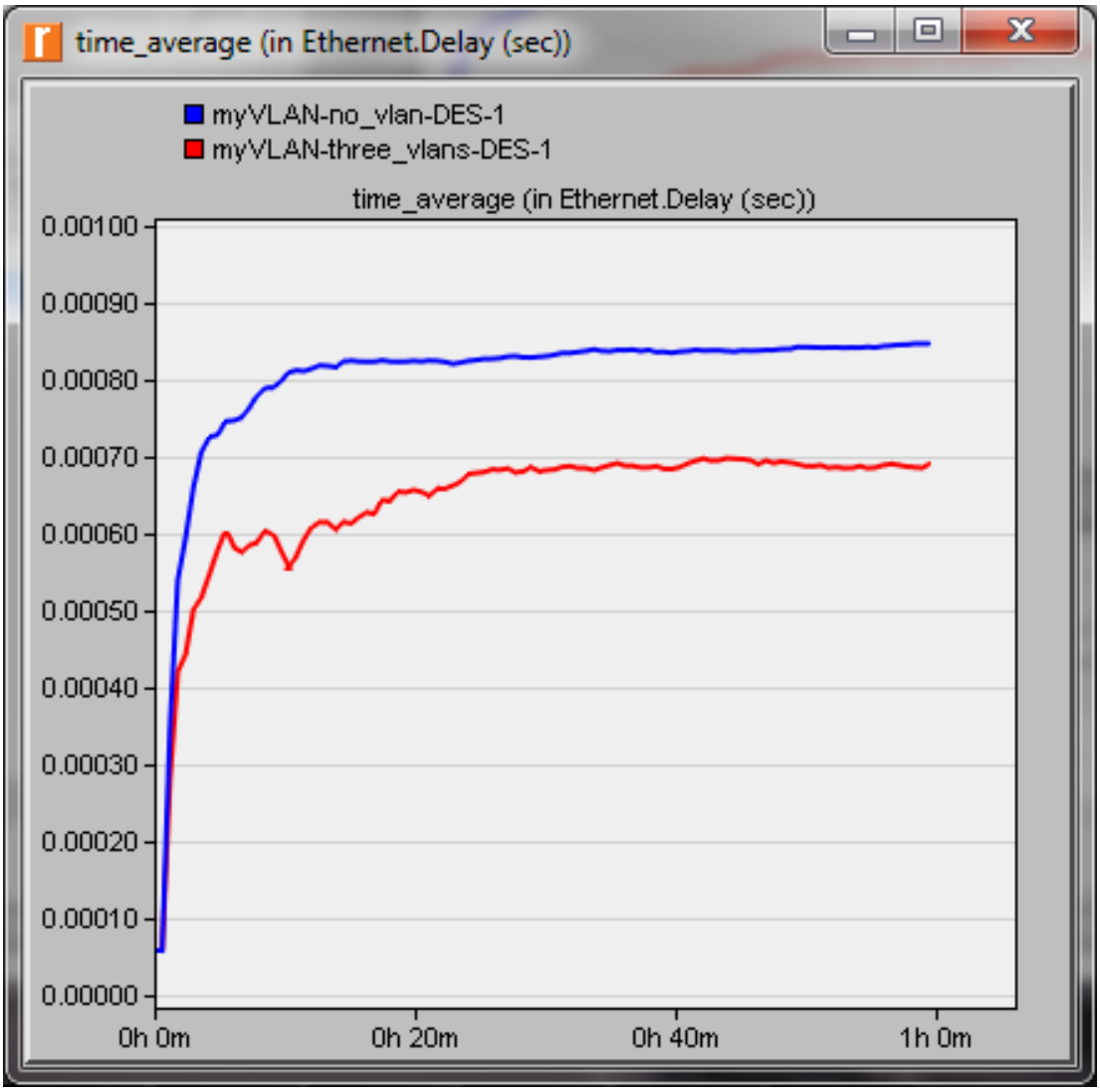

Рисунок 3.22 – Время задержки с VLAN и без использования VLAN

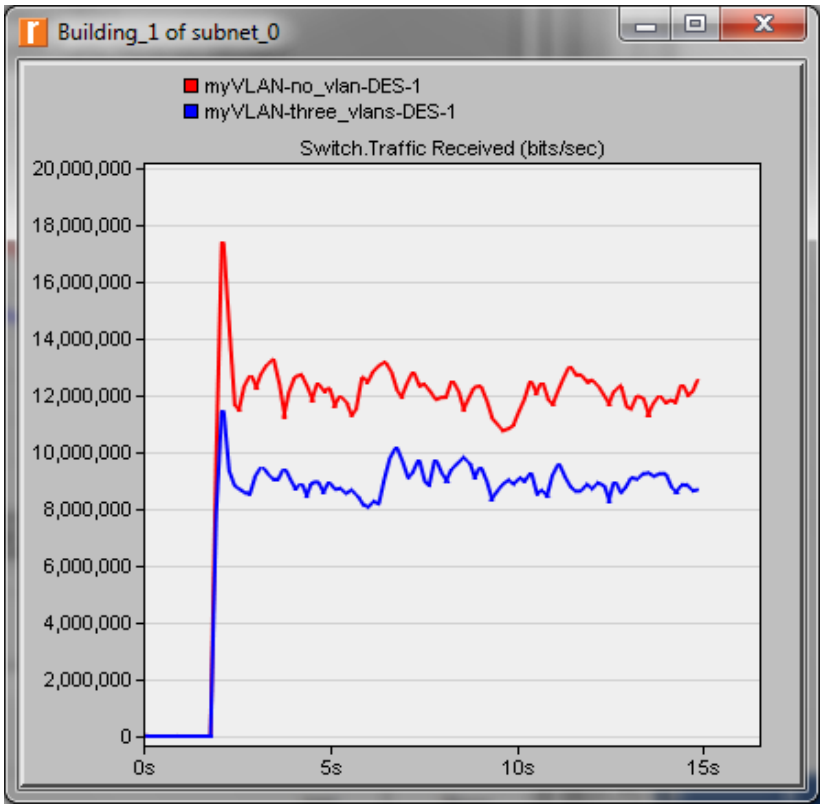

Рисунок 3.23 – Количество бит в секунду принятых коммутатором 1 с VLAN и без использования VLAN

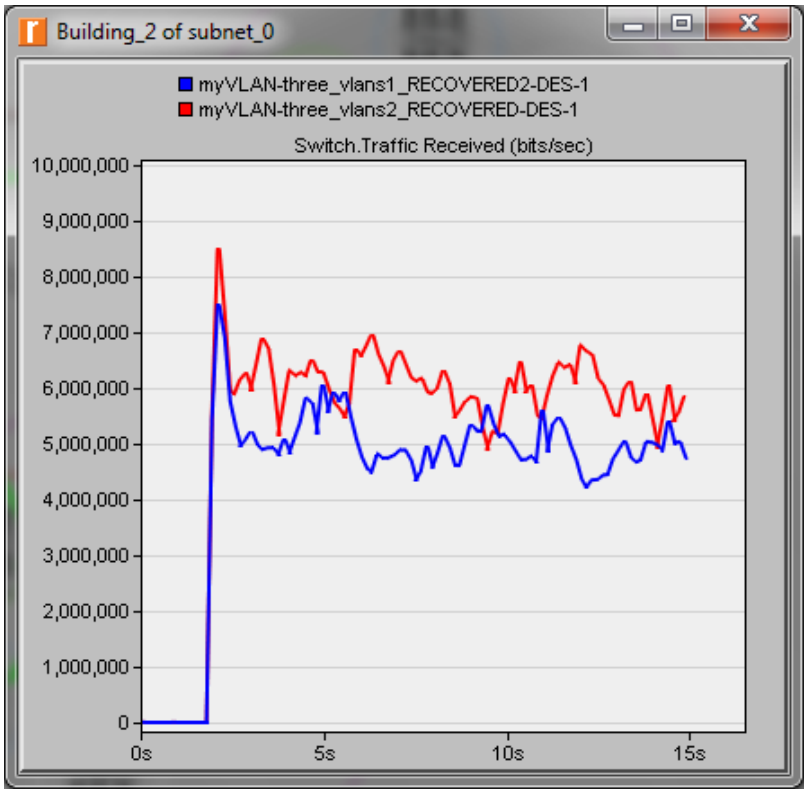

Рисунок 3.24 – Принятый трафик на втором коммутаторе

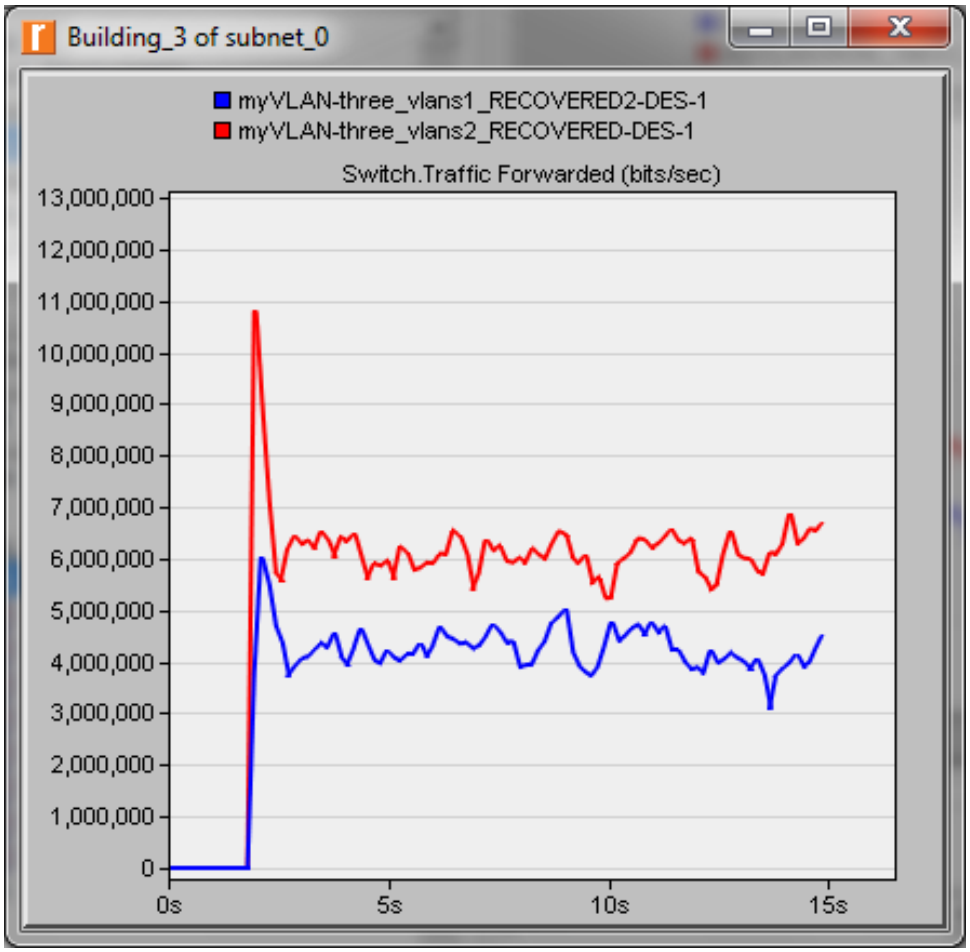

Рисунок 3.25 – Переданный трафик на третьем коммутаторе

Как видно из приведенного графиков, задержка значительно уменьшилась при использовании технологии VLAN и загрузка коммутаторов снизилась. Это можно объяснить тем, что количество пакетов в сети сокращается, ввиду того что отпадет необходимость массовой рассылки широковещательных пакетов всем работающим машинам. Широковещание ограничивается пределами VLAN и не выходит за его границы.

Результаты компьютерного моделирования показали, что использование технологии виртуальных локальных сетей (Virtual Local Area Network VLAN) в мультисервисных сетях, позволяет существенно снизить количество пакетов, находящихся в сети, а также уменьшить задержку и среднее время пребывания в сети, увеличивая тем самым производительность мультисервисной сети связи.

ЗАКЛЮЧЕНИЕ

В ходе выполнения работы в среде Riverbed Modeler была разработана имитационная модель мультисервисной сети. Разработанная имитационная модель позволяет моделировать поведение телекоммуникационной сети при различных сценариях, оценивать её пропускную способность, определять уровень загрузки буферов сетевых устройств, задержки сетевого трафика и т.п.

С помощью разработанной модели сетевой инфраструктуры микрорайона были проведены эксперименты по оценке работоспособности сети с конфигурациями межсетевого протокола различной версии: IPv4 и IPv6. Также проведены эксперименты по оценке эффективности работы сети и величины нагрузки, создаваемой на сетевые узлы при использовании технологии VLAN-каналов.

Основные результаты магистерской диссертации:

- получены характеристики работы сети при использовании межсетевого протокола IPv4 и IPv6;
- определено, что протокол IPv6 по полученным характеристикам имеет меньшее время задержки пакетов, чем при использовании протокола IPv4;
- IPv6 передает большее количество бит информации в одном пакете, по сравнению с IPv4;
- получены характеристики разделения сети на VLAN-каналы по видам предоставляемых услуг,
- в результате моделирования представлено, что использование VLAN-каналов снижает нагрузки на узлы по причине снижения широковещания в сети.

Анализ полученных результатов показал, что использование IPv6 способствует быстрой работе сети и большей пропускной способности, превос-

ходя устаревший протокол IPv4 по многим показателям. Однако стоит заметить, что в сетях малого масштаба сконфигурированных по IPv4 или по IPv6, разницы в скорости работы сети не наблюдается, в то же время загрузка сетевых узлов возрастает в сетях, настроенных по IPv6. Использование технологии VLAN при передаче услуг до абонентов по выделенным виртуальным каналам позволяет снизить нагрузку на активное сетевое оборудование и собственно на всю сеть, позволяя обрабатывать больше полезной информации.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

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

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

3. Общее описание RFC 793, 1981

4. Общее описание RFC 791, 1981

5. Общее описание RFC3330: Special-use IPv4 addresses (англ.); заменён RFC5735: Special-use IPv4 addresses (англ.), 2002

6. Общее описание RFC1700: Assigned Numbers, 1994

7. Общее описание RFC1122: Requirements for Internet Hosts — Communication Layers, 1989

8. Общее описание RFC1918: Address allocation for private internets, 1996

9. Общее описание RFC3927: Dynamic configuration of IPv4 link-local addresses, 2005

10. Новиков, Ю.В., Основы локальных сетей: курс лекций: 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. - 360 с.

11. 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.

12. Олифер В. Г., Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов / В. Г. Олифер, Н. А. Олифер. — 3-е изд. — СПб.:Питер, 2006. — 958 с.: ил.

13. Гольдштейн, Б.С. Протоколы сети доступа [Текст]. Том 2. 2-е изд., перераб. и доп. / Б. С. Гольдштейн. - М.: Радио и связь, 2002.

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

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

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

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

18. Берлин, А.Н. Основные протоколы Интернет – Изд.: Бином, 2013 - 504

19. Семенов, Ю.А. Алгоритмы телекоммуникационных сетей. Часть 1, 2 и 3. - изд.: Национальный Открытый Университет "ИНТУИТ" 2016 - 832

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

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

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

23. IPv6. Администрирование сетей / Н. Р. Мэрфи, Д. Мэлоун Изд.: Кудиц-образ, 2007 год, 320 с.

24. Иртегов, Д.В. Введение в сетевые технологии СПб.: БХВ-Петербург, 2004 – 560 с.

25. Общее описание RFC 1883, 1995

26. Общее описание RFC 5006, 2007

27. Общее описание RFC 6106, 2010

28. IPv6 используется уже в 10% сетевых устройств мира [Электронный ресурс]/ www.overclockers.ru - информационных сайт

https://www.overclockers.ru/softnews/73277/ipv6-ispolzuetsya-uzhe-v-10-setevyh-ustrojstv-mira.html (дата обращения 20.04.2016)

29. Cisco: к 2015 г. количество сетевых устройств может превысить 15 млрд [Электронный ресурс]/ www.cisco.com - официальный сайт компании Cisco http://www.cisco.com/web/RU/news/releases/txt/2011/060111b.html

30. Скляр, Б. Цифровая связь. Теоретические основы и практическое применение Изд. 2-е, испр. : Пер. с англ. М. : Издательский дом "Вильямс", 2003. — 1104 с. : ил.

31. Тимофеев, А.В. Адаптивное управление и интеллектуальный анализ информационных потоков в компьютерных сетях. – СПб.: Анатолия, 2012, 280 с Смелянский, Р. Л. Компьютерные сети. В 2 томах. Том 2. Сети ЭВМ:Р. Л. Издательство: Академия ISBN: 978-5-7695-7153-4.978-5-7695-7152-7, 2011 – 240 стр.

32. . TCP/IP. Для профессионалов / Т. Паркер, К. Сиян; 3-е изд. СПб.: Питер, 2004. - 859 с.: ил.

33. Дилип, Н. Стандарты и протоколы Интернета – Изд.: Русская Редакция, 2000 – 384 с.

34. Анализ сетевых протоколов: Лабораторный практикум по курсу «Сети ЭВМ и телекоммуникации»/ Н. Н. Коннов, В. Б. Механов. – Пенза: Изд-во ПГУ, 2010 – Ч. 1. – 68 с.

35. Web-протоколы. Теория и практика / Кришнамурти Б., Дж. Рексфорд; изд.: Бином, 2010 – 592 с.

36. Кульгин, М.В. Компьютерные сети. Практика построения, 2-е изд. — СПб.: Питер, 2003. — 416 с.

37. Проектирование и внедрение компьютерных сетей / М. Палмер, Р. Б. Синклер; Изд.: БХВ-Петербург 2004 - 752

38. Моделирование и синтез оптимальной структуры сети Ethernet / Благодаров А. В., Пылькин А. Н., Скуднев Д. М. и др.; Изд.: Горячая линия-Телеком, 2014 – 112 с.

39. Таненбаум, Э. Компьютерные сети, Учебное пособие по компьютерным сетям. 5-е изд. – СПб.: Питер, 2012. — 960 с.

40. Вишневский, В.М. Теоретические основы проектирования компьютерных сетей – Москва: Техносфера, 2003. - 512с.

41. Семенов, Ю.А. Телекоммуникационные технологии // book.itep.ru: сервер по телекоммуникационным технологиям. 2014. URL: http://book.itep.ru/4/41/eth_4111.htm (дата обращения: 11.06.2014).

42. Битнер, В. И. Михайлова, Ц. Ц. Сети нового поколения – NGN – М.: Горячая линия – Телеком, 2011 – 227 стр.

43. Берлин, А. Н. Оконечные устройства и линии абонентского участка информационной сети – М.: НОУ "Интуит", 2016г.- 395с.

44. Гулиян, Г. Б. Распределенные сети: современные технологии и основы проектирования – Изд.: НОЧ «МФПУ «Синергия» 2007 – 22 с.

45. Построение коммутируемых компьютерных сетей / Смирнова Е. В., Баскаков И. В., Пролетарский А. В. и др.; изд.: НОУ "Интуит"2016 – 202

46. Смирнова, Е.В. Технологии современных сетей Ethernet. Методы коммутации и управления потоками данных – изд.: БХВ-Петербург, 2012 – 272

47. Поляк-Брагинский, А.В. Локальные сети. Модернизация и поиск неисправностей – СПб.: БХВ-Петербург, 2006— 640 с.

48. Епанешников, А. М. Локальные вычислительные сети – изд.: Диалог-МИФИ, 2005 – 224 с.

49. Чекмарев, Ю.В. Локальные вычислительные сети - М.: ДМК Пресс, 2009 - 200 с.

50. Никифоров, С. В. Введение в сетевые технологии. Элементы применения и администрирования сетей : Учеб.пособие для вузов / С.В. Никифоров .- М. : Финансы и статистика , 2003 - 223 с.

51. Сети и телекоммуникации: учеб. пособие для вузов / Пескова С. А., Кузин А. В. и др. 3-е изд., стер. .- М. : Академия, 2008 .- 350 с.

52. Семенов, А.Б. Проектирование и расчет структурированных кабельных систем и их компонентов. – М.: ДМК Пресс; М.: Компания АйТи, 2003. – 416 с.

53. Кузьменко, Н. Г. Компьютерные сети и сетевые технологии – изд.: Наука и техника, 2013 – 368 с.

54. Основы локальных сетей / Новиков Ю.В., Кондратенко С.В. - М.: Интернет-Университет Информационных Технологий, 2005. — 360 с.

55. Вычислительная техника, сети и телекоммуникации. Учебное пособие для ВУЗов / Гребешков А.Ю., Попова Н.А. - М.: Гор. линия-Телеком, 2015 - 190 с.

56. Телекоммуникационные системы и сети: Учебное пособие. В 3-х томах под. ред. профессора В.П.Шувалова. - Изд.3-е,испр. и доп.- М.: Горячая линия-Телеком, 2003 - 647 с.: ил.

57. Вычислительные системы, сети и телекоммуникации / Пятибратов А. П., Гудыно Л. П., Кириченко А. А. М.: Финансы и статистика, 2004. — 512 с.: ил.

58. Тарасов, В.Н. Проектирование и моделирование сетей ЭВМ в системе OPNET Modeler: лабораторный практикум / В.Н. Тарасов, Н.Ф. Бахарева, А.Л. Коннов, Ю.А. Ушаков. – Оренбург: 2012. – 258 с.

59. Описание программного продукта Riverbed Modeler [Электронный ресурс]/ www.riverbed.com - официальный сайт компании Riverbed http://www.riverbed.com/gb/products/steelcentral/steelcentral-riverbed-modeler.html

60. Проектирование и внедрение компьютерных сетей / М. Палмер, Р. Б. Синклер – «БХВ-Петербург», 2004 – 740

61. Гулевич Д. С. Сети связи следующего поколения: Учеб. пособие / Д.С. Гулевич - Интернет-университет информационных технологий – ИНТУИТ.ру, БИНОМ. Лаборатория знаний, 2007. – 184 с.

62. Величко, В.В. Телекоммуникационные системы и сети: Учеб. пособие В 3 томах. Том 3. Мультисервисные сети / В.В. Величко, Е.А. Субботин, В.В. Шувалов, А.Ф; под ред. В.П. Шувалова. - М.: Горячая линия – Телеком, 2005. – 592 с.

63. Ершов, В.А. Мультисервисные телекоммуникационные сети: Учеб. пособие / В.А. Ершов, Кузнецов Н.А. – М.: Изд-во МГТУ им. Н.Э. Баумана, 2009. – 432 с.: ил.