

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

**РАЗРАБОТКА МОДЕЛИ КАМПУСНОЙ СЕТИ  
В СРЕДЕ OPNET MODELER**

Магистерская диссертация  
обучающегося по направлению подготовки 11.04.02 Инфокоммуникационные  
технологии и системы связи,  
магистерская программа «Системы и устройства радиотехники и связи»  
очной формы обучения, группы 07001532  
Ба Хала Ашраф Мохаммед Али

Научный руководитель  
доцент кафедры информационно-  
телекоммуникационных систем и  
технологий НИУ «БелГУ», к.т.н.,  
Девицына С.Н.

Рецензент  
доцент кафедры прикладной  
информатики и информационных  
технологий  
НИУ «БелГУ», к.т.н.,  
Маматов Е.М.

БЕЛГОРОД 2017

## ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ.....	4
1 ОБЩИЕ СВЕДЕНИЯ О БЕСПРОВОДНЫХ СЕТЯХ.....	6
1.1 Беспроводные технологии и стандарты беспроводных сетей.....	6
1.1.1 Стандарт Wi-Fi .....	6
1.1.2 Стандарт WiMAX.....	9
1.2 Методы маршрутизации в беспроводных сетях .....	12
2 ОБЗОР ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ МОДЕЛИРОВАНИЯ БЕСПРОВОДНОЙ КАМПУСНОЙ СЕТИ ГТУ г. САНА .....	17
2.1 Понятие и методы моделирование .....	17
2.2 Обзор и сравнение программного обеспечения для моделирования сетей связи.....	19
2.2.1 OPNET modeler 17.5.....	19
2.2.2 Симулятор OMNeT++.....	22
2.2.3 Симулятор NS-2 .....	24
2.2.4 Симулятор NS-3 .....	27
2.2.5 Программа Cisco Packet Tracker .....	28
2.3 Сравнение сетевых симуляторов.....	33
3 РАЗРАБОТКА И ИССЛЕДОВАНИЕ ИМИТАЦИОННОЙ МОДЕЛИ БЕСПРОВОДНОЙ КАМПУСНОЙ СЕТИ.....	35
3.1 Карта сети .....	35
3.2 Разработка имитационной модели беспроводной сети четвертого этажа главного корпуса ГТУ г.Сана .....	39
3.2.1 Создание эскиза сети .....	39
3.2.2 Моделирование сети в OpNet Modeler 17.5.....	39
3.3 IP протокол, маршрутизация в беспроводной сети связи.....	60
3.3.1 Создать новый проект.....	61

3.3.2 Создание и Конфигурирование сети.....	61
3.3.3 Конфигурирование маршрутизатора .....	62
3.3.4 Добавление оставшихся локальных сетей.....	63
3.3.5 Выбор Статистики .....	64
3.3.6 Настроить симуляцию .....	64
3.4 Пинг-сценарий.....	66
3.4.1 Сценарий со сбоям в сети.....	67
3.4.2 Запуск симуляции .....	69
3.4.3 Просмотр результатов .....	70
3.5 IP-адресация для интерфейса.....	72
3.6 Получение отчета Ping.....	74
3.7 Сравнение содержимого таблиц маршрутизации.....	75
ЗАКЛЮЧЕНИЕ .....	77
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ .....	78

## **ВВЕДЕНИЕ**

В настоящее время для моделирования и исследования информационных систем и сетей широко используются компьютерные технологии, что выражается в создании разного рода специализированных программных продуктов. Подобные программы, как правило, сочетают в себе аналитические методы и средства имитационного моделирования, позволяя всесторонне рассмотреть и проанализировать объект исследования. Созданием таких программ занимается множество компаний, одной из которых является Opnet Inc.

Компания Opnet создает и поддерживает несколько пакетов программ – Opnet Modeler, Opnet IT Guru, Opnet SP Guru и пр. Каждый из них имеет свои особенности и область применения – например, для моделирования оптических сетей (Opnet SP Guru). Наиболее универсальным по перечню решаемых задач в этом списке выглядит Opnet Modeler, который используется в данной диссертационной работе.

Целью магистерской диссертации является разработка имитационной модели кампусной сети государственного технического университета города Сана (ГТУ г. Сана) Республики Йемен для проверки её работоспособности при передаче трафика различного вида с учетом требований QoS.

Учитывая, что сети образовательных учреждений имеют сложную инфраструктуру, и основным является требования доступности сетевых сервисов в любой точке университетского кампуса, принято решение разработки исходной модели на базе беспроводных технологий.

Для достижения поставленной цели в диссертации решены следующие задачи:

- анализ существующих подходов к построению сети университета;

- выбор средств имитационного моделирования для разработки модели беспроводной кампусной сети;
- разработка логической схемы проектируемой сети с учетом выбранных технологий;
- создание имитационной модели и тестирование выбранных решений построения сети.

# ГЛАВА 1 ОБЩИЕ СВЕДЕНИЯ О БЕСПРОВОДНЫХ СЕТЯХ

## 1.1 Беспроводные технологии и стандарты беспроводных сетей

Беспроводные технологии — подкласс информационных технологий, служат для передачи информации на расстояние между двумя и более точками, не требуя связи их проводами. Для передачи информации может использоваться инфракрасное излучение, радиоволны, оптическое или лазерное излучение.

В настоящее время существует множество беспроводных технологий, или стандартов передачи данных, наиболее известные пользователям по их маркетинговым названиям, такие как Wi-Fi, WiMAX и Bluetooth и так далее. Каждая технология обладает определёнными характеристиками, которые определяют её область применения.

### 1.1.1 Стандарт Wi-Fi

Wi-Fi – это торговая марка Wi-Fi Alliance для беспроводных сетей на базе стандарта IEEE 802.11. Ноутбук или коммуникатор без подключения к сети Интернет сегодня является практически бесполезным куском «железа». Благодаря широкому использованию Wi-Fi для решения проблемы подключения к Интернету этот термин стал известным.

Несмотря на то, что поначалу в некоторых пресс-релизах WECA фигурировало словосочетание Wireless Fidelity (беспроводная точность), на данный момент от такой формулировки отказались, и термин Wi-Fi никак не расшифровывается.

Продукты, которые предназначались изначально для систем кассового обслуживания, были выведены на рынок под маркой WaveLAN и обеспечивали скорость передачи данных от 1 до 2 Мбит/с. Создатель Wi-Fi – Вик Хейз (Vic Hayes) находился в команде, участвовавшей в разработке таких стандартов, как

IEEE 802.11b, IEEE 802.11a и IEEE 802.11g. Обычно схема сети Wi-Fi содержит не менее одной точки доступа и не менее одного клиента. Также возможно подключение двух клиентов в режиме точка-точка (Ad-hoc), когда точка доступа не используется, а клиенты соединяются посредством сетевых адаптеров напрямую.

Точка доступа передает свой идентификатор сети (SSID) с помощью специальных сигнальных пакетов на скорости 0,1 Мбит/с каждые 100 мс. Поэтому 0,1 Мбит/с – наименьшая скорость передачи данных для Wi-Fi. Зная SSID сети, клиент может выяснить, можно ли подключиться к данной точке доступа. При попадании в зону действия двух точек доступа с идентичными SSID приемник может выбирать между ними на основании данных об уровне сигнала. Стандарт Wi-Fi дает клиенту полную свободу при выборе критериев для соединения.

Устройства Wi-Fi очень распространены на рынке. Совместимость оборудования гарантируется благодаря обязательной его сертификации с логотипом Wi-Fi. Излучение от Wi-Fi-устройств в момент передачи данных на два порядка меньше, чем от сотового телефона. Технология позволяет развернуть сеть без прокладки кабеля, что может уменьшить стоимость развертывания или расширения сети. Места, где нельзя проложить кабель, например, вне помещений или в зданиях, могут обслуживаться беспроводными сетями. Технология позволяет мобильным устройствам иметь доступ к сети.

Стандарт шифрования WEP может быть легко взломан даже при правильной конфигурации именно из-за слабой стойкости данного алгоритма. Несмотря на то, что уже современные устройства поддерживают более совершенный протокол шифрования данных WPA и WPA2, многие старые точки доступа не поддерживают его и требуют своевременной замены.

Принятие стандарта IEEE 802.11i (WPA2) в июне 2004 года сделало доступной более эффективную схему шифрования и аутентификации, которая

уже применяется в новом оборудовании. Для реализации протоколов WPA и WPA2 требуется надёжный пароль, чем обычный придуманный пользователем.

Стандарт IEEE 802.11 определяет два режима работы – Ad-hoc (BSS – Basic Service Set) и инфраструктурный ESS – Extended Service Set. Режим Ad-hoc (иначе называемый «точка-точка») – это простая сеть, в которой связь между клиентами устанавливается сразу напрямую. В режиме инфраструктурный ESS беспроводная сеть состоит минимум из одной точки доступа, подключенной к проводной сети, и некоторого набора беспроводных клиентских станций.

Для организации беспроводной сети в замкнутом пространстве используют передатчики со всенаправленными антеннами. Нужно иметь в виду, что через стены с большим содержанием металлической арматуры (в железобетонных зданиях -несущие стены) радиоволны диапазона 2,4 ГГц иногда могут не проходить, поэтому в комнатах, разделенных такой стеной, придется уже ставить свои точки доступа. Мощность, излучаемая передатчиком точки доступа или же клиентской станции, работающей по стандарту IEEE 802.11, не превышает 0,1 Вт, но многие производители беспроводных точек доступа ограничивают мощность только программным путем, и элементарно просто поднимать мощность до 0,2-0,5 Вт. Для сравнения – мощность, излучаемая телефоном, на порядок больше в момент звонка – до 2 Вт . Поскольку, в отличие от сотового, элементы сети расположены далеко от головы, в целом можно думать, что беспроводные компьютерные сети более безопасны с точки зрения здоровья, чем сотовые телефоны.

Продукты для беспроводных сетей, соответствующие стандарту IEEE 802.11, предлагают четыре уровня средств безопасности: физический, идентификатор набора служб (SSID – Service Set Identifier), идентификатор управления доступом к среде (MAC ID – Media Access Control ID) и шифрование.



Многие организации употребляют дополнительное шифрование (к примеру VPN) для защиты от вторжения. В настоящее время основным методом взлома WPA2 является подбор пароля, поэтому нужно использовать сложные пароли для того, чтобы усложнить задачу подбора пароля.

### **1.1.2 Стандарт WiMAX**

WiMAX (Worldwide Interoperability for Microwave Access) – телекоммуникационная технология, разработанная с целью предоставления универсальной беспроводной связи на довольно больших расстояниях для широкого спектра устройств. Основана на стандарте IEEE 802.16, который также называют Wireless MAN (WiMAX можно считать жаргонным названием, так как это не технология, а название форума, на котором Wireless MAN согласован).

WiMAX служит для соединения точек доступа Wi-Fi друг с другом и другими сегментами сети, а так же для обеспечения беспроводного широкополосного доступа как альтернативы выделенным линиям и xDSL. WiMAX позволяет осуществлять доступ в интернет на высоких скоростях, с большим покрытием, чем у Wi-Fi-сетей. Это позволяет использовать технологию в качестве магистральных каналов, продолжением которых выступают традиционные выделенные и xDSL-линии, а также локальные сети. В результате данный подход даёт возможность создавать масштабируемые высокоскоростные сети в рамках городов.

WiMAX – это система дальнего действия, которая покрывает километры пространства, которая обычно использует лицензированные спектры частот для предоставления соединения с интернетом типа точка-точка провайдером конечному пользователю. Разные стандарты семейства 802.16 обеспечивают разные виды доступа, от сотового до фиксированного. В отличие от WiMAX Wi-Fi – это система короткого действия, которая покрывает десятки метров,

использовавшаяся нелицензированные диапазоны частот для обеспечения доступа к сети. Обычно Wi-Fi используют пользователи для доступа к локальной сети, которая вовсе может быть и не подключена к Интернету. Если WiMAX можно вообще сравнить с мобильной связью, то Wi-Fi будет похож на радиотелефон.

WiMAX и Wi-Fi имеют абсолютно разный механизм Quality of Service (QoS). WiMAX использует механизм, основанный на установлении соединения между станцией и устройством данного пользователя. Каждое соединение оборудовано на определенном алгоритме планирования, который может обеспечивать параметр QoS для каждого данного соединения. Wi-Fi, в свою очередь, использует механизм QoS похожий тому, что используется в Ethernet, при котором пакеты получают различный приоритет. Такой подход не обещает одинаковый QoS для того или иного соединения.

Ряд преимуществ присущ всему данному семейству WiMAX, хотя его версии существенно отличаются друг от друга. Разработчики этого стандарта искали разумные решения как для фиксированного, так и для сотового применения, но присоединить все требования в рамках одного стандарта так и не вышло. Хотя ряд базовых требований совпадает, нацеленность технологий на разные рыночные ниши привела к созданию двух разных версий. Каждая из спецификаций WiMAX определяет свои диапазоны частот, ширину полосы пропускания, мощность излучения, методы передачи и доступа, способы кодирования и модуляции сигнала, принципы повторного использования радиочастот и остальные показатели. Поэтому WiMAX-системы, основанные на версиях стандарта IEEE 802.16 e и d, несовместимы.

Главное различие данных технологий состоит в том, что фиксированный WiMAX позволяет обслуживать лишь статических абонентов, а сотовый

сосредоточен на работу с пользователями, двигающимися со скоростью до 150 км/ч.

Мобильность означает наличие функций роуминга и переключения между базовыми станциями при движении абонента. В отдельном случае мобильный WiMAX может служить и для обслуживания фиксированных пользователей. С изобретением мобильного WiMAX все больший акцент делается на разработке мобильных устройств, в том числе обычных мобильных смартфонов, и компьютерной периферии. Оборудование для использования сетей WiMAX поставляется разными производителями и может быть установлено как в помещении так и вне его. Следует обратить внимание, что оборудование, рассчитанное на размещение внутри помещений и не требующее определенных навыков при установке, гораздо более удобно, однако способно работать на более меньших расстояниях от базовой станции, чем профессионально установленные внешние устройства.

Поэтому оборудование, установленное внутри помещений, требует больших инвестиций в развитие инфраструктуры данной сети. В общем виде WiMAX сети состоят из следующих частей: базовых и абонентских станций, также оборудования, связывающего базовые станции, с поставщиком сервисов, и с Интернетом.

Структура сетей семейства стандартов IEEE 802.16 похожа с традиционными GSM-сетями (базовые станции действуют на расстояниях до десятков километров, для их установки не нужно строить вышки – разрешается установка на крышах домов при соблюдении правила прямой видимости между станциями). WiMAX применяется как и для решения проблемы так и для предоставления доступа в сеть (офисным и районным сетям).

Для соединения базовой станции с абонентской используется высокочастотный диапазон радиоволн от 1,5 до 11 ГГц. В прекрасных условиях

скорость обмена данными может достигать 70 Мбит/с, при этом не нужна прямой видимости между базовой станцией и приемником. Между базовыми станциями устанавливаются соединения, использующие диапазон частот от 10 до 66 ГГц, скорость обмена данными может достигнуть до 140 Мбит/с. При этом одна из базовых станций подключается к сети провайдера с использованием классических проводных соединений. Чем большее число БС подключено к сетям провайдера, тем выше скорость передачи данных и надежность сети [2].

Приведем сравнительную таблицу основных стандартов (таблица 1.1).

Таблица 1.1 – Сравнительная характеристика стандартов беспроводных сетей

Стандарт	Wi-Fi (IEEE 802.11b)	WiMAX (IEEE802.16e)
частотный диапазон	2,4-2,483 ГГц	2,3-2,5 ГГц
диапазон действия	20-300 m	1-5 км
пропускная способность кбит/с	11000	30 Мбит/с
размер стека протокола,кбайт	более 1000	
мах. Количество узлов в сети	10	
область применения	передача мультимедийной информации (интернет, почта, видео)	создание или соединения точек доступа Wi-Fi.

В магистерской диссертации будет реализована модель Wi Fi сети.

## 1.2 Методы маршрутизации в беспроводных сетях

Определенно три вида маршрутизации – простая, фиксированная и адаптивная. Разница между ними в степени учета изменения топологии и нагрузки сети при решении задачи выбора данного маршрута.

Обыкновенная маршрутизация отличается тем, что при выборе маршрута не учитывается ни изменение топологии сети, ни изменение ее состояния. Она не обеспечивает направленной передачи пакетов и имеет достаточно маленькую

эффективность. Ее плюсами являются элементарность реализации алгоритма маршрутизации и обеспечение устойчивой работы сети при выходе из строя ее элементов. Немногое практическое применение получили разновидности простой маршрутизации (случайная и лавинная).

Приоритет случайной маршрутизации заключается в том, что для передачи пакета из узла связи выбирается одно, абсолютно случайно выбранное доступное направление. Пакет "гуляет" по сети и с конечной вероятностью когда-либо но достигает в конце концов своего адресата. При этом не обеспечивается ни оптимальное время доставки, ни эффективное использование пропускной способности сети.

Лавинная маршрутизация предусматривает передачу пакета из узла практически по всем направлениям, кроме того откуда этот пакет поступил узел. Так как это происходит в каждом узле, имеет место явление "размножение" пакета, что очень резко ухудшает использование пропускной способности сети. Чтобы этого не случилось, нужно помечать копии данного пакета и удалять в каждом узле повторно проходящие через него дубликаты.

Основное преимущество такого метода – это гарантированное обеспечение оптимального времени доставки пакета своему адресату, так как из всех направлений, по которым передается пакет, хотя бы одно из них обеспечивает такое время. Данный метод может пригодится в незагруженных сетях, когда требования по минимизации времени и надежности доставки пакетов высоки.

Фиксированная маршрутизация отличается тем, что при выборе маршрута учитывается изменение топологии сети и не придаёт значение изменение ее нагрузки. Для каждого узла назначения направление передачи определяется по таблице маршрутов, которая и определяет меньшие пути. Таблицы «рождаются» в центре управления сетью. Они составляются с нуля и модифицируются при изменении топологии сети. Нехватка адаптации к изменению нагрузки приводит к

задержкам пакетов сети. Различают одно путьевую и много путьевую разновидности маршрутизации. Одно путьевая строится на основе единственного пути передачи пакетов между двумя абонентами, что сопряжено с неустойчивостью к перезагрузкам, а много путьевая-строится на основе нескольких возможных путей между двумя абонентами, из которых выбирается более предпочтительный путь. Фиксированная маршрутизация используется в сетях с мало изменяющейся топологией.

Адаптивной называют маршрутизацию, при которой принятие решения о направлении передачи пакетов происходит с учетом изменения как топологии, так и нагрузки сети. Есть несколько модификаций адаптивной маршрутизации, различаются они тем, чем какая именно информация используется при выборе маршрута. Получили распространение модификации: локальная, распределенная, централизованная и гибридная маршрутизации.

Локальная маршрутизация основана на использовании информации, имеющаяся в данном узле и включающей в себя таблицу маршрутов, которая определяет все направления передачи пакетов из данного узла, данные о состоянии связи, работают или нет, длину очереди пакетов, ждущих передачи. Информация о состоянии других узлов не используется. Таблица маршрутов вычисляет кратчайшие маршруты, обеспечивающие доставку пакета адресату за кратчайшее время. Преимущество такого метода состоит в том, что принятие решения о выборе маршрута происходит с использованием самых последних данных о состоянии узла. Минус метода в его "близорукости", так как выбор маршрута происходит без учета глобального состояния всей сети. Всегда имеется опасность передачи пакета по перегруженному маршруту.

Распределенная адаптивная маршрутизация построена на использовании информации, указанной для локальной маршрутизации, и данных, получаемых от соседних узлов сети. В каждом узле формируется каталог маршрутов ко всем

узлам назначения, где указываются маршруты с меньшим временем задержки пакетов. До начала работы сети это время оценивается судя из топологии сети. В процессе работы сети узлы периодически обмениваются с соседними узлами, называемыми таблицами задержки, в которых указывается длина очереди пакетов узла. После обмена таблицами задержки каждый узел считает задержки и корректирует маршруты уже с учетом поступивших данных и длины очередей в самом узле. Обмен таблицами задержки может проходить не только периодически, но и асинхронно в резких изменений нагрузки или топологии сети. Учет состояния соседних узлов при выборе маршрута повышает эффективность алгоритмов маршрутизации, но это достигается за счет увеличения загрузки сети служебной информацией. Помимо того, сведения об изменении состояния узлов «разлетаются» по сети достаточно медленно, поэтому выбор маршрута происходит по несколько устаревшим данным.

Централизованная адаптивная маршрутизация определяется тем, что задача маршрутизации для каждого узла сети решается в ЦМ (центре маршрутизации). Каждый узел периодически формирует сообщение о своем состоянии (длине очередей и работоспособности линий связи) и передает его в ЦМ. По этим данным в центре маршрутизации для каждого узла составляется каталог маршрутов. Разумеется, что передача сообщений в ЦМ, формирование и рассылка каталог маршрутов – все это сопряжено с временными задержками, естественно, с потерей эффективности такого метода, особенно при большой пульсации нагрузки в сети. Кроме этого, есть опасность потери управления сетью при отказе ЦМ.

Гибридная адаптивная маршрутизация основана на использовании таблиц маршрутов, рассылаемых центром маршрутизации узлам сети, в сочетании с анализом длины очередей в узлах. Вывод, здесь реализуются принципы централизованной и локальной маршрутизации. Гибридная маршрутизация компенсирует минусы централизованной и локальной ,и воспринимает их

преимущества, такие как: маршруты центра соответствуют глобальному состоянию сети, а учет текущего состояния узла обеспечивает своевременность решения задачи [4].



## **ГЛАВА 2 ОБЗОР ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ МОДЕЛИРОВАНИЯ БЕСПРОВОДНОЙ КАМПУСНОЙ СЕТИ ГТУ Г. САНА**

### **2.1 Понятие и методы моделирование**

Моделирование это метод познания, который предполагает построение и изучение модели, а затем перенос полученных данных на моделируемый объект - оригинал. Модель – это мысленная (идеальная) или физическая (материальная) система, которая отображает объект так, что ее изучение дает новую информацию об этом объекте. Оригинал (прототип, образец) – это объект, на который переносится информация, полученная в результате исследования модели.

Научной основой моделирования служит теория аналогии. Под аналогией понимается сходство объектов по качественным и количественным признакам в результате их сравнения. Аналогия предполагает подобие между различными объектами в определенных свойствах, функциях, пропорциях элементов. Являясь также логической основой моделирования, научная аналогия есть умозаключение, в котором на основании сходства ряда признаков у двух объектов делается вывод о том, что одному из них (оригиналу) присущи такие свойства, которые обнаружены при исследовании другого объекта (модели).

Процесс моделирования состоит из следующих этапов: определение задачи и фиксация свойств оригинала; понимание проблематичности изучения оригинала в природных условиях; выбор модели, адекватно описывающей характерные свойства оригинала; изучение модели в соответствии с задачей; перенос результатов исследования модели на оригинал; проверка результатов. Различают несколько видов моделирования.

#### **Мысленное (идеальное) моделирование**

Включает в себя различные представления в виде воображаемых моделей. Здесь с моделированием неразрывно связана идеализация – мысленное

конструирование понятий, концепций об объектах, не существующих в действительности. Для них существует лишь близкий аналог в реальном мире. Примерами идеальных объектов являются геометрические понятия: точки, линии, плоскости, идеальный газ, абсолютно черное тело, общественно-экономическая формация, государство и т. д.

### **Физическое (материальное) моделирование**

Характеризуется тем, что исследования проводятся на моделях, обладающих физическим подобием и сохраняющих полностью или частично природу изучаемых явлений.

По характеристикам модели можно получить все характеристики оригинала благодаря математическим вычислениям.

Сейчас физическое моделирование широко применяется для разработки и экспериментального изучения различных сооружений, машин, для прогнозирования климатических явлений, изучения эффективных способов горных изысканий и т. д.

### **Символическое (знаковое) моделирование**

Связано со знаковым представлением некоторых свойств оригинала. Символические (знаковые) модели – это разнообразные топологические, графические и символные изображения (в виде географических карт, графиков, схем, химических формул и т. п.) изучаемых объектов.

Разновидностью символического (знакового) моделирования является математическое моделирование – способ изучения явлений, имеющих различное физическое содержание, но описываемых одинаковыми математическими моделями. К математическим моделям можно отнести алгоритмы и программы, составленные для ЭВМ и моделирующие определенные процессы, описанные дифференциальными уравнениями, заложенными в основу этих алгоритмов.

## **Численное моделирование**

На компьютере основывается на математической модели изучаемого объекта и применяется при больших объемах вычислений, необходимых для ее исследования. Путем расчетов на ЭВМ различных вариантов осуществляется накопление информации и производится отбор наиболее вероятных ситуаций. В настоящее время моделирование выступает как эффективный общенаучный инструмент познания, метод прогнозирования инженерно-конструкторских разработок, метод машинной имитации долгосрочных программ в области экономики, анализа и оценки различных вариантов принимаемых решений и их последствий.

### **2.2 Обзор и сравнение программного обеспечения для моделирования сетей связи**

В настоящее время существуют различные программные средства для моделирования и исследования беспроводных сетей и систем связи:

- OPNET modeler 17.5;
- OMNeT++;
- NS-2;
- NS-3;
- Cisco Packet Tracer.

#### **2.2.1 OPNET modeler 17.5**

OPNET Modeler [2] предлагает пользователям графическую среду для создания, выполнения и анализа событийного моделирования сетей связи. Это удобное программное обеспечение может быть использовано для большого ряда задач, например, типичные создание и проверка протокола связи, анализ

взаимодействий протокола, оптимизация и планирование сети. Также возможно осуществить с помощью пакета проверку правильности аналитических моделей, и описание протоколов. Общий вид главного окна системы показан на рисунке 2.1.

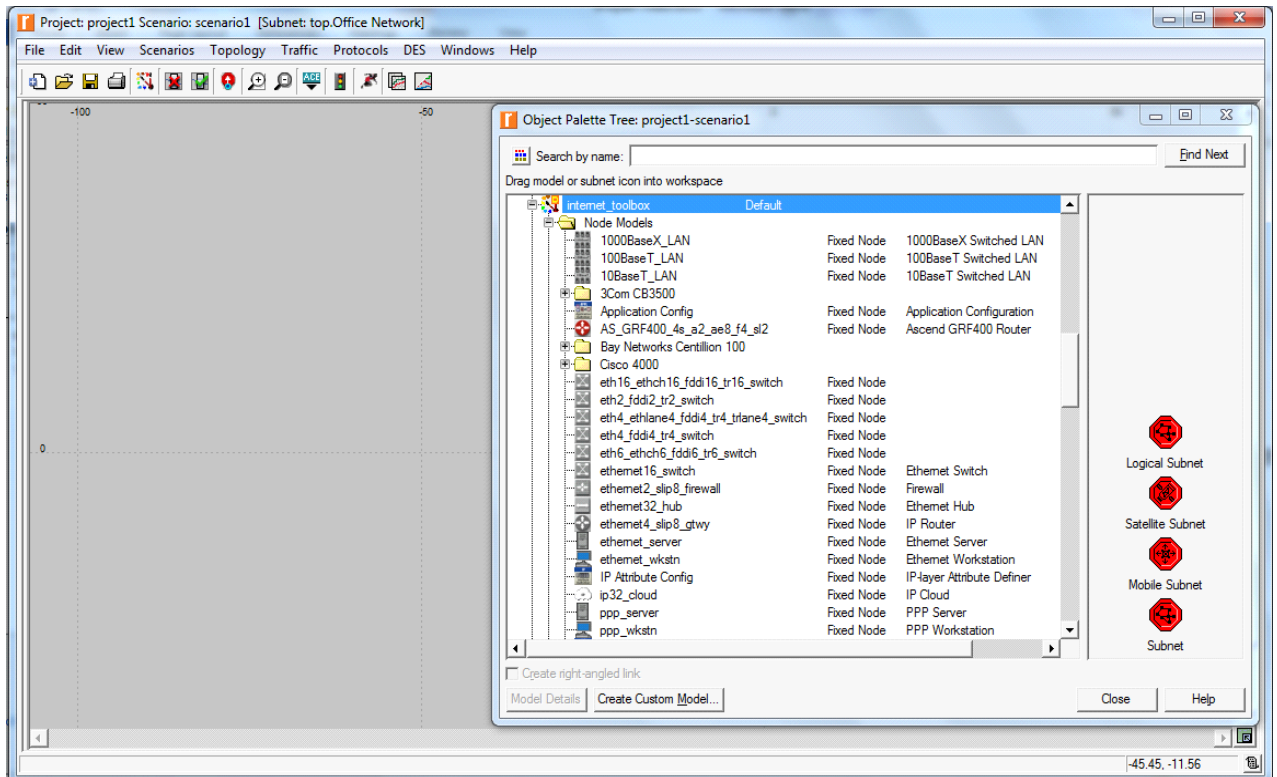


Рисунок 2.1 – Главное окно OPNET Modeler17.5

В рамках так называемого редактора проекта могут быть созданы палитры сетевых объектов, которым пользователь может присвоить различные формы соединения узлов и связи вплоть до имеющих вид головоломки. Автоматизированное порождение сетевой топологии кольца, звезды, случайной сети, также поддерживается и резервируется утилитами для импортируемых сетевых топологий в различных форматах. Случайный трафик может быть автоматически сгенерирован из алгоритмов, указанных пользователем, а также импортирован из входящих в стандартную комплектацию пакета форматов реальных трафиков линий. Результаты моделирования могут быть проанализированы, а графы и анимация трафика, опять же будут сгенерированы

автоматически. Новая особенность это автоматическое преобразование в формат html 4.0x. Одним из плюсов из создания модели сети с помощью программного обеспечения является то, что уровень гибкости, обеспечиваемый ядром моделирования, тот же, что и для моделирования, написанных с нуля, но объектное построение среды позволяет пользователю намного быстрее делать разработку, усовершенствования и производить модели для многократного использования. Есть несколько сред редактора – по одной для каждого типа объекта. Организация объектов иерархическая, сетевые объекты (модели) связаны набором узлов и объектов связи, при этом как объекты узла связаны набором объектов, типа модулей очередности, модулей процессора, передатчиков и приемников. Версия ПО для моделирования радиоканала содержит модели антенны радиопередатчика, антенны приемника, перемещающихся объектов узла (включая спутники). Логика поведения процессора и модулей очередности определяет модель процесса, которую пользователь может создавать и изменять в пределах редактора процесса, в котором пользователь может определить модель процесса через комбинацию алгоритма работы конечного автомата (finite-state machine – FSM) и операторов языка программирования C/C++. Вызов события модели процесса в течение моделирования управляется возбуждением прерывания, а каждое прерывание соответствует событию, которое должно быть обработано моделью процесса. Основа связи между процессами – структура данных, называемая пакетом. Могут быть заданы форматы пакета, т. е. они определяют, какие поля могут содержать такие стандартные типы данных, как целые числа, числа с плавающей запятой и указатели на пакеты (эта последняя способность позволяют инкапсулировать моделирование пакета). Структура данных, вызывающая информацию по контролю за интерфейсом (interface control information – ICI), может быть разделена между двумя событиями моделей процесса – это ещё один механизм для межпроцессорной связи, это очень удобно

для команд моделирования и соответствует архитектуре многоуровневого протокола. Процесс также может динамически порождать дочерние процессы, которые упростят функциональное описание таких систем, как серверы. Несколько основных моделей процесса входят в базовую комплектацию пакета, моделируя популярные протоколы работы с сетями и алгоритмы, вроде протокола шлюза границы (border gateway protocol - BGP), протокола контроля передачи. Интернет протокол (TCP/IP), ретрансляции кадров (frame relay), Ethernet, асинхронного режима передачи (asynchronous transfer mode - ATM), и WFQ (weighted fair queuing). Базовые модели полезны для быстрого развития сложных имитационных моделей для общих архитектур сети, а также для обучения, чтобы дать точное функциональное описание протокола студентам. Существует возможность сопровождения комментариями и графикой (с поддержкой гипертекста) моделей сети, узла или процесса. Одним из недостатков системы является большая стоимость на представленный продукт.

### **2.2.2 Симулятор OMNeT++**

Данный симулятор представляет собой систему моделирования на основе дискретных событий, которая может быть использована для таких задач как:

- моделирование проводных и беспроводных коммуникационных систем;
- протоколов моделирования;
- моделирование сетей массового обслуживания.

Программа OMNeT++ подходит для моделирования любой сети, основой которой является дискретное событие. Процесс удобно отображается в виде объектов, обменивающимися сообщениями. OMNeT++ использует язык C++ для имитационных моделей. Имитационные модели в совокупности с языком высокого уровня NED собираются в крупные компоненты и представляют собой большие системы. Симулятор имеет графические инструменты для создания

моделей и оценки результатов в режиме реального времени. Модели программы собираются из компонентов множественного использования, называемых модулями. Модули можно использовать много раз и объединять по принципу блоков LEGO. Модули соединяются между собой с помощью портов, и объединяются в составные модули с использованием высокоуровневого языка программирования NED (рисунок 2.2). Количество вводимых модулей неограниченно. Модули связываются посредством передачи сообщений, которые содержат произвольные структуры данных. Модули могут передавать сообщения по определенным портам и соединениям серверу или непосредственно друг другу. Последнее, к примеру, полезно для моделирования беспроводных сетей.

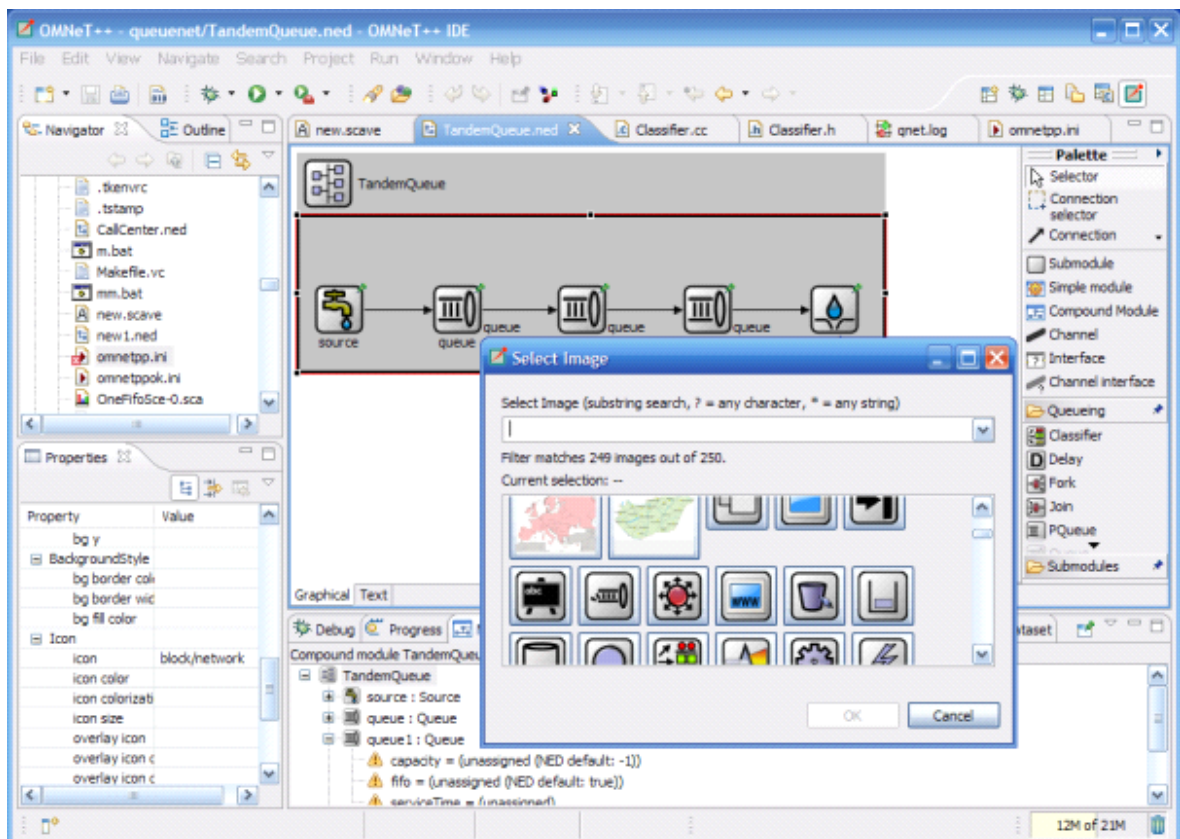


Рисунок 2.2 – Графический NED редактор

Процесс моделирования может работать в различных пользовательских интерфейсах. Графически анимированный пользовательский интерфейс удобен

для демонстрации и отладки сети, а интерфейс командной строки удобен для внесения изменений. Компоненты OMNeT++:

- корневая библиотека моделирования;
- OMNeT ++ IDE на базе платформы Eclipse;
- графический интерфейс выполняемого моделирования, ссылки на исполняемый файл (Tkenv);
- пользовательский интерфейс командной строки для выполнения моделирования (Cmdenv);
- документация, примеры. OMNeT++ работает на базе самых распространенных операционных систем: (Linux, Mac OS/X, Windows).

### **2.2.3 Симулятор NS-2**

Является программным обеспечением (ПО) с открытым кодом (Open Source software), предназначенным для дискретно-событийного моделирования проводных и беспроводных (мобильных) систем связи). Основными языками в составе симулятора являются C++ и Tcl (Tool Command Language) (рисунок 2.3).



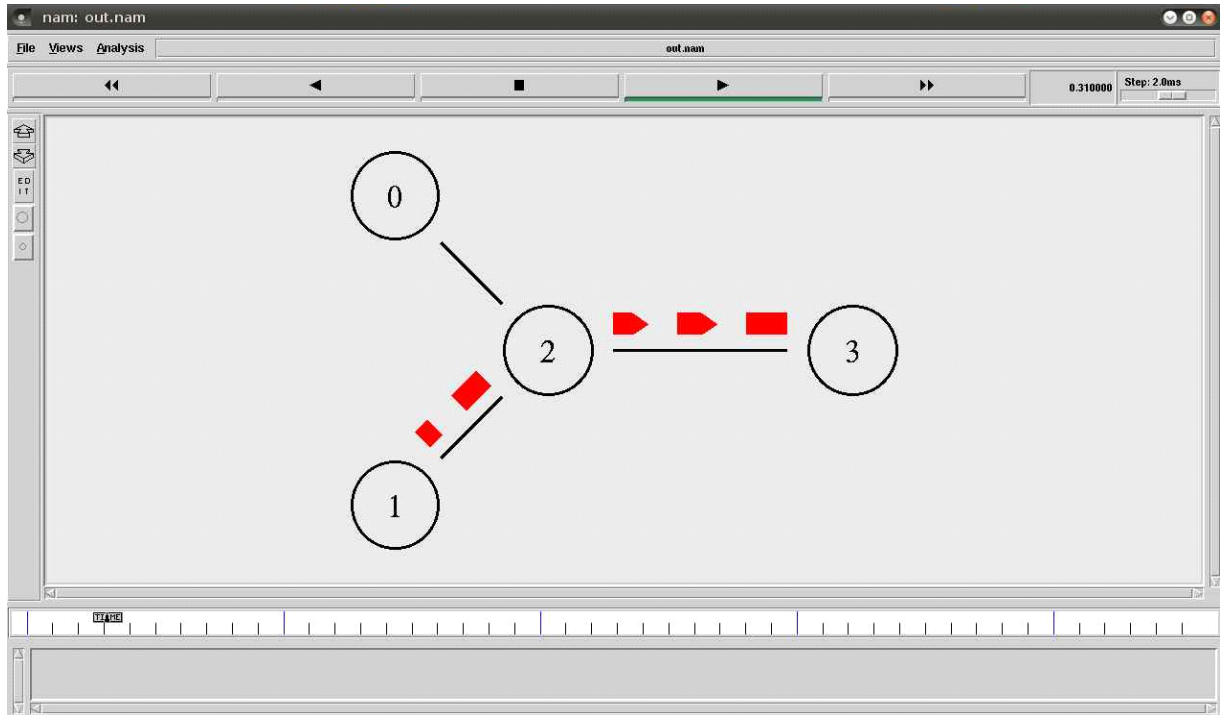


Рисунок 2.3 – Главное окно NS2

Использование двух языков программирования в ns2 объясняется следующими причинами. С одной стороны, для детального моделирования протоколов необходимо использовать системный язык программирования, обеспечивающий высокую скорость выполнения и способный манипулировать достаточно большими объемами данных. С другой стороны, для удобства пользователя и быстроты реализации и модификации различных сценариев моделирования привлекательнее использовать язык программирования более высокого уровня абстракции. Такой подход является компромиссом между удобством использования и скоростью. В ns2 в качестве системного языка используется C++, позволяющий обеспечить:

- высокую производительность;
- работу с пакетам потока на низком уровне абстракции модели;
- модификацию ядра ns2 с целью поддержки новых функций и протоколов.

В качестве языка программирования высокого уровня абстракции используется язык скриптов Tcl, позволяющий обеспечить ряд положительных

свойств, присущих языку Tcl/Tk (Т.К. OTcl является объектно-ориентированным расширением языка Tcl):

- простота синтаксиса;
- простота построения сценария моделирования;
- возможность соединения воедино блоков, выполненных на системных языках программирования и простую манипуляцию ими.

Объединение для совместного функционирования C++ и OTcl производится с помощью TclCl (Classes Tcl). TclCl – интерфейс между объектами C++ и OTcl, которым пользуются ns2.

Однако, архитектура ns-2 не оптимальна и требует доработок. В частности, разделяемая модель объектов C++/OTcl представляет некоторые проблемы:

Малая распространенность и документированность языка OTcl, а также сложность отладки написанных с его помощью скриптов. Во-вторых, существуют ограничения на совместное использование объектов C++.

Эффективность использования памяти. Симулятор должен поддерживать оба потока данных – полный и ограниченный. Другими словами, моделируемое приложение должно переслать 100,000 байтов данных удаленному узлу, но фактическое содержимое данных может быть достаточно абстрактным. На данный момент симулятор ns-2 оптимизирован для ограниченных потоков данных. Трассировка. Для упрощения работы с моделями с большим количеством элементов и уменьшения объема регистрируемых и трассируемых событий, статистика моделирования должна гибко конфигурироваться пользователем. Некоторые возможности уже присутствуют в симуляторе ns-2: возможность трассирования только пакетов или слежение за определенным каналом. Более того, необходимо позволить пользователю определять тип регистрируемых данных, например, нужно ли регистрировать порты источника и приемника при исследовании протокола TCP.

## 2.2.4 Симулятор NS-3

NS3 – является мощным сетевым симулятором для моделирования телекоммуникационных систем и распространяется под лицензией GNU GPLv2. Симулятор решает одну из главных проблем моделирования сетей – проблему стоимости оборудования. Сетевые симуляторы являются программными продуктами, позволяющими выполнять имитационное моделирование телекоммуникационных систем. Применение имитационного моделирования позволяет проводить эксперименты, не разворачивая реальную сеть, что является трудоемким, дорогостоящим и, как правило, протяженным во времени процессом.

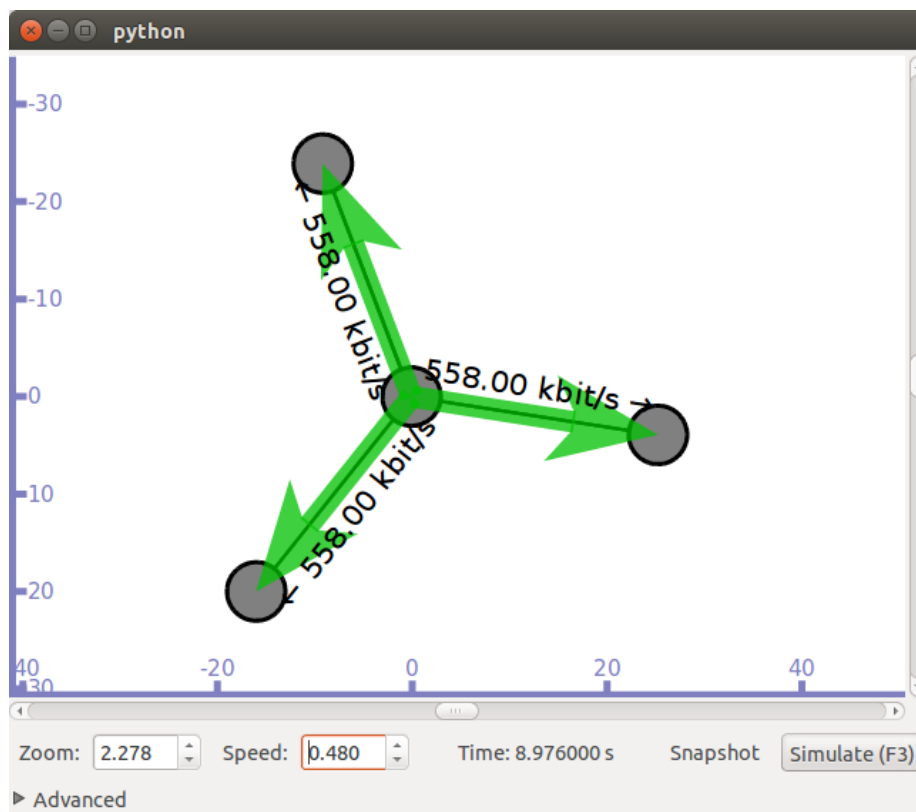


Рисунок 2.4 – Главное окно NS3

В NS3 разработаны модели беспроводных сетей различных типов, позволяющие проводить моделирование с движущимися объектами в трёхмерном

пространстве. Кроме того, реализованы модели проводных и смешанных топологий различной сложности, в том числе, Mesh-сетей на основе стека протоколов 802.11s. Разработан Frame Work под названием Flow Monitor, предоставляющий различные, а главное гибкие методы сбора самых различных показаний с моделируемых сетевых узлов и каналов связи. Симулятор «по умолчанию» не имеет собственного графического интерфейса, однако используются такие средства как Net Animator и PyViz, позволяющие выводить схему на экран для наблюдения за работой протокола. Таким образом, функциональность NS3 превосходит многие коммерческие симуляторы.

### **2.2.5 Программа Cisco Packet Tracker**

Packet Tracer – симулятор сети передачи данных, выпускаемый фирмой Cisco Systems. Позволяет делать работоспособные модели сети, настраивать (командами Cisco IOS) маршрутизаторы и коммутаторы, взаимодействовать между несколькими пользователями (через облако). Включает в себя серии маршрутизаторов Cisco 1800, 2600, 2800 и коммутаторов 2950, 2960, 3650. Кроме того есть серверы DHCP, HTTP, TFTP, FTP, рабочие станции, различные модули к компьютерам и маршрутизаторам, устройства WiFi, различные кабели.

Packet Tracer способен моделировать большое количество устройств различного назначения, а так же немало различных типов связей, что позволяет проектировать сети любого размера на высоком уровне сложности.

Моделируемые устройства:

- коммутаторы третьего уровня:
- Router 2620 XM;
- Router 2621 XM;
- Router-PT.
- Коммутаторы второго уровня:

- Switch 2950-24;
- Switch 2950T;
- Switch-PT;
- соединение типа «мост» Bridge-PT.
- Сетевые концентраторы:
- Hub-PT;
- повторитель Repeater-PT.
- Оконечные устройства:
- рабочая станция PC-PT;
- сервер Server-PT;
- принтер Printer-PT.
- Беспроводные устройства:
- точка доступа AccessPoint-PT.
- Глобальная сеть WAN.
- Типы связей:
- консоль;
- медный кабель без перекрещивания (прямой кабель);
- медный кабель с перекрещиванием (кросс-кабель);
- волоконно-оптический кабель;
- телефонная линия;
- Serial DCE;
- Serial DTE.

Так же целесообразно привести те протоколы, которые студент может отслеживать:

- ARP;
- CDP;
- DHCP;

- EIGRP;
- ICMP;
- RIP;
- TCP;
- UDP.

Интерфейс программы Cisco Packet Tracer представлен на рисунке 2.5.

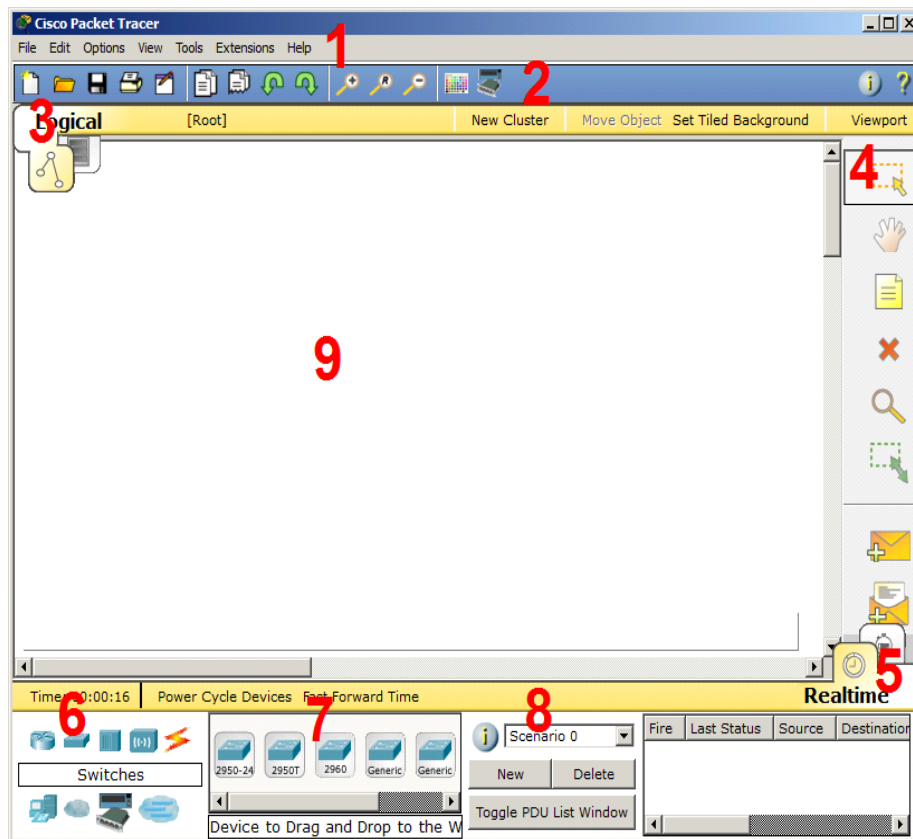


Рисунок 2.5 – Интерфейс программы Cisco Packet Tracer

1. Главное меню программы.
2. Панель инструментов – дублирует некоторые пункты меню.
3. Переключатель между логической и физической организацией.
4. Ещё одна панель инструментов, содержит инструменты выделения, удаления, перемещения, масштабирования объектов, а так же формирование произвольных пакетов.



Данная панель содержит в своей левой части типы доступных устройств, а в правой части доступные модели. При выполнении различных лабораторных работ, эту панель придется использовать намного чаще, чем все остальные. Поэтому рассмотрим ее более подробно.

При наведении на каждое из устройств, в прямоугольнике, находящемся в центре между ними будет отображаться его тип. Типы устройств, наиболее часто используемые в лабораторных работах Packet Tracer, представлены на рисунке 2.8.



Рисунок 2.8 – Основные типы устройств

Рассматривать конкретные модели устройств каждого типа, не имеет большого смысла. Отдельного рассмотрения заслуживают типы соединений. Перечислим наиболее часто используемые из них (рассмотрение типов подключений идет слева направо, в соответствии с приведенным на рисунке 2.9).



Рисунок 2.9 – Типы соединений устройств в Packet Tracer

1. Автоматический тип – при данном типе соединения PacketTracer автоматически выбирает наиболее предпочтительные тип соединения для выбранных устройств.

2. Консоль – консольные соединение.



3. Медь Прямое – соединение медным кабелем типа витая пара, оба конца кабеля обжаты в одинаковой раскладке. Подойдет для следующих соединений: коммутатор – коммутатор, коммутатор – маршрутизатор, коммутатор – компьютер и др.

4. Медь кроссовер – соединение медным кабелем типа витая пара, концы кабеля обжаты как кроссовер. Подойдет для соединения двух компьютеров.

5. Оптика – соединение при помощи оптического кабеля, необходимо для соединения устройств имеющих оптические интерфейсы.

6. Телефонный кабель – обыкновенный телефонный кабель, может понадобится для подключения телефонных аппаратов.

7. Коаксиальный кабель – соединение устройств с помощью коаксиального кабеля.

### 2.3 Сравнение сетевых симуляторов

Для сравнения рассмотренных выше систем моделирования составим таблицу, включающую в себя наиболее важные параметры, которым должны соответствовать данные сетевые симуляторы, необходимые для успешного выполнения поставленной задачи.

Для разработки имитационной модели беспроводной телекоммуникационной кампусной сети была выбрана программа OPNET modeler потому что программа OPNET modeler позволяет строить модели без программирования.

Таблица 2.1 – Сравнение систем моделирования

Среда моделирования	Наличие протоколов маршрутизации	Наличие инструментов для обработки результатов моделирования	Доступность	Операционные системы

		ия		
OPNET Modeler	+	+	+	Win 98/NT/2000/ XP/7/8 Linux
OMNeT++	-	+	-	Linux, macOS, Windows
Ns-2	+	+	+	Win98/NT/2000/XP/7/8 Linux
Ns-3	-	-	+	Linux, FreeBSD, macOS
Cisco packet tracer	+		+	Linux, Android 4.1+, iOS 8+ Micro soft Windows

Программная система сама генерирует модель сети на основе исходных данных о ее топологии и используемых протоколах, об интенсивностях потоков запросов между компьютерами сети, протяженности линий связи, о типах используемого оборудования и приложений.

Программа OPNET Modeler предлагает пользователям графическую среду для создания, выполнения и анализа событийного моделирования сетей связи. Это удобное программное обеспечение может быть использовано для решения многих задач.

## ГЛАВА 3 РАЗРАБОТКА И ИССЛЕДОВАНИЕ ИМИТАЦИОННОЙ МОДЕЛИ БЕСПРОВОДНОЙ КАМПУСНОЙ СЕТИ

### 3.1 Карта сети

На территории студенческого городка располагается шесть учебных корпусов. С ростом информационных технологий появляется необходимость разворачивания единой интегрированной информационной структуры университета, объединяющей группу зданий в единое информационное пространство. Сетевые технологии позволят повысить эффективность применения компьютеров, например, создать информационные системы, обеспечивающие решение задач дистанционного и автоматизированного обучения, хранения информации, документооборота, обмена сообщениями и организация групповой работы над проектами. Очевидно, что информационная система будет постоянно расширяться, поэтому добавление новых компонентов или внедрение новых технологий не должны требовать полной перестройки уже работающей и отлаженной системы.

Создание сети значительно облегчается, если при ее проектировании используется иерархическая модель. Согласно правилам построения иерархических сетей и структурированных систем в каждом корпусе следует разместить коммутаторы здания (уровень распределения) и коммутаторы этажа (уровень доступа). В главном корпусе сосредоточено наибольшее количество разнообразных отделов, поэтому в нем также разместятся коммутатор уровня ядра и серверная ферма. Коммутаторы корпусов соединяются с коммутатором уровня ядра, образуя звездообразную топологию.

На рисунке 3.1 представлена логическая схема беспроводной телекоммуникационной кампусной сети университета.

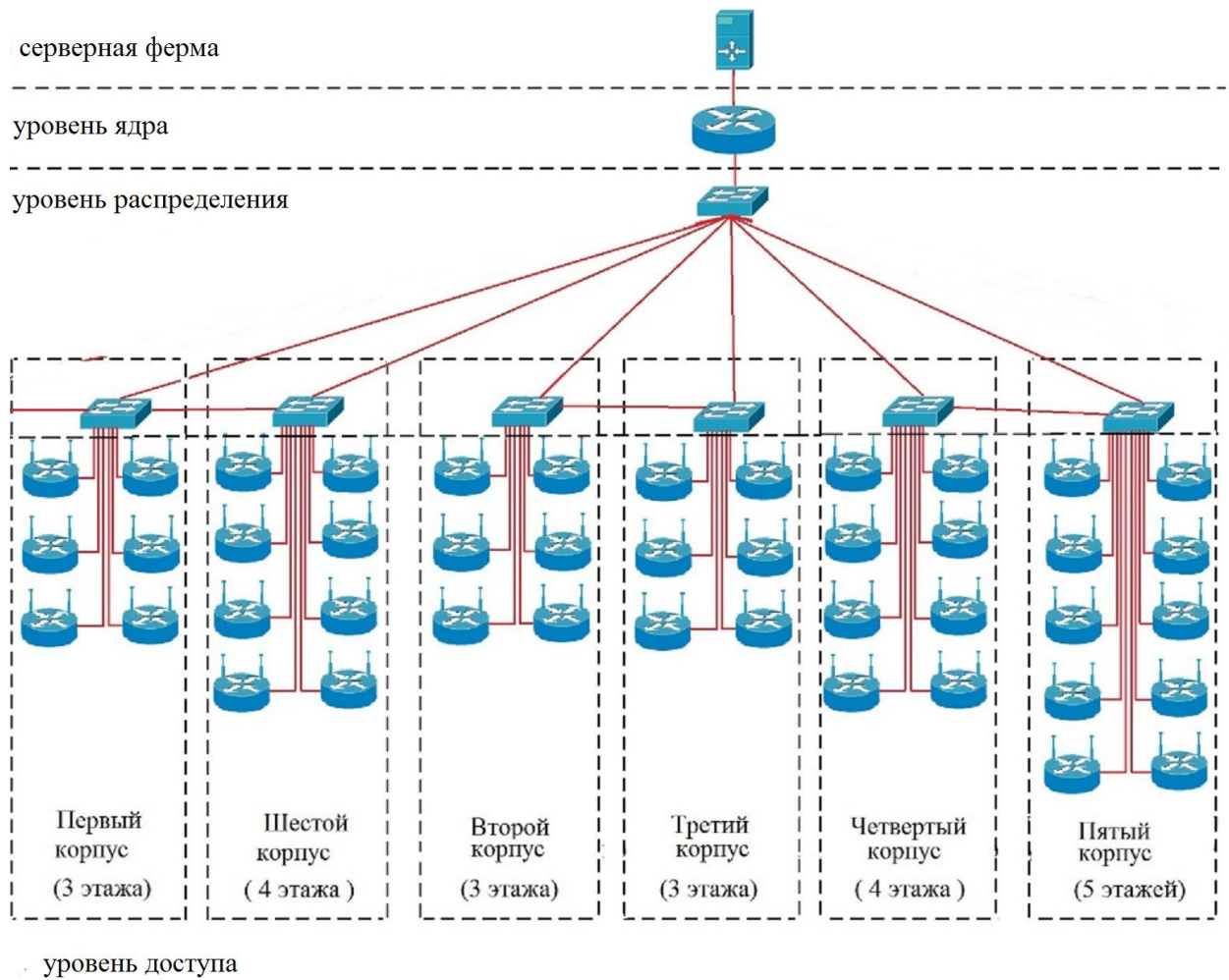


Рисунок 3.1 – Логическая схема беспроводной телекоммуникационной кампусной сети [5]

Согласно схеме, сформируем сеть в программе OPNET Modeler (рисунок 3.2).

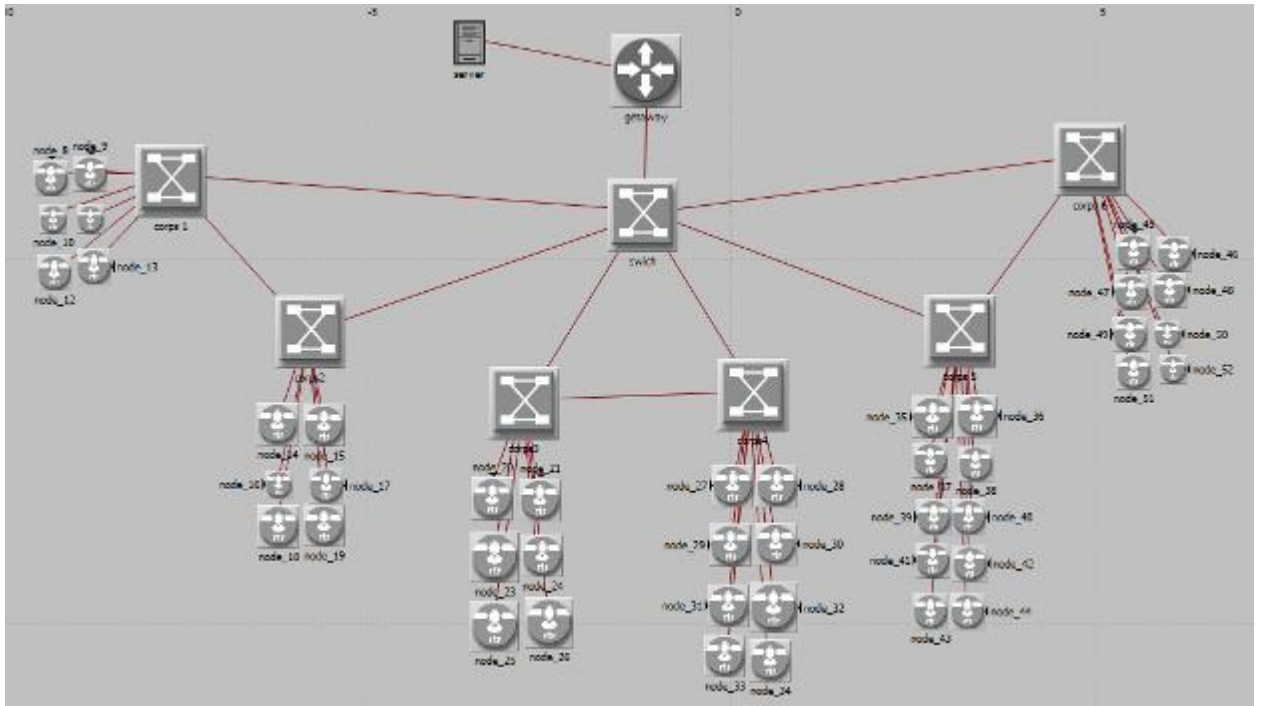


Рисунок 3.2 – Схема беспроводной телекоммуникационной кампусной сети ГТУ г. Сана в программе OPNET Modeler [3]

На рисунке 3.3 и рисунке 3.4 представлены схемы беспроводной телекоммуникационной кампусной сети четвертого этажа главного корпуса ГТУ г. Сана.

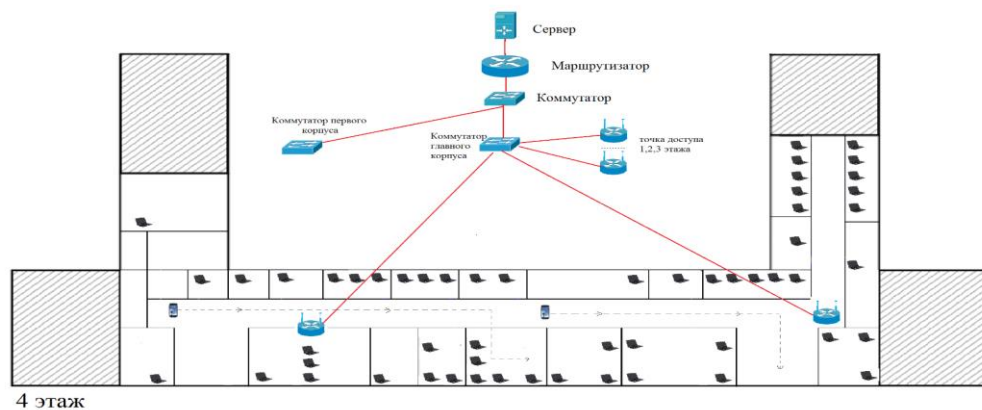


Рисунок 3.3 – Логическая схема беспроводной телекоммуникационной кампусной сети четвертого этажа главного корпуса ГТУ г. Сана [5]

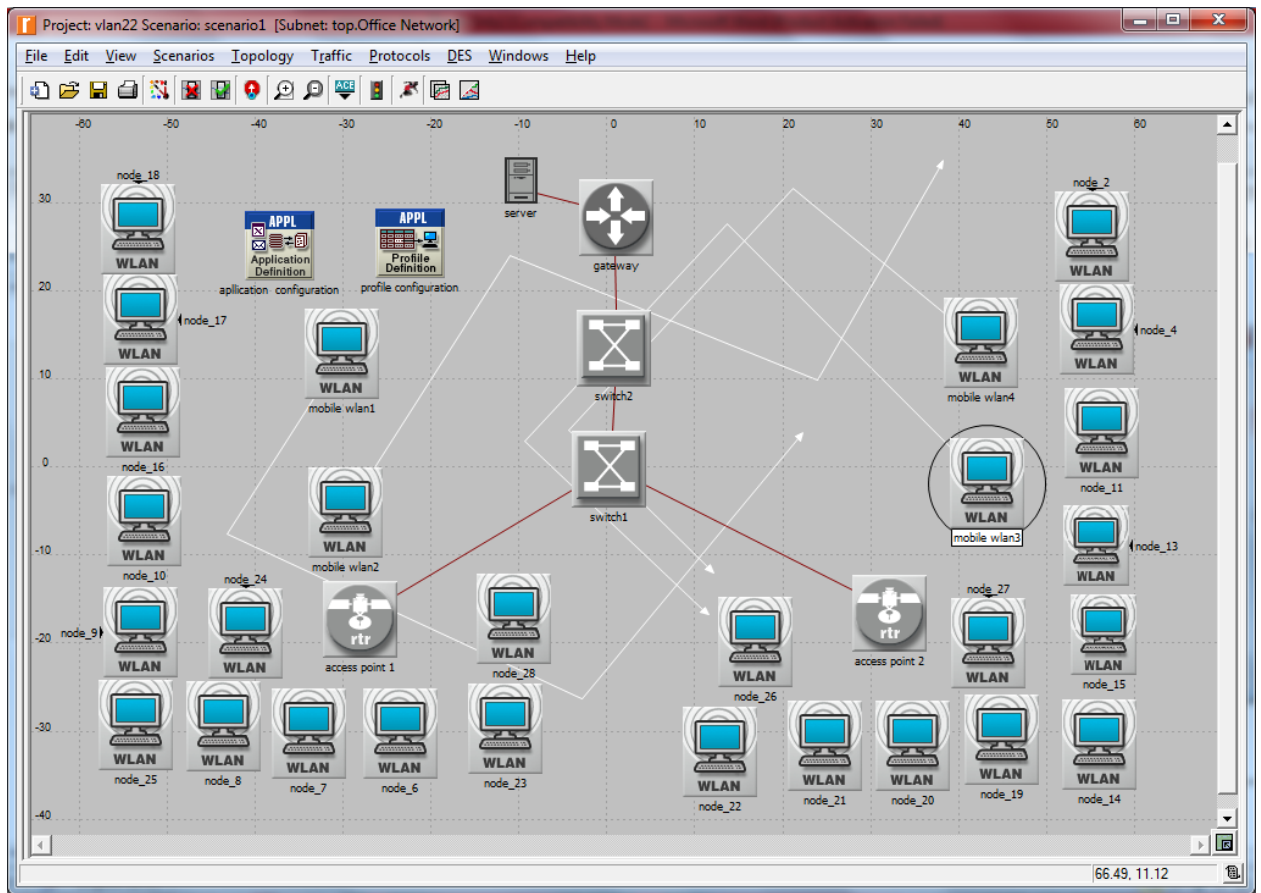


Рисунок 3.4 – Схема беспроводной телекоммуникационной кампусной сети четвертого этажа главного корпуса ГТУ г. Сана в программе OPNET Modeler [3]

Использование коммутируемых сетей порождает проблему надежности сети, так как древовидная топология коммутируемых локальных сетей очень уязвима – отказ любой линии связи или коммутатора приводит к потере связности сети, сеть фактически распадается на два или более сегмента. Для повышения надежности каждый корпус имеет дополнительное соединение с близлежащим зданием.

Беспроводные сети корпусов строятся идентично, поэтому нет необходимости рассматривать сеть каждого здания, каждого этажа в отдельности. Разработаем модель на примере беспроводной телекоммуникационной сети четвертого этажа главного корпуса.

## 3.2 Разработка имитационной модели беспроводной сети четвертого этажа главного корпуса СГТУ

### 3.2.1 Создание эскиза сети

Сначала нужно описать компанию, сферу деятельности, организационную структуру, объяснить необходимость взаимодействия между отделами и с внешними организациями, обосновать выбор оборудования, приложений, алгоритмов маршрутизации, программного обеспечения. Рассмотрим пошаговый алгоритм создания модели сети.

### 3.2.2 Моделирование сети в OpNet Modeler 17.5

#### Этап 1

При создании модели сети сначала необходимо дать названия проекту и сценарию в нем: *File-New* – название проекта: WLAN\_GTUSana

– название сценария : scenario 1 (рисунок 3.5).

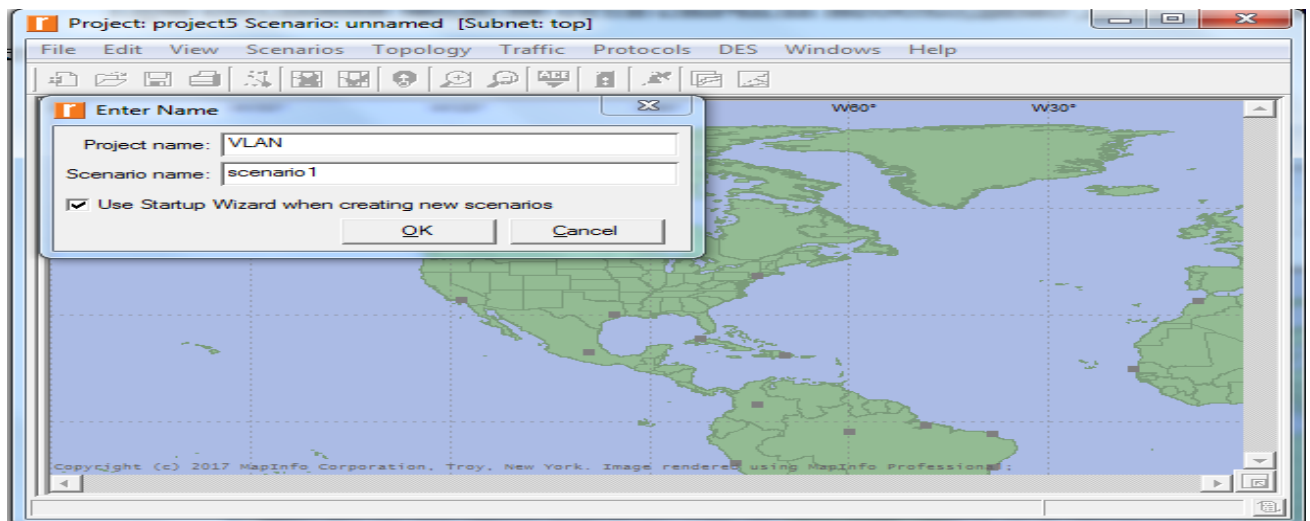


Рисунок 3.5 – Название проекта [3]

Далее выбираем размер сети (в первой части работы строим кампусную сеть, выбираем *campus*), выделяем необходимое и нажимаем клавишу *Next* (рисунок 3.6).

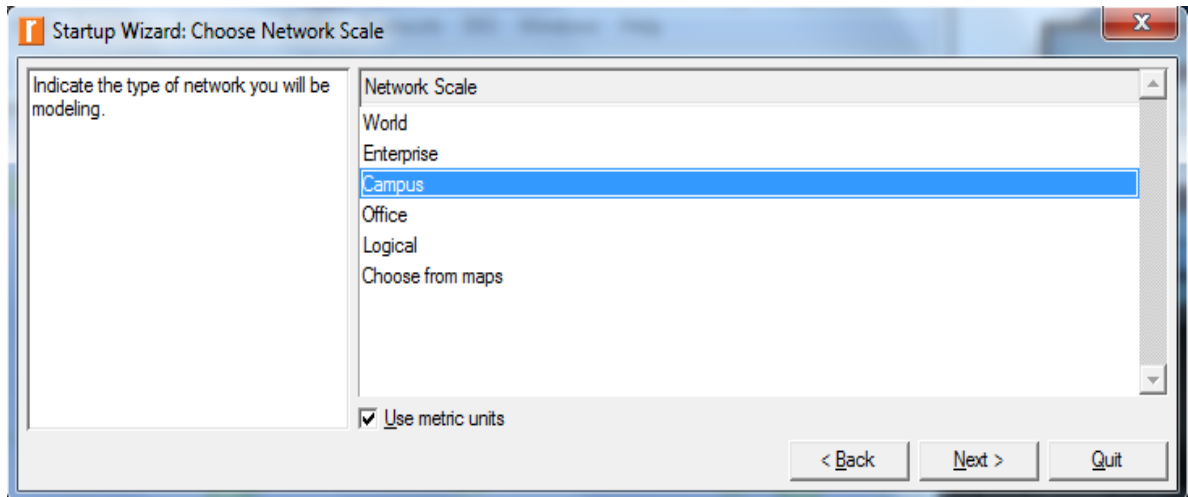


Рисунок 3.6 – Выбор размера сети [3]

На следующем этапе необходимо выбрать конкретные размеры местности (м), на которой будет располагаться сеть (механизм выбора размеров местности аналогичен выбору размера сети). Для создаваемой сети установим размеры 250x150 метров (рисунок 3.7).

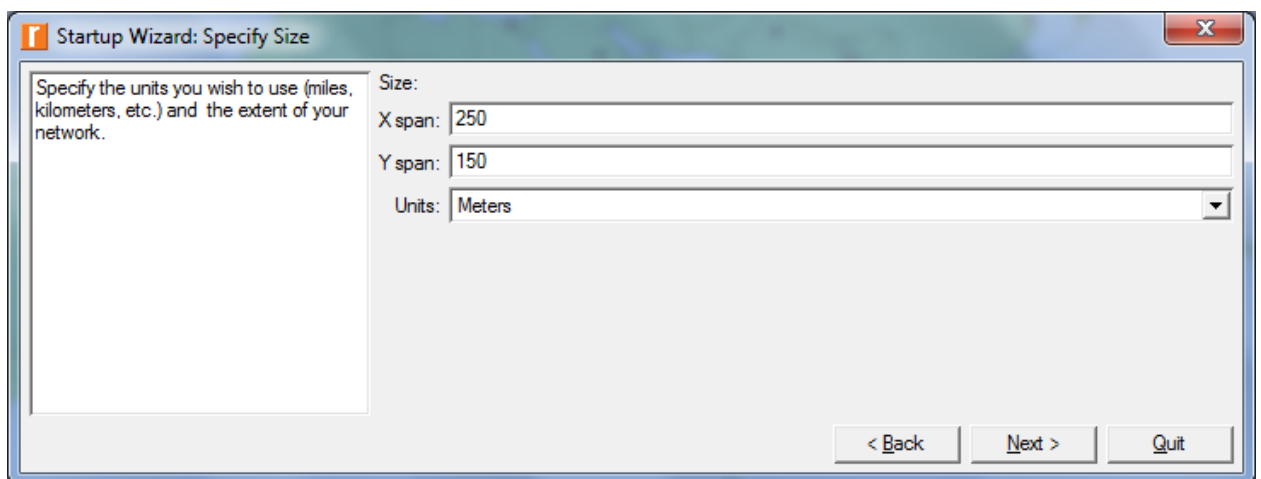


Рисунок 3.7 – Выбор конкретные размеры сети [3]



Далее необходимо определиться с выбором оборудования и технологий, которые будут применяться для создания сети. Для этого в списке выделяем необходимый элемент, при этом в поле *Include* появится надпись *Yes* – означающая, что этот пакет включен в проект (рисунок 3.8).

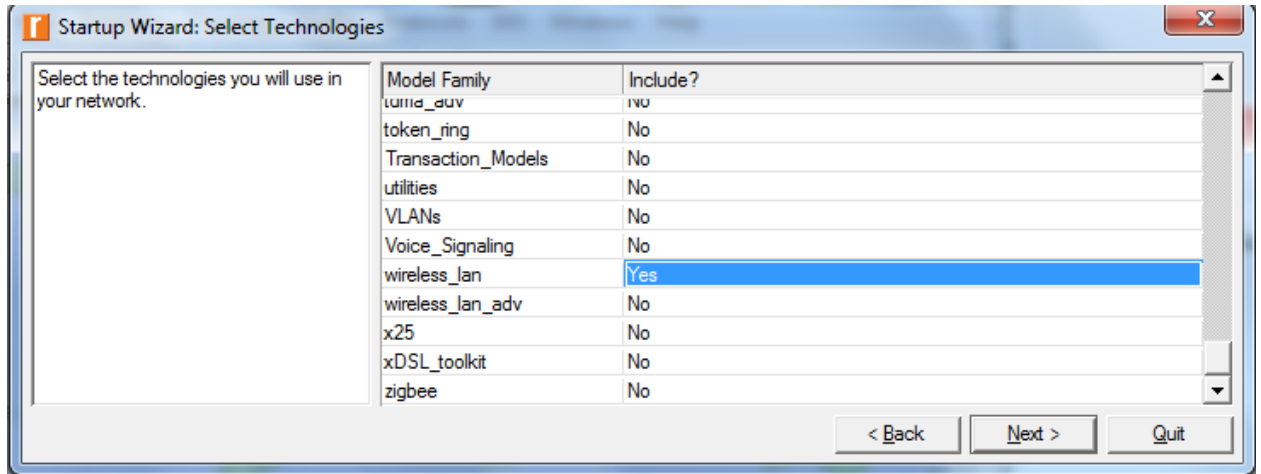


Рисунок 3.8 – Выбор оборудования и технологий [3]

После нажатия клавиши *Next*, программа предлагает убедиться в правильности введенных данных. После проверки параметров создаваемого проекта и нажатия клавиши *Ok* появляется рабочая область, где будет создаваться сеть, и палитра, где отображаются элементы, которые можно использовать в проекте сети (рисунок 3.9).

Набор элементов можно изменить путем нажатия клавиши *Configure Palette*. Элементы на рабочую область можно переносить из палитры. Для этого выделяем элемент в палитре щелчком левой кнопки мыши, вторым аналогичным щелчком, но уже в рабочей области, добавляем элемент в рабочую область.

Кроме того, в программе есть возможность создания комбинированных элементов из шаблонов. Для этого выбираем на панели инструментов *Topology* -> *Rapid Configuration* и, следуя пунктам, конфигурируем шаблон.

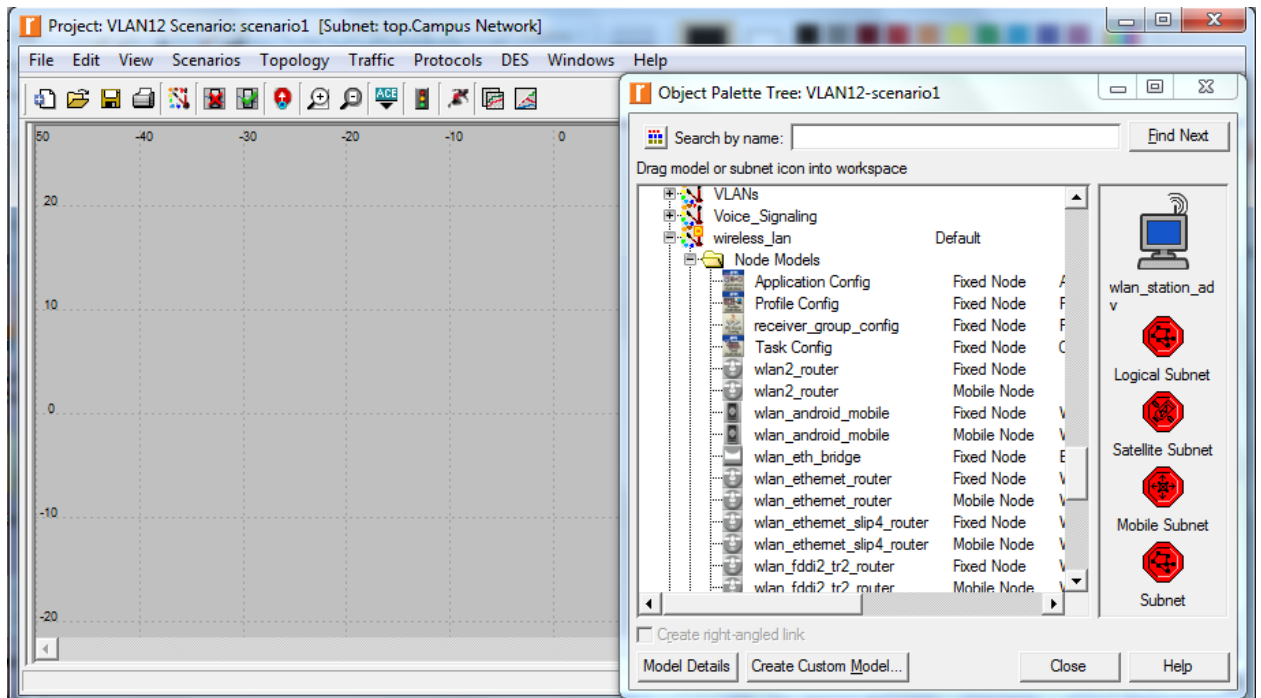


Рисунок 3.9 – Палитра проекта и рабочая область [3]

Модель сети создается с помощью редактора с использованием узлов (nodes) и каналов связи (links) из базы ресурсов (окно с изображениями узлов и связей, Object Palette). В таблице 3.1 показаны компоненты для сети.

Таблица 3.1 – Таблица компонентов сети [3]

Кол.	Компонент	База ресурсов	Описание
24	wlan_wkstn (Fixed node)	wireless_lan	Компьютеры (фиксированный узел)
4	wlan_wkstn (Mobile node)	wireless_lan	Компьютеры (мобильный узел)
1	ethernet_server	internet_toolbox	сервер
2	ethernet16_switch	internet_toolbox	коммутатор
1	ethernet4_slip8_gtwy	internet_toolbox	Маршрутизатор
2	wlan_ethernet_router	wireless_lan	Wireless LAN и Ethernet IP Router
5	100BaseT	internet_toolbox	Соединительные линии
1	Application Config	wireless_lan	Application Config определяет стандартные и пользовательские приложения, используемые в имитационном моделировании, включая параметры трафика и качества обслуживания
1	Profile Config	wireless_lan	Profile Config определяет режимы использования приложений пользователем или группой пользователей

На рисунке 3.10 представлена схема беспроводной сети главного корпуса ГТУ г. Сана в программе OPNET Modeler.

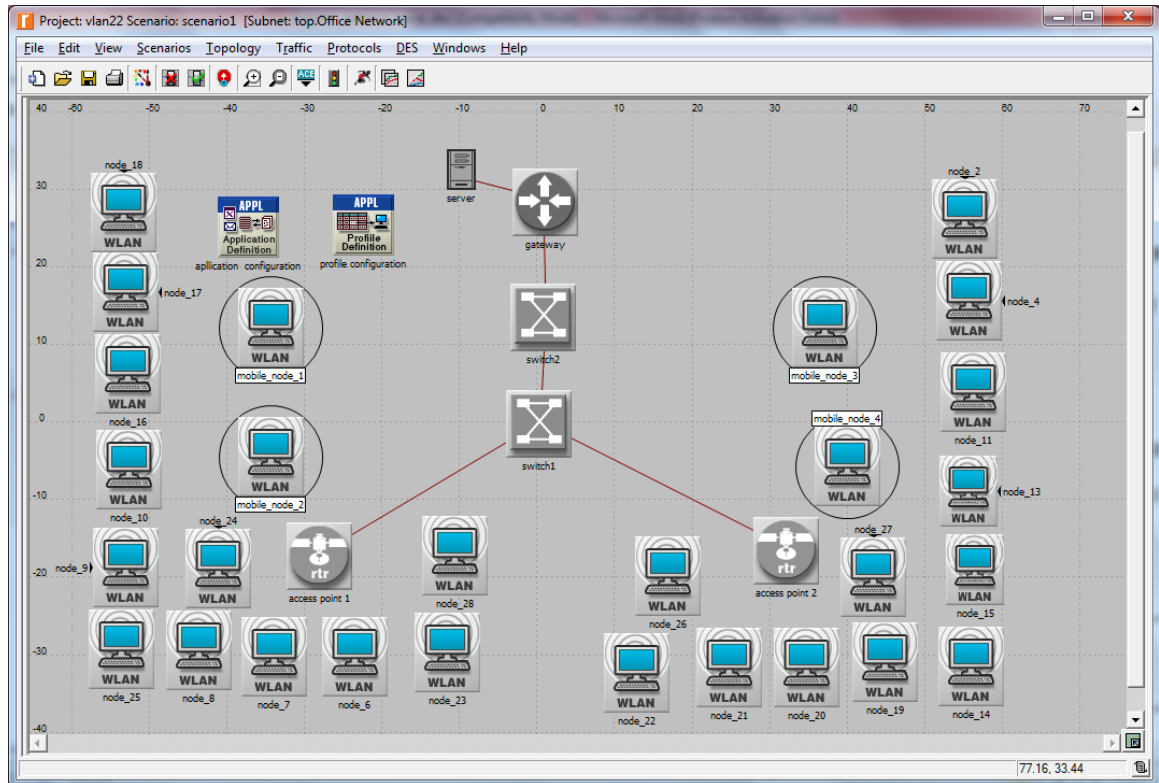


Рисунок 3.10 – Схема беспроводной сети главного корпуса ГТУ г.Сана в программе OPNET Modeler [3]

Созданная модель отражает взаимосвязь сетевых элементов беспроводной сети главного корпуса ГТУ г. Сана.

## Этап 2: Задать профили трафика, настроить оборудование, выбрать тип собираемой статистики

Для настройки оборудования необходимо нажать правой клавишей мыши на этом оборудовании и выбрать в меню пункт *Edit Attributes* (рисунок 3.11). В зависимости от выбранного оборудования в рабочей области появится окно с различным набором настраиваемых параметров.

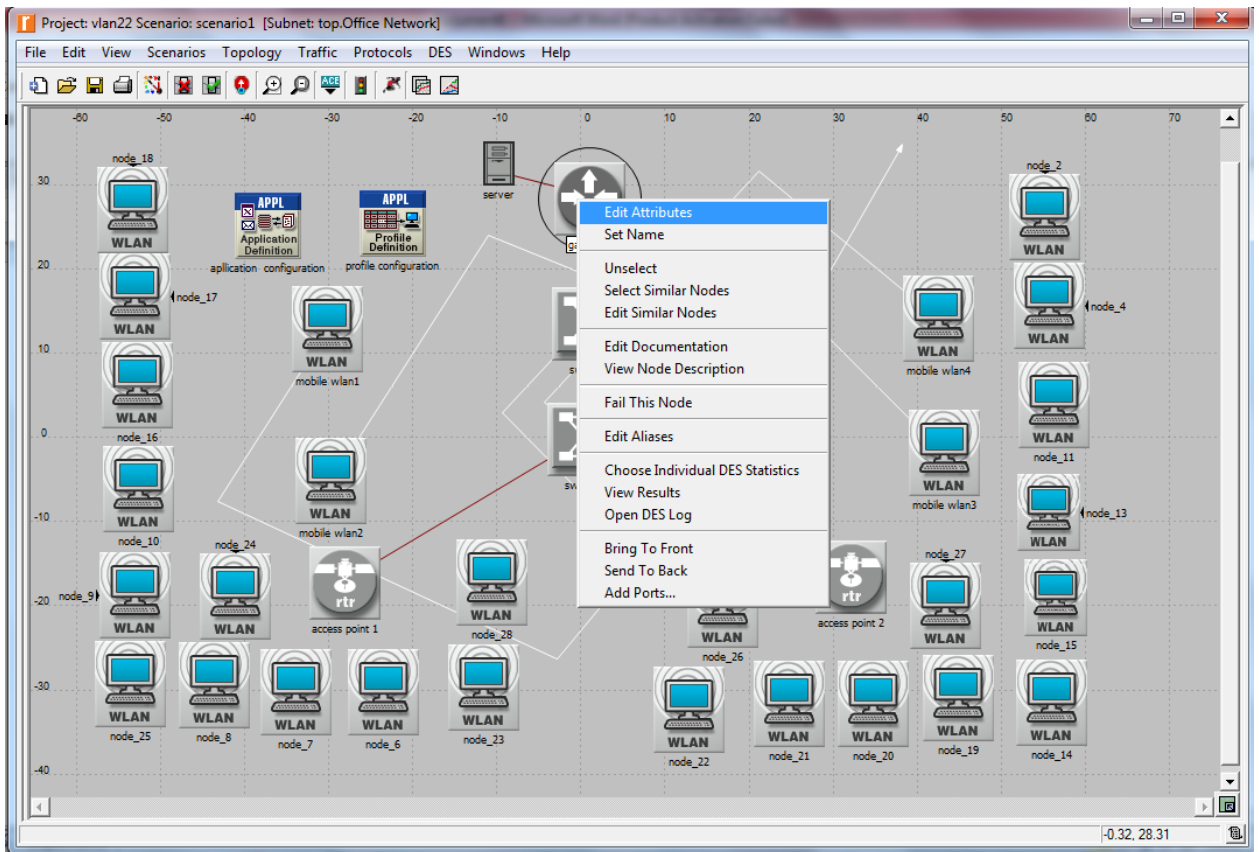


Рисунок 3.11 – Пункт *Edit Attributes* [3]

### Этап 3: Настройка параметров приложения и профиля

Тип трафика задается с помощью элемента палитры *Application Definition*. Элемент *Application Definition* необходимо перенести из палитры в рабочую область и разместить рядом с сервером.

*Application Definition* содержит характеристики приложений, создаваемых в виде потоков и имеющих собственные параметры трафика. Для создания потоков на *Application Definition* нужно нажать правую кнопку мыши и выбрать графу *Edit Attributes* (рисунок 3.12), примерно созданы 3 стандартных потока для таких случаев. Сюда входит доступ к базам данных, обработка электронной почты, передача файлов, работа в Интернете и т.д.

После создания потоков приложений необходимо сконфигурировать профили пользователей, работающих в спроектированной сети. Эту функцию выполняет элемент палитры *Profile Definition*.

Каждому профилю дается название и описывается ряд пользовательских характеристик: время начала работы, продолжительность, окончание, интенсивность его пребывания и работы в сети и какими из предложенных (созданных) приложений он пользуется. Указанные параметры задаются аналогично *Application Definition* через пункт меню *Edit Attributes* (рисунок 3.13).

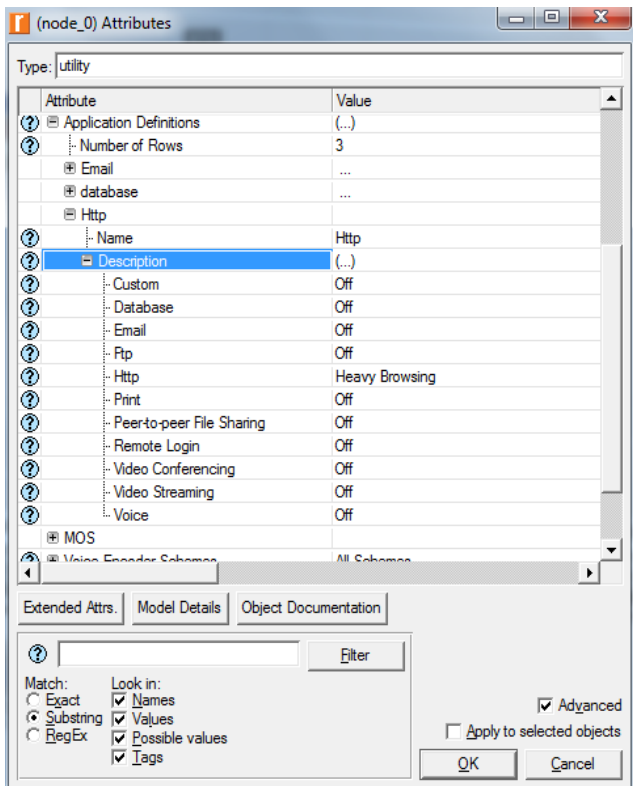


Рисунок 3.12 – Диалоговое окно настроек параметров для *Application Definition* [3]

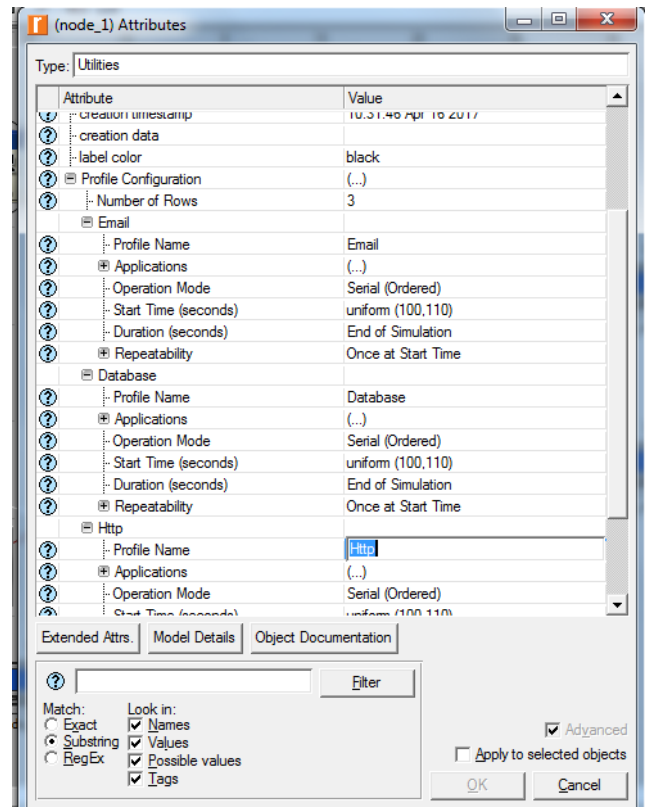


Рисунок 3.13 – Настройка профилей пользователей [3]

## Этап 4: Настройка сервера

При настройке сервера нужно прописать тип трафика, генерируемого пользователями. Самые распространенные типы трафика: данные, речь, видео. Каждый из них предъявляет различные требования к передаче, обеспечению необходимого качества обслуживания, выделению достаточной пропускной способности. В зависимости от направления деятельности предприятия/фирмы по сети будет передаваться трафик различного рода. Соответственно при проектировании важно правильно рассчитать загрузку каналов и оборудования. Проверить расчеты позволяет моделирование планируемой нагрузки.

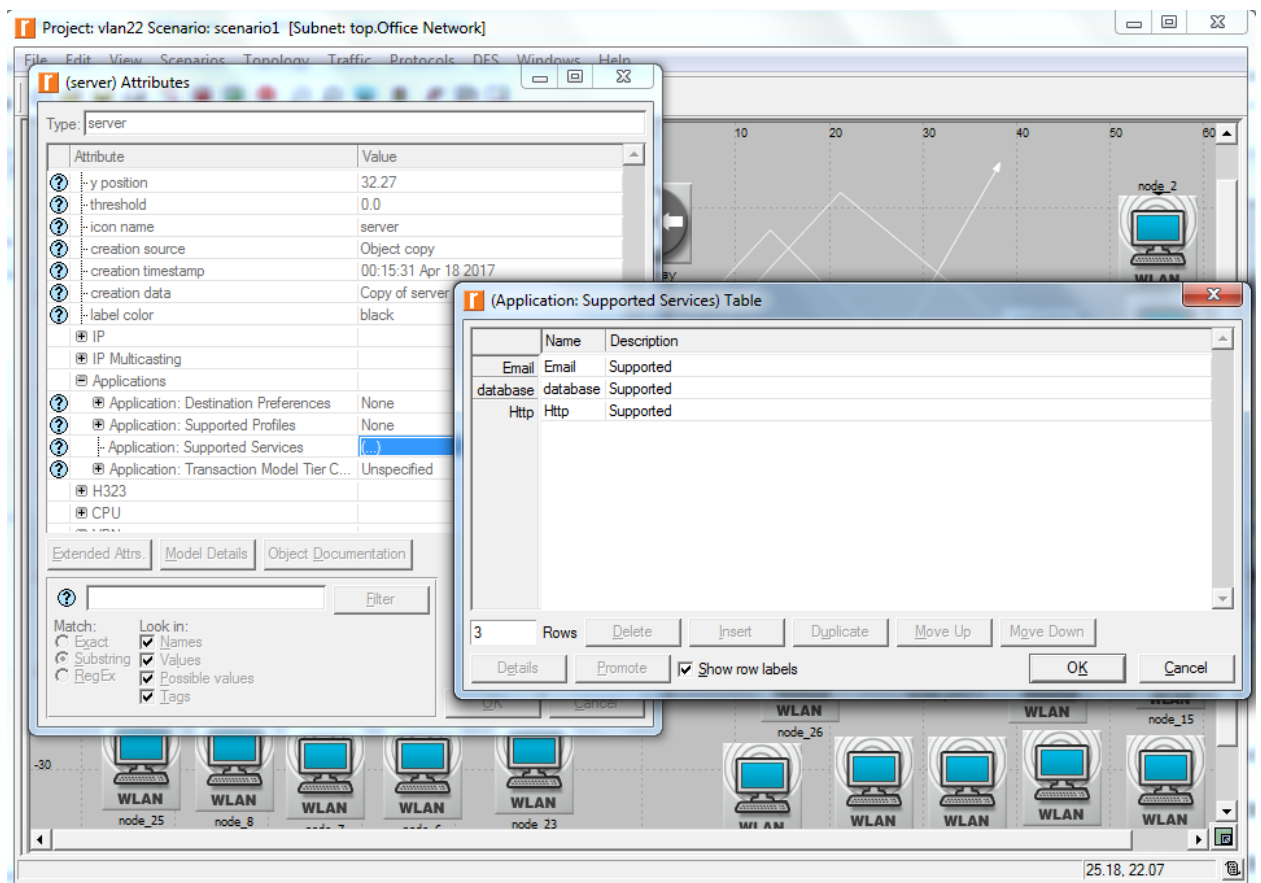


Рисунок 3.14 – Настройки сервера [3]

Тип собираемой статистики указывается также через пункт меню *Choose Individual Statistics*. Для сервера необходимо собрать следующие типы статистики:

загрузка процессора, обращение к приложениям сервера – полученный и отправленный трафик (*Application Demand – Traffic Sent, Traffic Received*), загрузка сервера *FTP, HTTP, E-mail, DB*, в разделе *Requesting Server Custom Application* выбрать *Application Response, Total Request/Response Size, Traffic Received/Sent, Application/Group Response Time*.

### Этап 5: Настройка маршрутизатора

Для настройки параметров маршрутизатора нужно нажать правой кнопкой мыши на его название и выбрать графу *Edit Attributes* (рисунок 3.15).

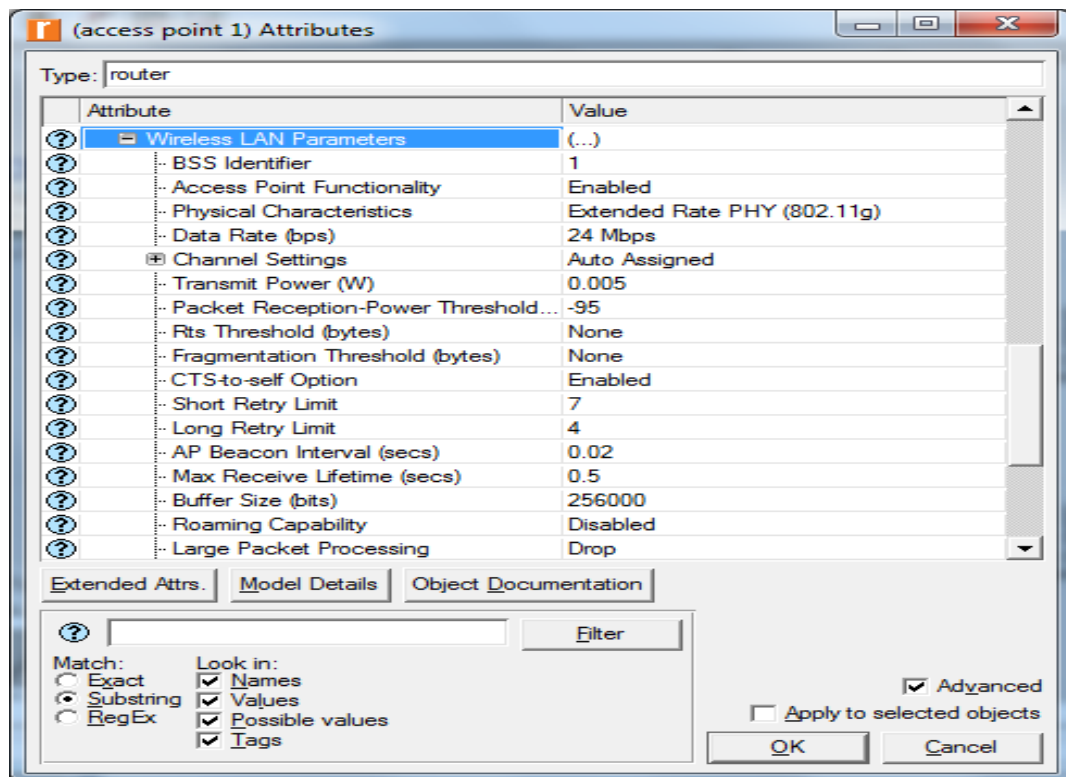


Рисунок 3.15 – Настройки маршрутизатора [3]

На диалоговом окне настроек параметров роутера можно задать имя беспроводной сети (BSS Identifier), выбор стандарта связи, скорость передачи (Data Rates) и т.д.

Для маршрутизатора обязательно собрать следующие статистические показатели: загрузка процессора, объем переданного, полученного, отброшенного трафика и т.д.

### Этап 6: Настройка коммутатора

Как правило, дополнительная настройка коммутатора не требуется, если нет необходимости реконфигурации портов или настройки *VLAN*. Для коммутатора можно указать тип собираемой статистики – нажать правой кнопкой мыши на объект и выбрать графу *Choose Individual Statistic*. Далее галочками выбрать интересующие параметры. Для коммутатора обязательно собрать следующий статистические показатели: объем трафика переданного, полученного, отброшенного.

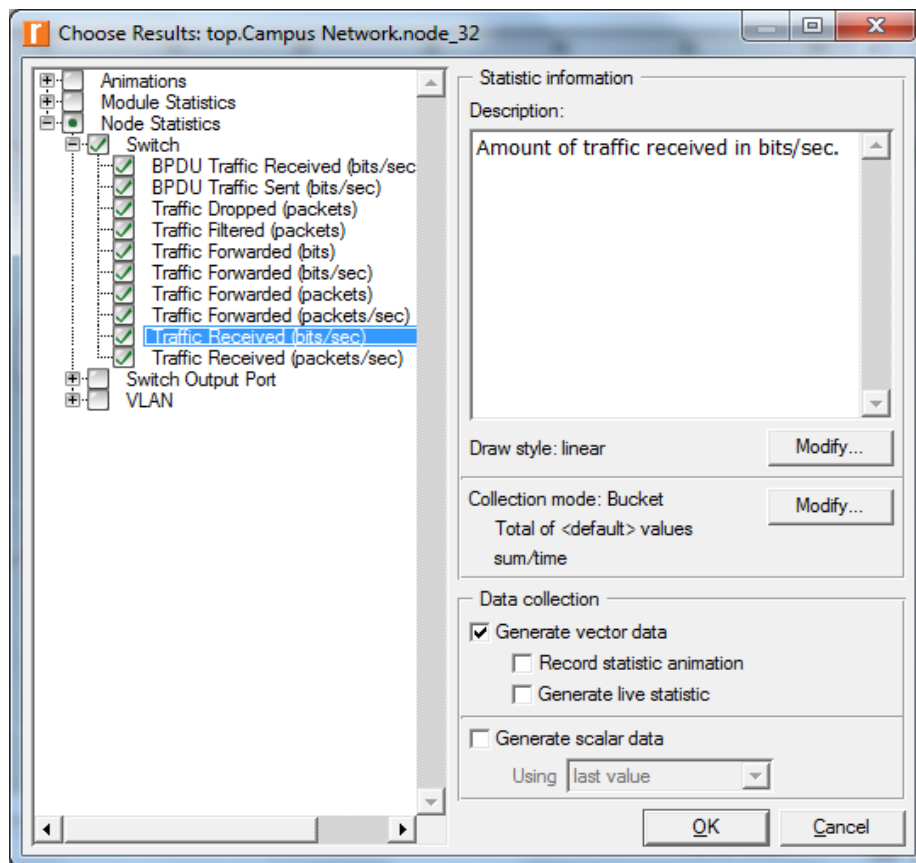


Рисунок 3.16 – Выбор типа собираемой статистики для коммутатора [3]



### **Этап 7: Настройка оконечных пользователей**

При настройке оборудования для оконечных пользователей нужно указать название и тип пользователя. Оконечный пользователь (рабочая станция) для WLAN сети может быть представлен двумя способами: фиксированный узел или мобильный узел.

Подключения оконечных пользователей к маршрутизатору, происходит следующим образом. Выбираем пункт меню *Edit Attributes*: выбрать Wireless LAN → Wireless LAN Parameters на поле BSS Identifier укажет имя и параметры беспроводной сети и заполняется графа *Application – Supported Profiles*, указывающая, сколько и какого рода пользователей будут присутствовать в этой сети. Здесь аналогично серверу создаются потоки, учитывающие пользователей сети, на основе профилей, созданных в элементе рабочей области *Profile Definition* (рисунок 3.17).

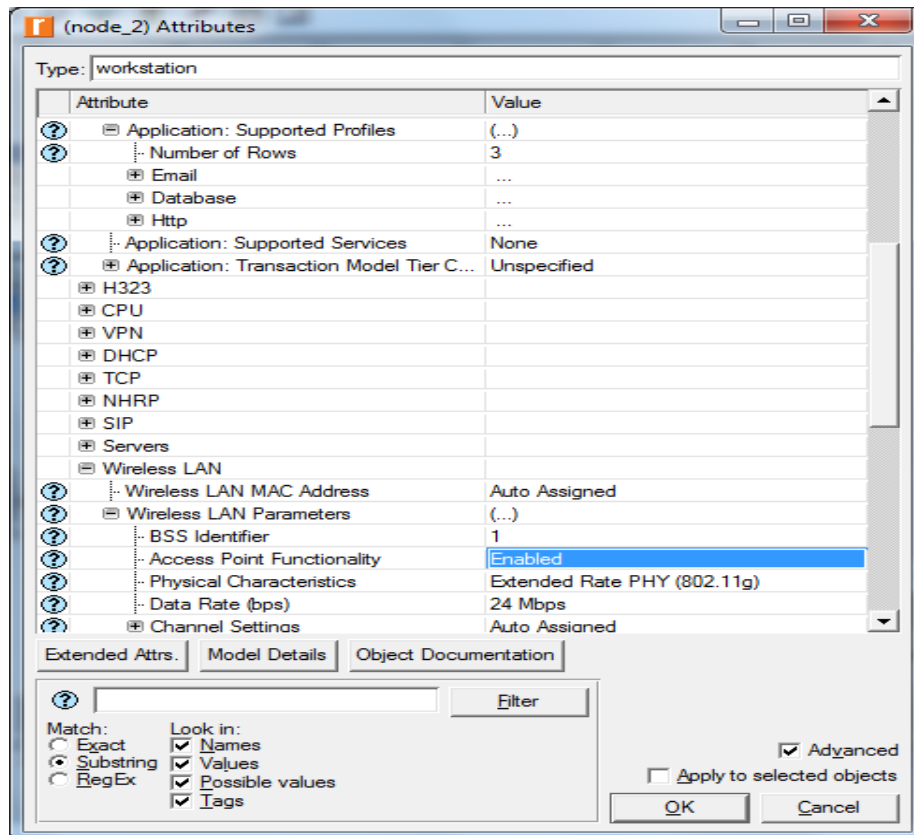


Рисунок 3.17 – Настройка рабочих станций [3]

### Этап 8: Построить траекторию для мобильных рабочих станций

Выбрать из меню пункт Topology → Define Trajectory...

Нажать левую кнопку мышки на рабочей области и указать линий движений для мобильных рабочих станций и нажать Complete чтобы сохранить траекторию.

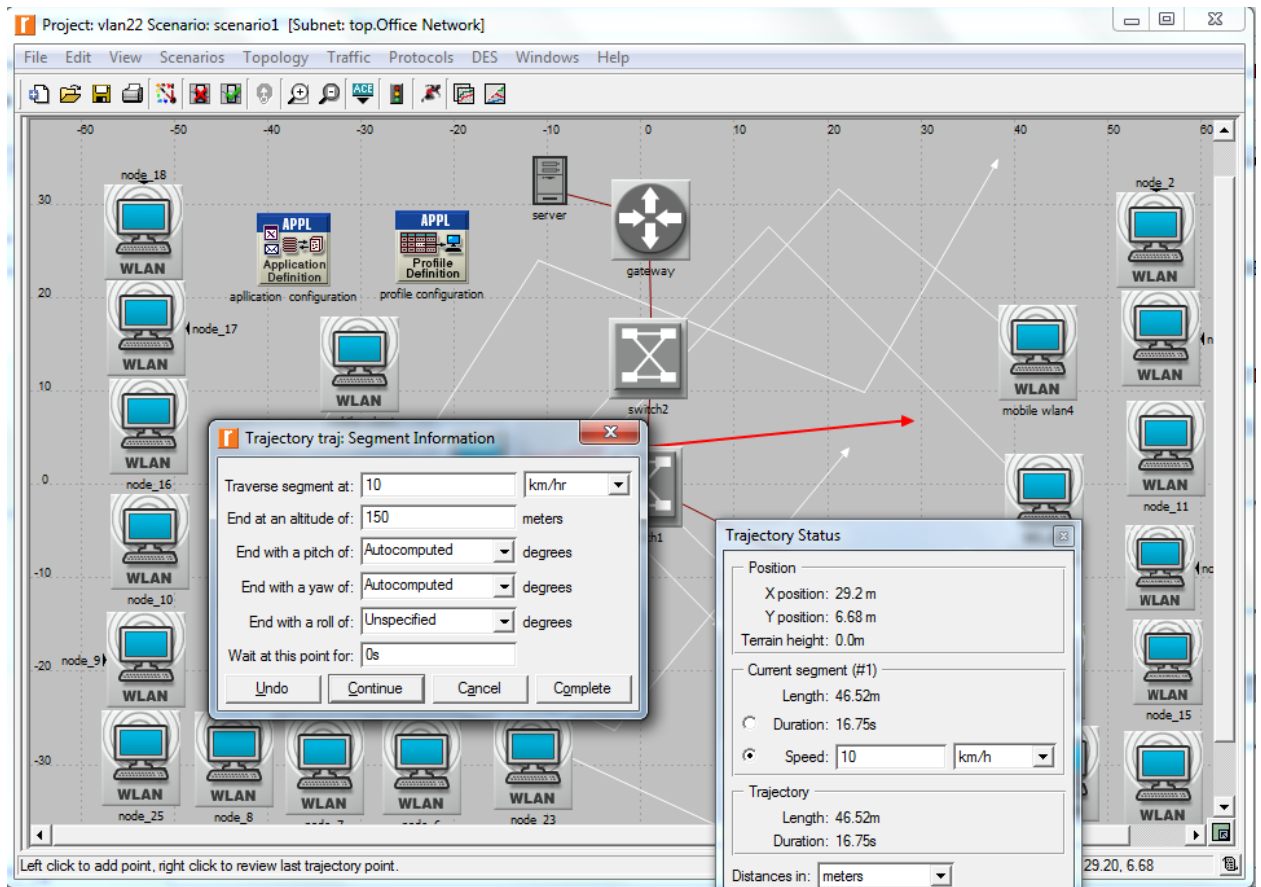


Рисунок 3.18 – Построить траекторию для мобильных рабочих станций [3]

Для конечных пользователей снять следующую статистику:

- задержку, вариацию задержки, объем трафика полученного, отправленного для типов приложений: Video Called Party, Video Calling Party, Voice Application;
- количество загруженных объектов/страниц (Downloaded Objects/Pages) для Client http;
- размеры загруженных файлов (Downloaded File Size) и Downloaded Response Time для Client Ftp;
- объемы полученного/переданного трафика (Traffic Received/Sent) для Client E-mail и Client DB;
- загрузку, задержку, объем полученного/переданного трафика (Traffic Received/Sent) в разделе Ethernet [8].

### Этап 9: Настройка протокола сети

Выбрать из меню пункт **Protocols** → **Wireless LAN** → **Configure PHY and Data Rate...**

На диалоговом окне настроек протокола нужно выбрать стандарт беспроводной связи (Technology ) и скорость передачи беспроводной сети. Как показано на рисунок 3.19:

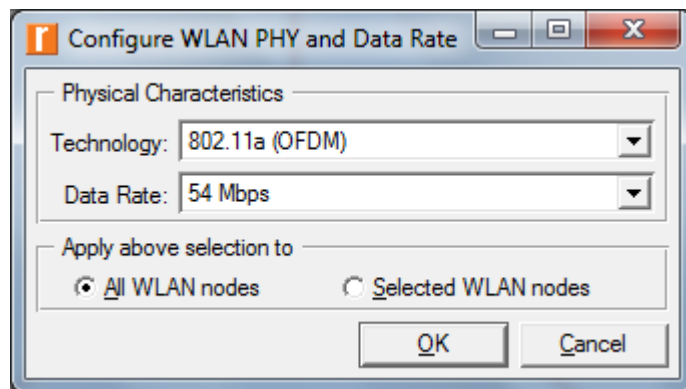


Рисунок 3.19 – Настройки протокола сети [3]

Теперь можно приступить к симуляции, предварительно сохранив проект, нажав в меню проекта кнопку *Save*. Проект будет сохранен в *C:\Documents and Settings\user\op\_models*. При повторном запуске программы *OpNET* для открытия существующего проекта необходимо в меню *File* выбрать *Open* и название своего проекта.

### Этап 10: Произвести симуляцию. Оценить полученные результаты

Перед началом процесса симуляции необходимо настроить некоторые параметры симуляции. Для этого на панели инструментов нужно нажать кнопку *configure/run simulation* и войти в режим симуляции (рисунок 3.20).

Пакет *OpNet Modeler* предлагает указать продолжительность работы сети (в данном случае – 3 ч). В следующих закладках имеется возможность настройки

глобальных параметров сети, параметров моделирования для каждого элемента, вывода отчетов, анимации во время моделирования и др. Теперь можно запускать процесс моделирования. Чтобы запустить симуляцию нужно нажать кнопку *Run* (рисунок 3.21).

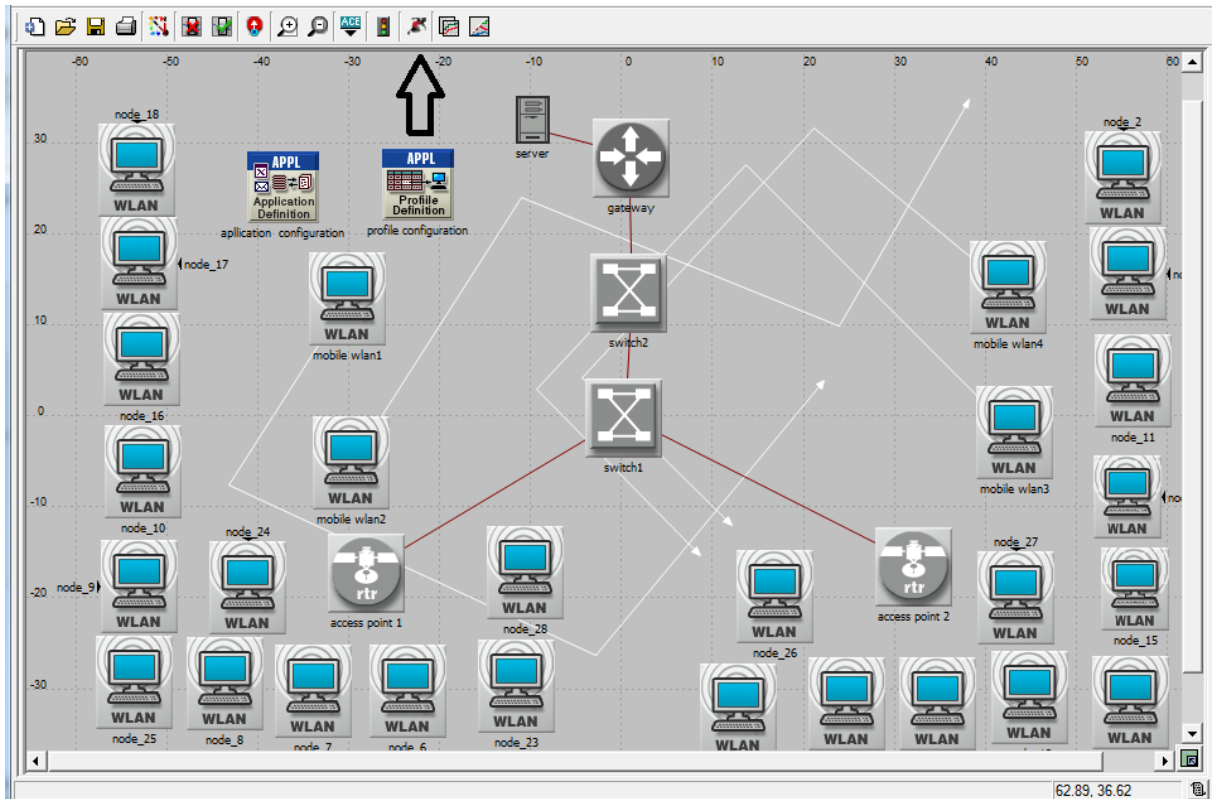


Рисунок 3.20 – Кнопка запуска режима симуляции [7]

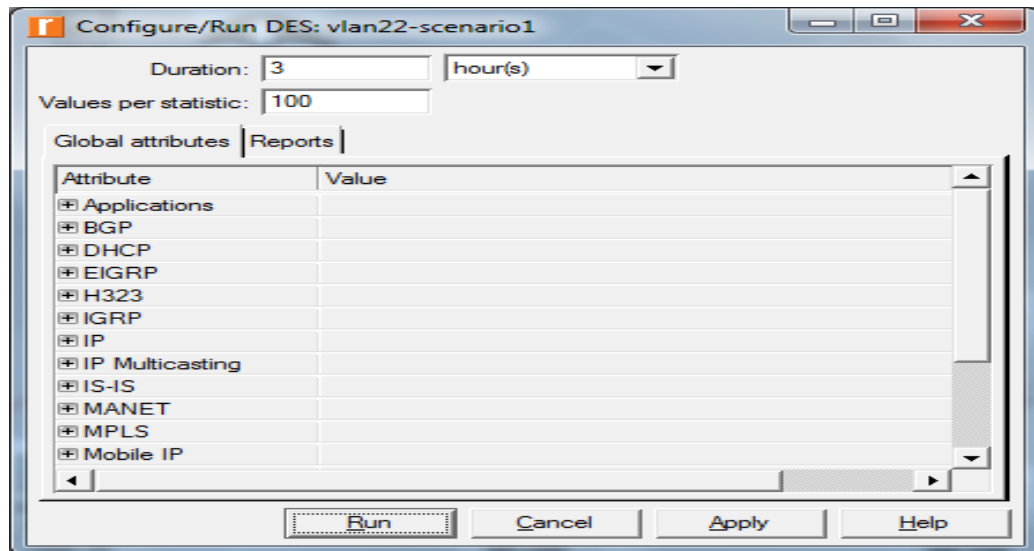



Рисунок 3.21 – Настройка параметров моделирования [7]

После завершения процесса симуляции нагрузку на сеть можно увидеть, перейдя на закладку *Simulation Speed* (рисунок 3.22).

Во время моделирования процессов, происходящих в построенной сети, в реальном времени на экране строится график активности, состоящий из двух кривых: синяя отображает ситуацию в каждый момент времени, (время откладывается по оси абсцисс), красная показывает среднее значение.

Для просмотра результатов моделирования работы сети «под нагрузкой» выбираем пункт *View Result*, для этого на рабочей области необходимо кликнуть правой кнопкой мыши и в меню выбрать соответствующий пункт либо нажать на панели инструментов кнопку 

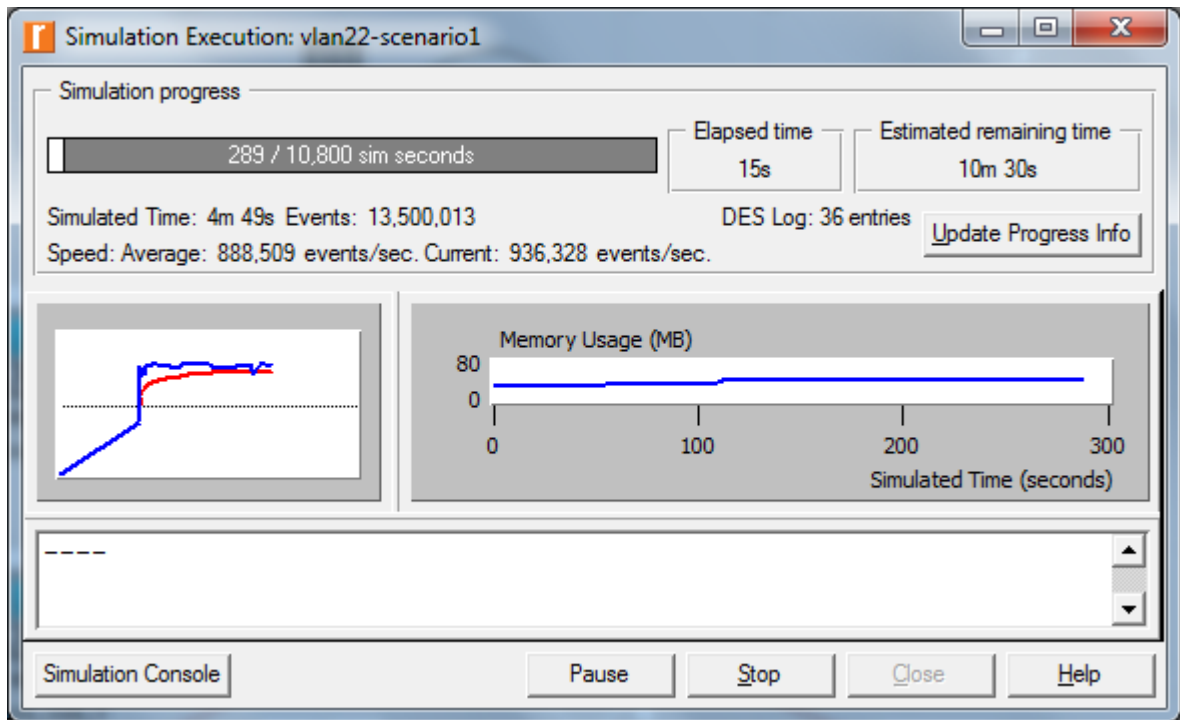


Рисунок 3.22 – Результаты моделирования [7]

В окне *View Result* зелеными галочками можно выбрать интересующий тип статистики на различном оборудовании, например на рисунке 3.23 показан график количества отправленных и получаемых пакетов за единицу времени (*Traffic Forwarded u Traffic Received*) на коммутаторе.

На рисунке 3.24 представлен график нагрузки на канал, по которому можно оценить пропускную способность канала, т.е. видно, что за 15м работы сети по каналу передавалось в среднем 4000-6000 кбит/с.

На рисунке 3.25 представлен график задержки на точке доступа 2, на рисунке 3.26 – задержка между gateway и коммутатором 2, рисунке 3.27 – задержка между сервером и gateway, рисунке 3.28 – задержка между коммутатором 1 и точкой доступа 2 и на рисунке 3.29 – задержка между коммутатором 2 и 1.

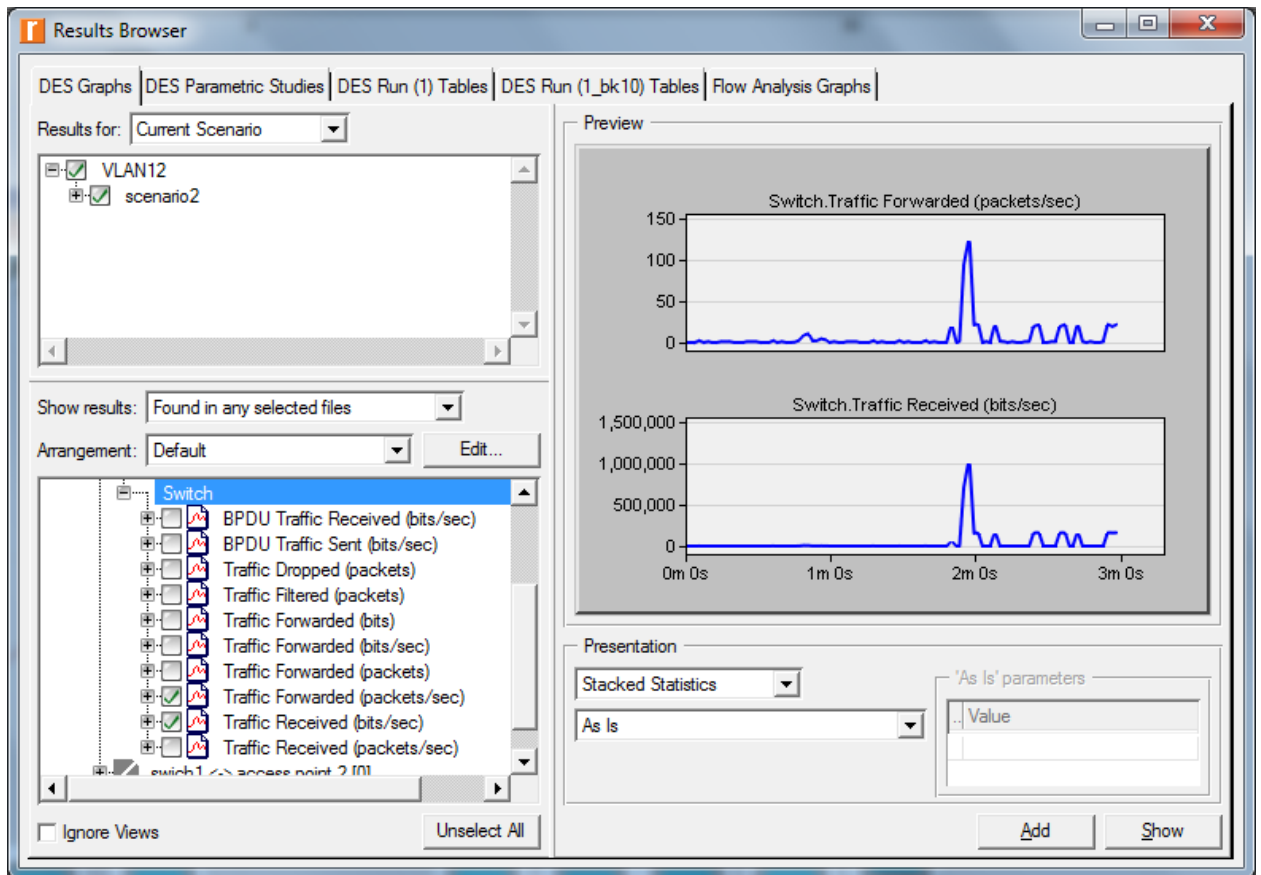


Рисунок 3.23 – Количество отправленных и получаемых пакетов за единицу времени, пак/s [7]



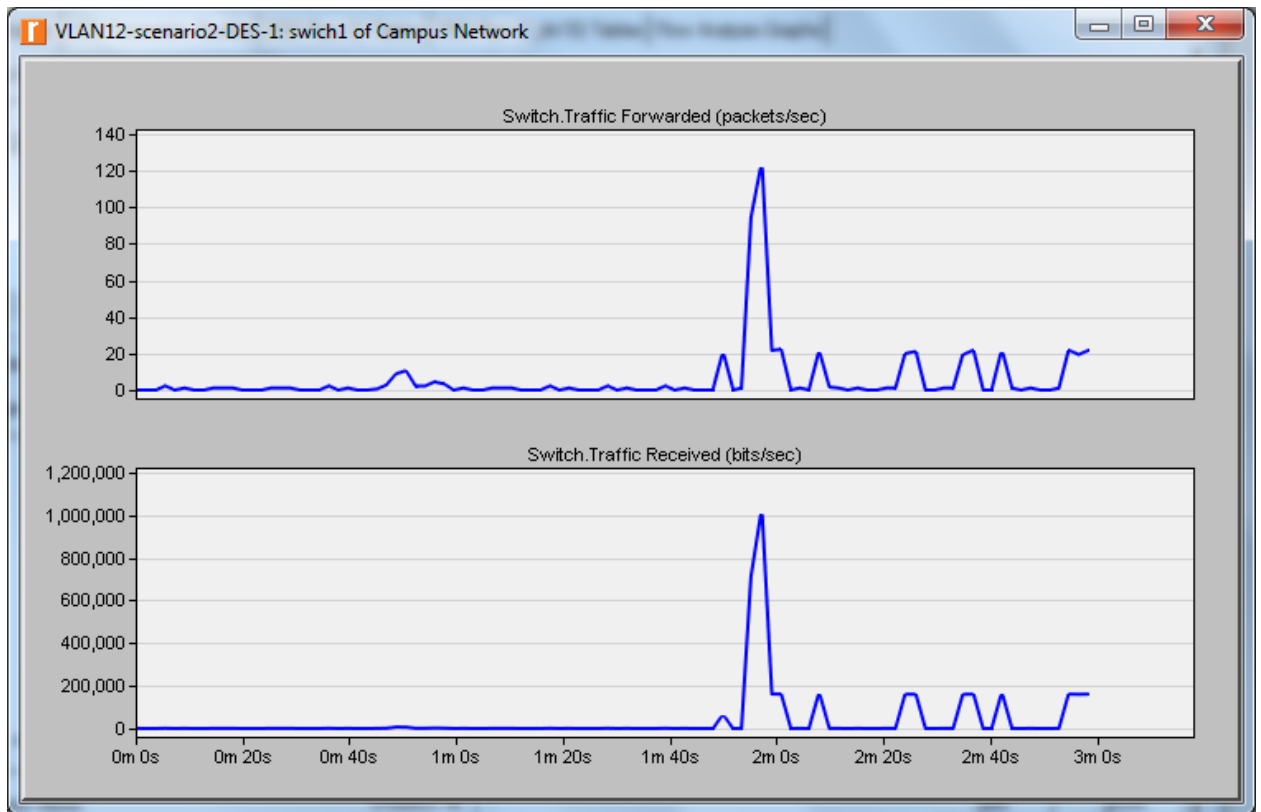


Рисунок 3.24 – График нагрузки в канале [7]

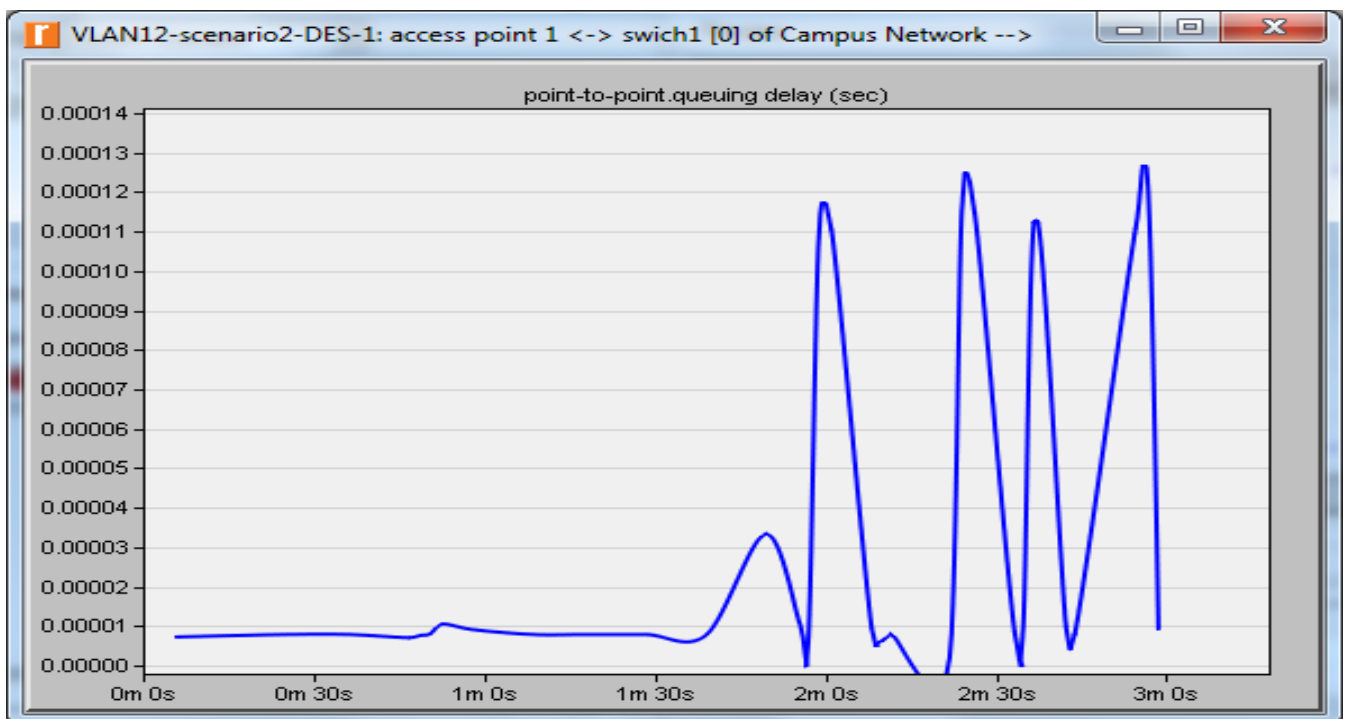


Рисунок 3.25 – Задержка между точкой доступа 1 и коммутатором 1

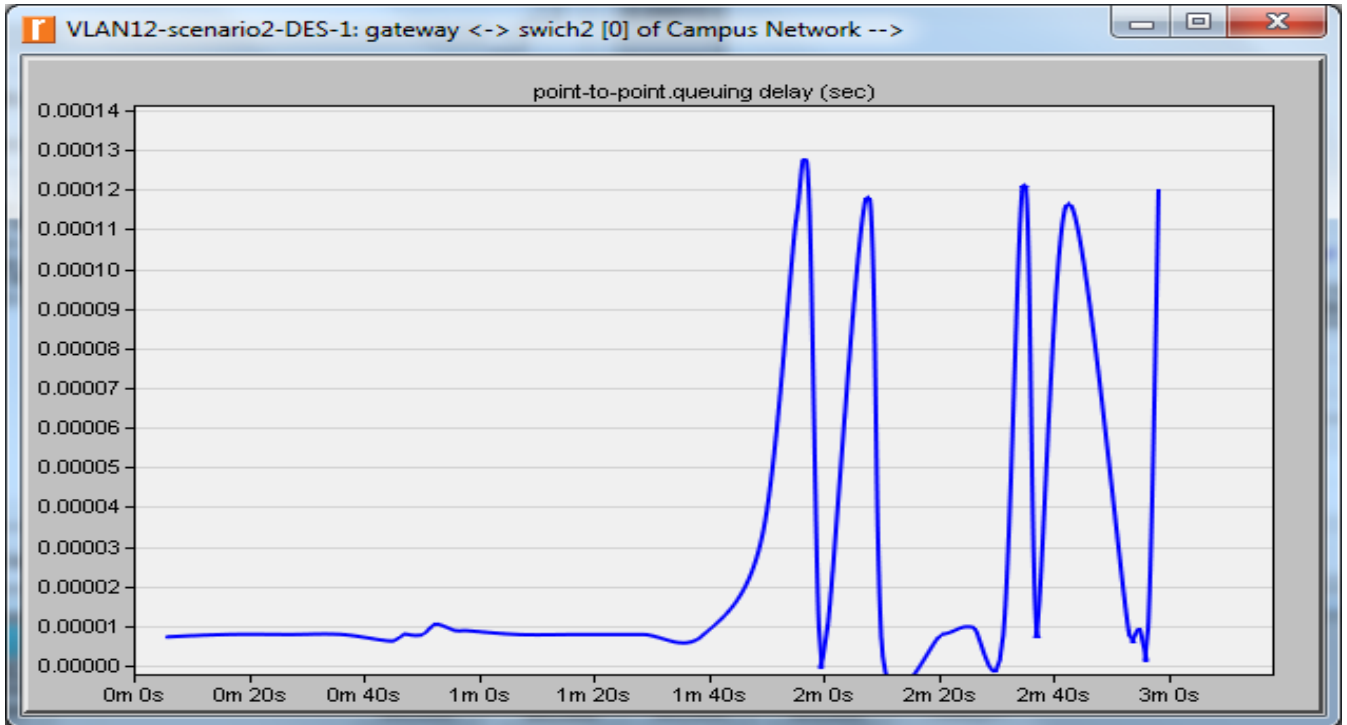


Рисунок 3.26 – Задержка между gateway и коммутатором 2

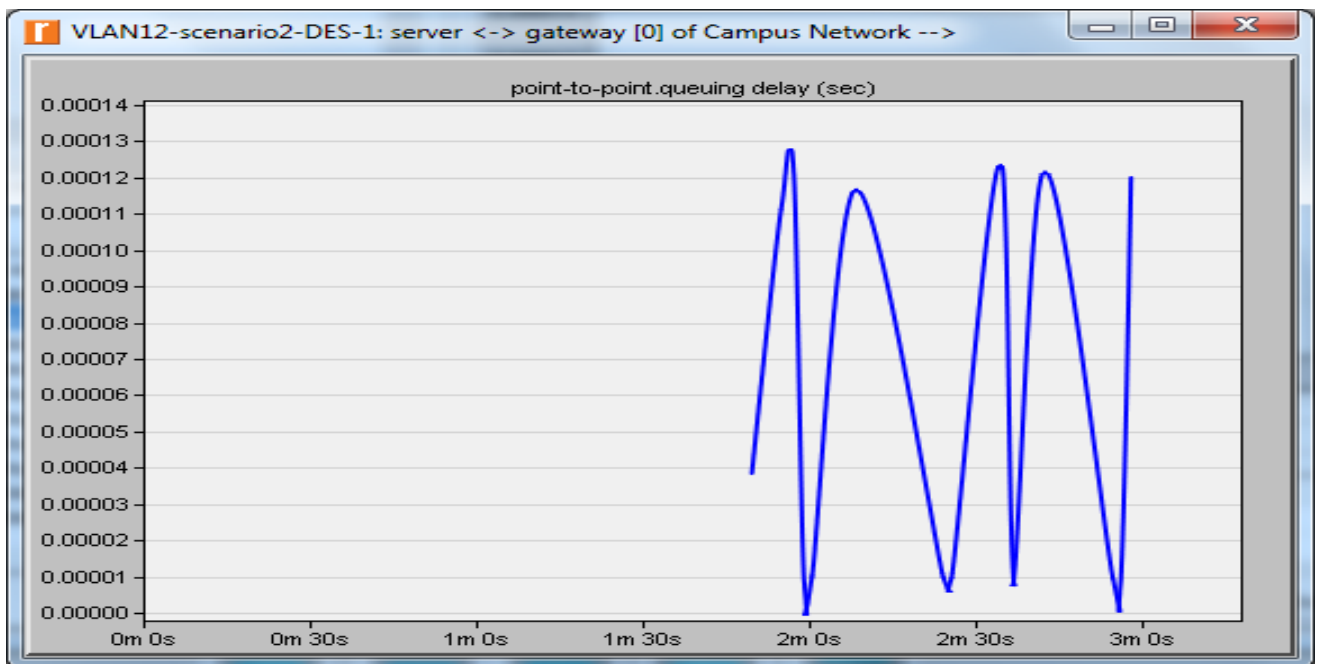


Рисунок 3.27 – Задержка между сервером и gateway

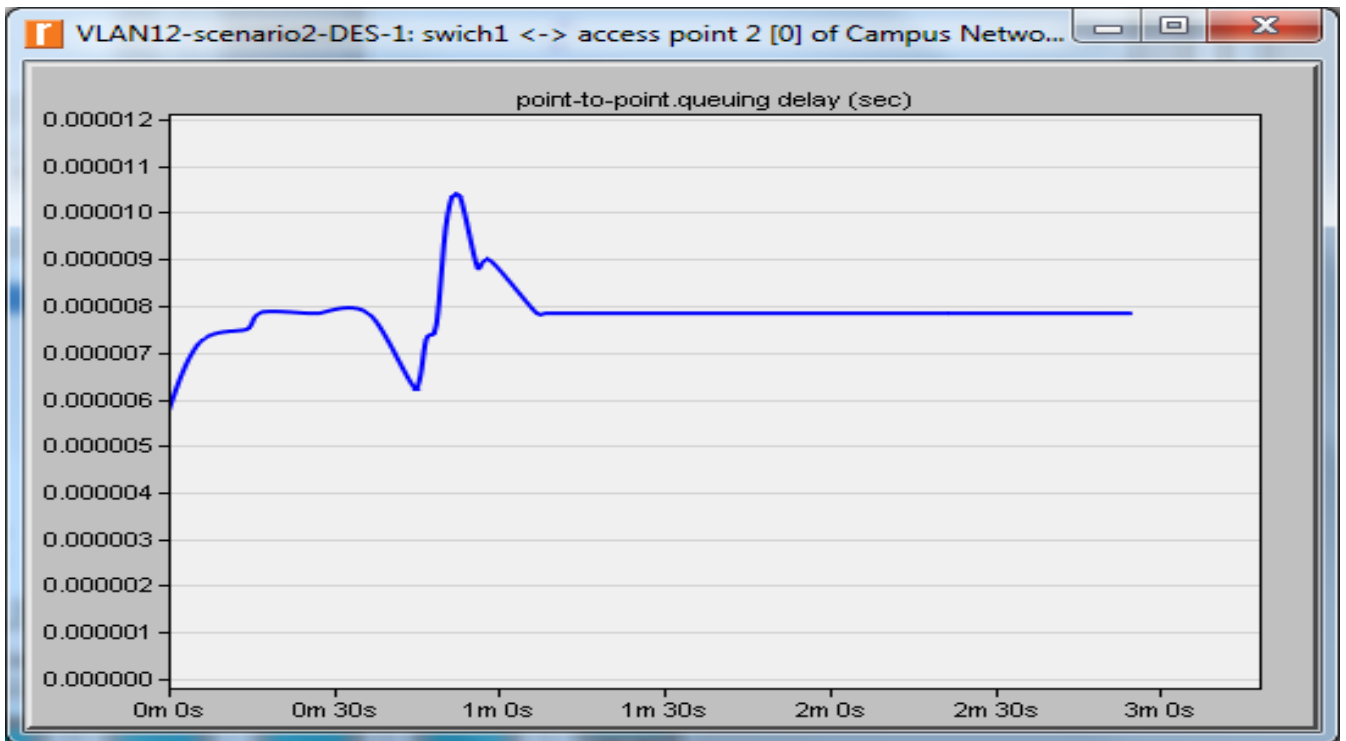


Рисунок 3.28 – Задержка между коммутатором 1 и точкой доступа 2

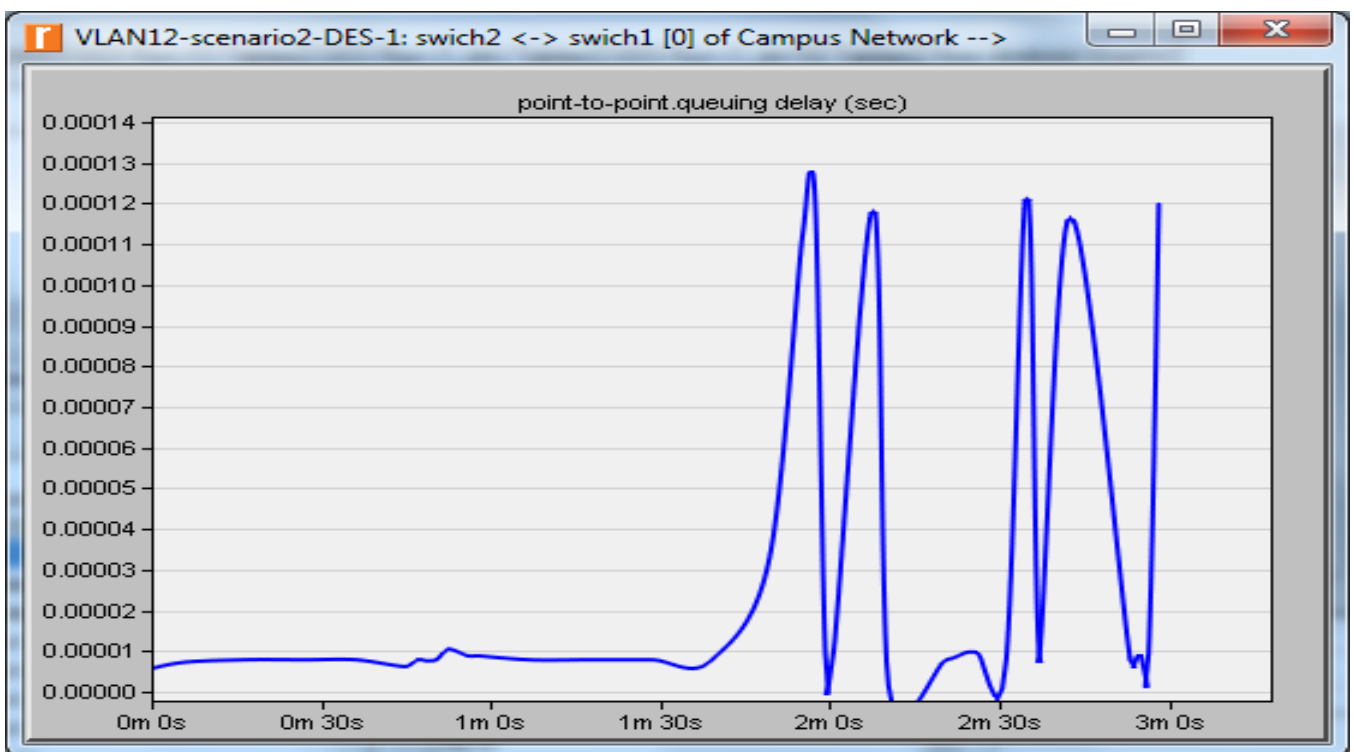


Рисунок 3.29 – Задержка между коммутатором 2 и 1

Таким образом, полученная модель позволяет оценить важнейший параметр качества сервиса – задержки.

### **3.3 IP протокол, маршрутизация в беспроводной сети связи**

Маршрутизатор в сети должен иметь возможность просматривать адрес назначения в пакете и затем определить, какой из выходных портов является лучшим выбором, чтобы отправить пакет к нужному адресу. Маршрутизатор принимает такие решения, консультируясь с таблицей пересылки.

Основопологающая проблема маршрутизации заключается в том, как маршрутизаторы получают информацию в своих таблицах переадресации?

Алгоритмы маршрутизации необходимы для построения таблиц маршрутизации и, следовательно, для пересылки таблиц.

Основная проблема маршрутизации – найти путь с наименьшей стоимостью между любыми двумя узлами, где стоимость пути равна сумме затрат всех ребер, составляющих путь.

Маршрутизация достигается в большинстве практических сетей путем запуска протоколов маршрутизации между узлами. Протоколы обеспечивают распределенный, динамичный способ решения проблемы поиска недорогих пути при наличии сбоев связи и узла и изменения краевых затрат.

Одним из основных классов алгоритмов маршрутизации является алгоритм вектор-расстояние. Каждый узел конструирует вектор, содержащий расстояния (затраты) ко всем остальным узлам, и распределяет этот вектор своим ближайшим соседям. RIP – это канонический пример протокола маршрутизации, построенного на алгоритме вектор-расстояние. Маршрутизаторы выполняющие RIP регулярно отправляют свои рекламные сообщения. (Например, каждые 30 секунд). Маршрутизатор также отправляет сообщение об обновлении всякий раз, когда

инициированное обновление с другого маршрутизатора приводит к изменению его таблицы маршрутизации.

Протокол управляющих сообщений Интернета (ICMP) может использоваться для анализа производительности созданных маршрутов. Он может использоваться для моделирования трафика между маршрутизаторами без необходимости запуска приложений на конечном узле.

Для примера настроим сеть, которая использует протокол RIP в качестве протокола маршрутизации и проанализируем таблицы маршрутизации, сгенерированные на маршрутизаторах. В результате моделирования можно оценить, как на RIP влияют сбои. Также будем использовать ICMP анализа созданных маршрутов.

### **3.3.1 Создать новый проект**

1. Запускаем программу и выбираем «Создать» в меню «Файл».
2. Выбираем «Проект» и нажимаем «ОК» → Называем проект <любое название > \_RIP и сценарий No\_Failure → Нажимаем ОК.
3. В диалоговом окне «Мастер запуска: начальная топология» убедимся , что «Создать пустой сценарий» → Нажимаем «Далее» → Выбираем «Campus» в списке «Network Scale» → Далее → ОК.

### **3.3.2 Создание и Конфигурирование сети**

Инициализировать сеть:

1. Диалоговое окно «Object Palette» теперь должно находиться поверх рабочего пространства проекта.
2. Добавляем в рабочую область проекта следующие объекты : один ethernet4\_slip8\_gtwy Маршрутизатор и два объекта (подсети)100BaseT\_LAN.

3. Используем линию связи 100BaseT для соединения добавленных объектов, как показано на рисунке 3.30.

4. Закрываем окно «Object Palette» и сохраним проект.

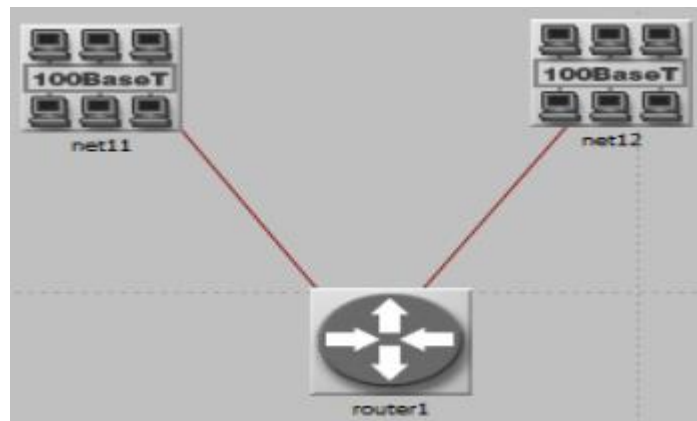


Рисунок 3.30 – Линия связи 100BaseT

### 3.3.3 Конфигурирование маршрутизатора

Для того чтобы конфигурировать маршрутизаторы нужно выполнить следующие шаги:

1. Щелкнем правой кнопкой мыши по маршрутизатору(router) и редактируем свойства или характеристики роутера (Edit Attributes )

А. Экспорт таблицы маршрутизации (рисунок 3.31). Это просит маршрутизатор экспортировать свою таблицу маршрутизации в конце моделирования в журнал моделирования OPNET.

2. Нажимаем «ОК», а затем «Сохранить проект».

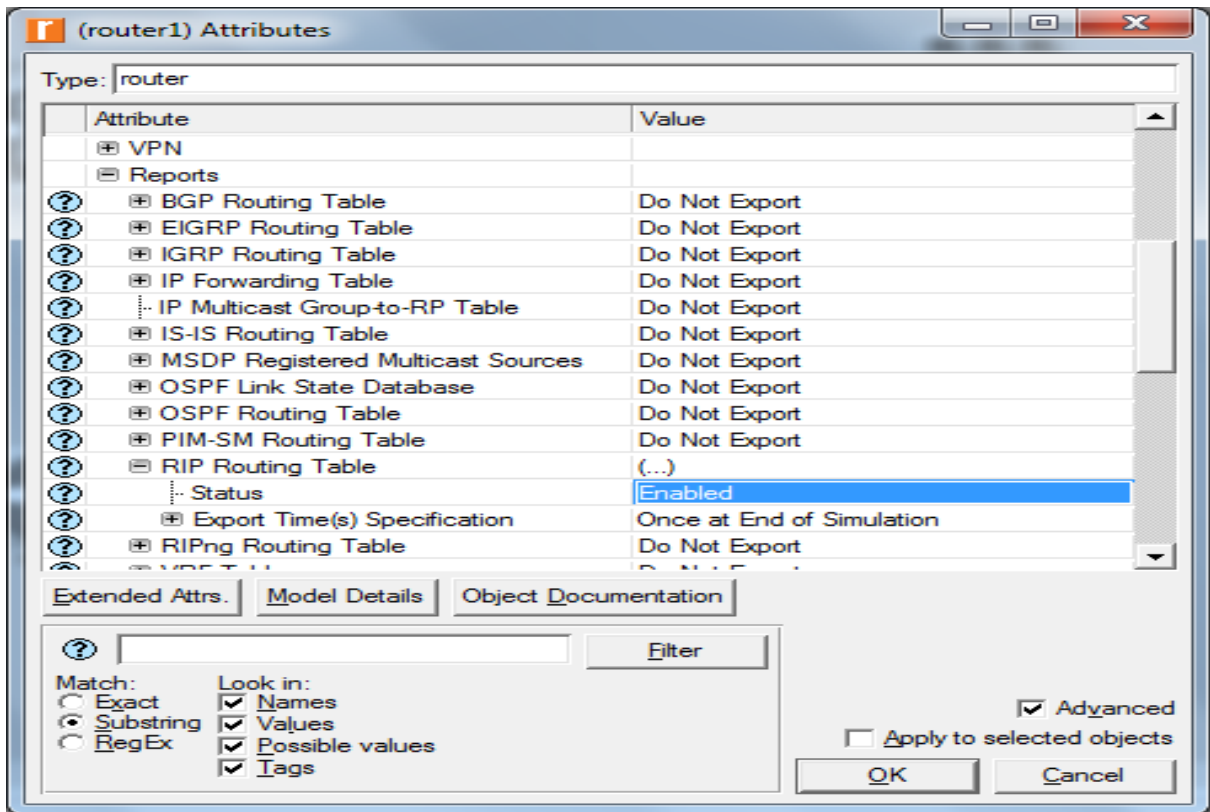


Рисунок 3.31 – Экспорт таблицы маршрутизации

### 3.3.4 Добавление оставшихся локальных сетей

1. Выделяем одновременно (с помощью Ctrl + A) все пять объектов, которые у нас есть в рабочей области проекта (один маршрутизатор, две локальных сетей и две линии связи), скопируем их и вставляем.

2. Расположим объекты так, как это показано на рисунке 3.32.

3. Подключаем маршрутизаторы, как показано, используя PPP\_DS3-линии.

(Канал PPP DS3 имеет скорость передачи данных 44,736 Мбит / с)

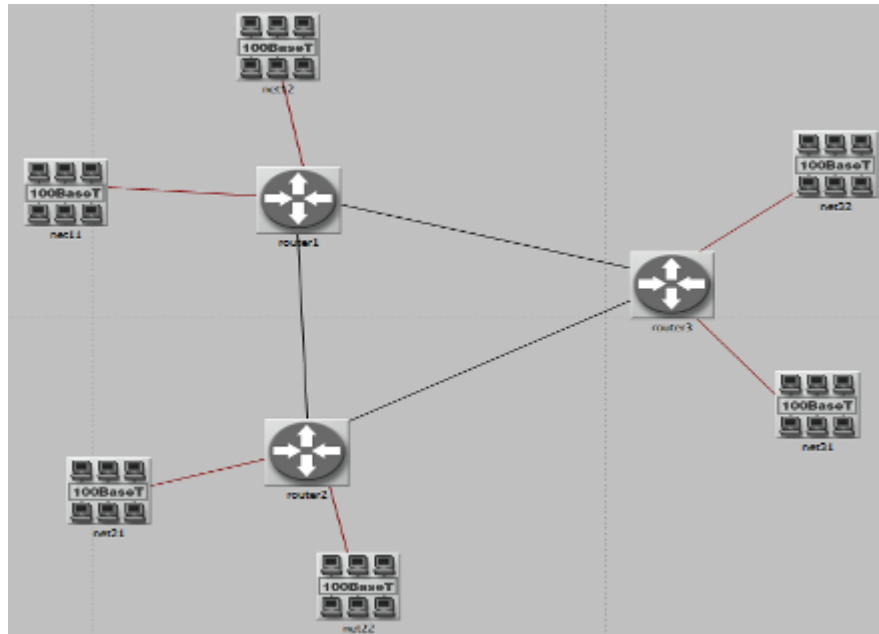


Рисунок 3.32 – Расположение объектов

### 3.3.5 Выбор Статистики

Для тестирования производительности RIP, соберем следующие статистические данные:

1. Щелкаем правой кнопкой мыши в любом месте рабочей области проекта и выберите «Choose Individual Statistics».
2. В окне «Choose Results» проверяем следующие статистические данные:
  - A. Global Statistics → RIP → Traffic Sent (бит / сек).
  - b. Global Statistics · RIP · Traffic Received (bits/sec).
  - c. Nodes Statistics · Route Table · Total Number of Updates
3. Нажимаем кнопку «ОК», а затем «Сохранить проект».

### 3.3.6 Настроить симуляцию

Здесь нужно настроить некоторые параметры моделирования:

1. Нажимаем на Run и появится окно «Настройка моделирования»



2. Установим продолжительность симуляции 10,0 минут.

3. Переходим на вкладку «Global Attributes» и изменяем следующие:

А. Протокол динамической маршрутизации IP = RIP. Это устанавливает протокол RIP в протокол маршрутизации всех маршрутизаторов в сети как показано на рисунке 3.33.

б. IP Interface Addressing Mode = Auto Addressed/Export. То есть ставим режим адресации на автоматически как показано на рисунке ниже (номер рис)

с. RIP Sim Efficiency = Disabled (рисунок 3.34). Это заставляет RIP постоянно обновлять таблицу маршрутизации в случае каких-либо изменений в сети (как мы увидим во втором сценарии).

4. Нажимаем кнопку «ОК» и «Сохранить проект».

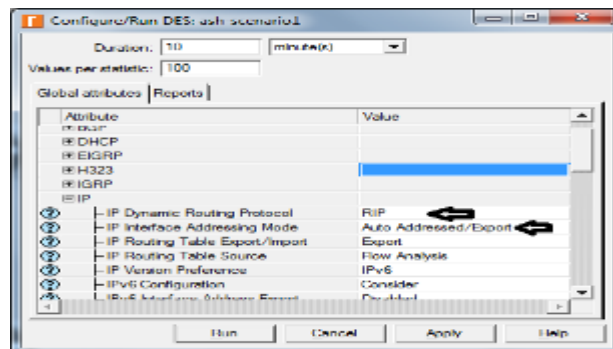


Рисунок 3.33 – Настройка симуляции

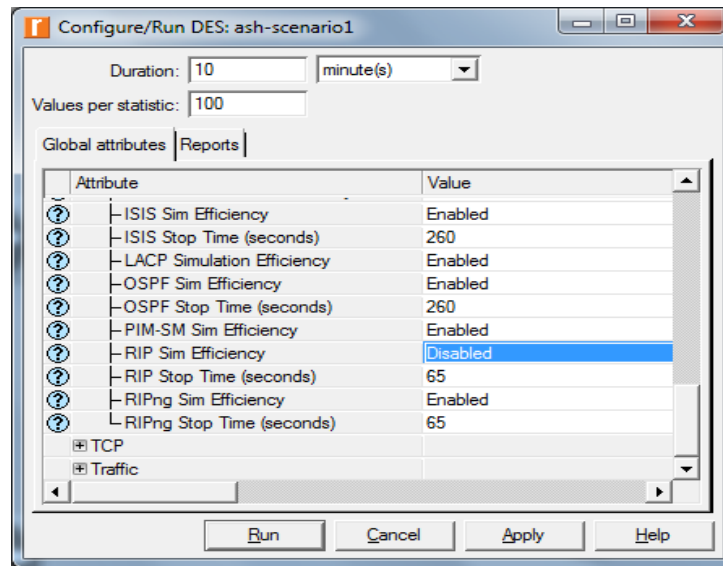


Рисунок 3.34 – Настройка симуляции

### 3.4 Пинг-сценарий

В этом сценарии мы будем использовать модель ping для фиксирования списка перемещаемых узлов, в то время как сообщение ICMP-запроса отправляется адресату, и ICMP-ответ принимается от место назначения.

1. Выбираем «Дубликат сценария» в меню «Сценарии» и назовем его «ICMP\_Ping». → Нажимаем «ОК».

2. Выбираем одновременно маршрутизатор\_1 и маршрутизатор\_3 и выбираем меню «Протоколы» → IP → Demands → Configure Ping Traffic on Selected Nodes.

На выбранных узлах.

3. Меняем характеристику (Pattern attribute) на фиксирования маршрута, как показано на рисунке 3.35 → ОК.

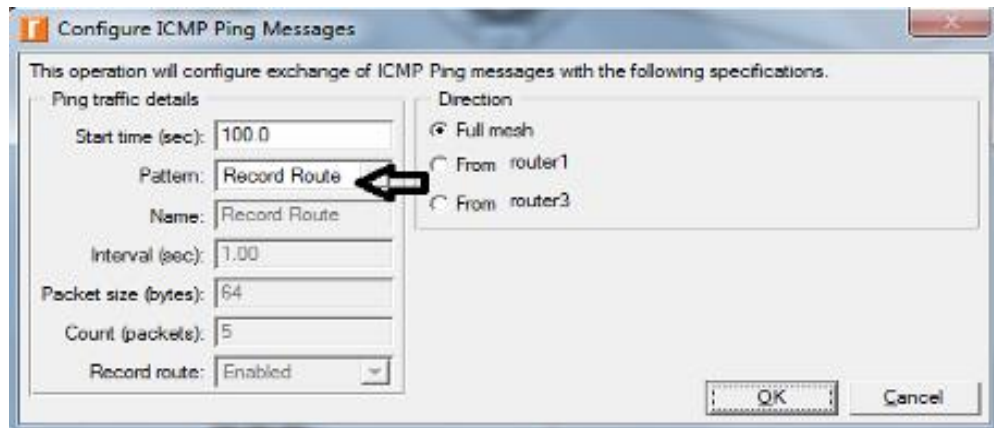


Рисунок 3.35 – Выбор характеристики Pattern attribute

Обратите внимание, что узел Ping Parameter будет добавлен в пространство проекта. Кроме того, требование ping создается между маршрутизатором 1 и маршрутизатором 3 как линия, как на рисунке 3.36.

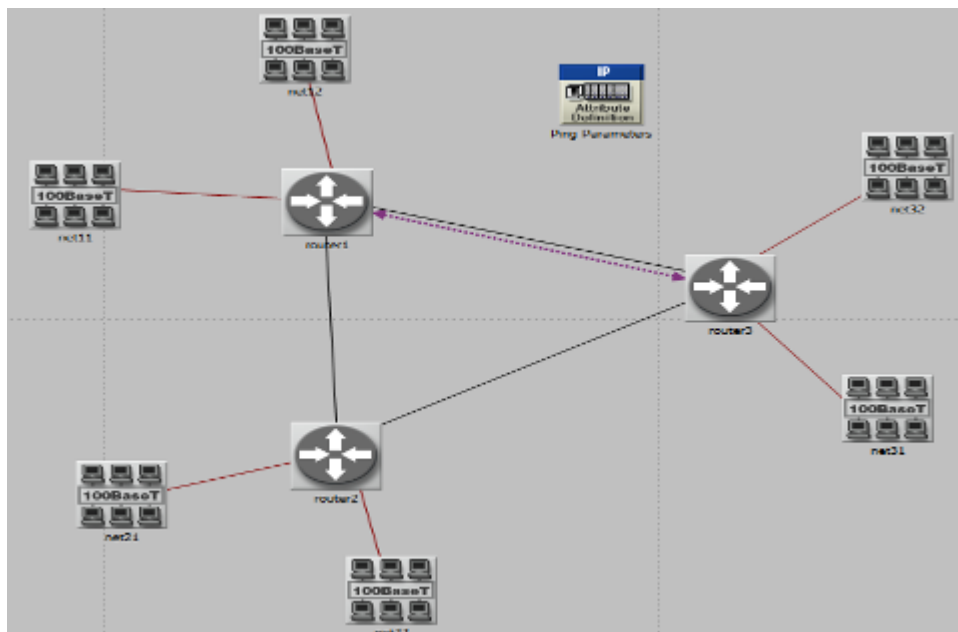


Рисунок 3.36 – Требование ping между маршрутизатором 1 и маршрутизатором 3

### 3.4.1 Сценарий со сбоем в сети

Маршрутизаторы в сети, которые мы делали выше, будут строить свои таблицы маршрутизации без никакой необходимости дальнейшего обновления,

потому что мы не имитировали какие-либо сбой в канале связи. В этом сценарии мы будем моделировать так чтобы был сбой в канале связи для того чтобы мы могли сравнить поведение маршрутизаторов в обоих случаях.

1. Переходим в сценарий No\_Failure и выбираем Duplicate Scenario из меню Scenarios и называем его Failure то есть сбой. Нажимаем ОК.

2. Открываем Object Palette и заходим в Utilities а затем добавляем Failure Recovery то есть восстановление отказа и назовем его просто отказ(Failure) как на рисунке 3.37.

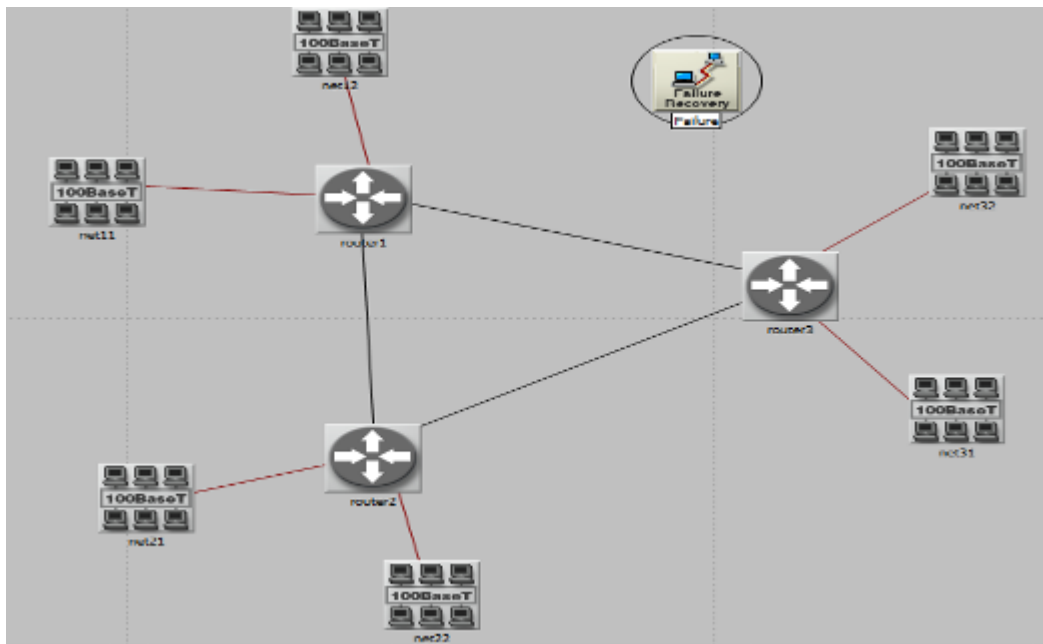


Рисунок 3.37 – Добавления failure

3. Настраиваем объект отказ и ставим данные как на рисунке 3.38:

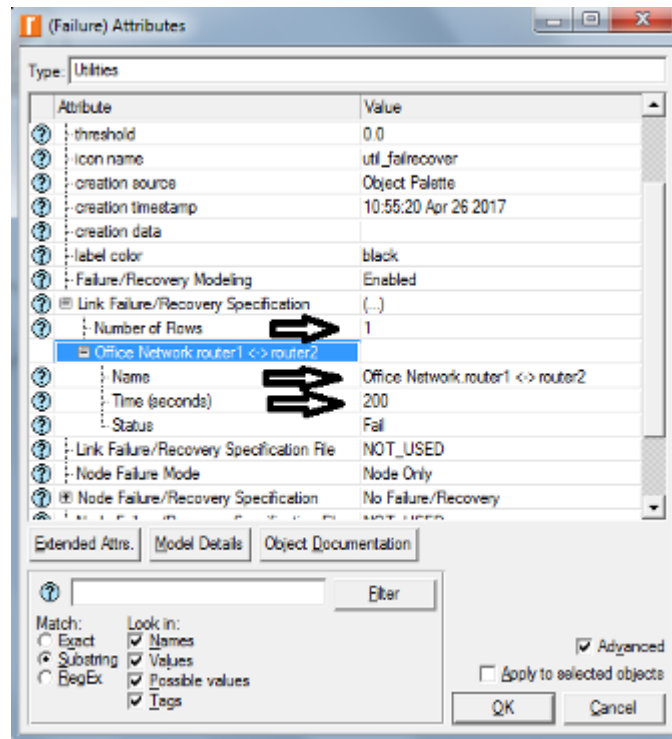


Рисунок 3.38 – Настройка failure

Это приведет к возникновению ошибки в канале связи между первым роутером и вторым через 200 секунд как начнется симуляция.

### 3.4.2 Запуск симуляции

Для одновременного запуска моделирования для обоих сценариев выполняем следующие:

1. Переходим в меню «Сценарии» →· Выбираем «Управление сценариями».
2. Изменяем все значения в столбце Результаты на <collect all> как показано на рисунке 3.39.

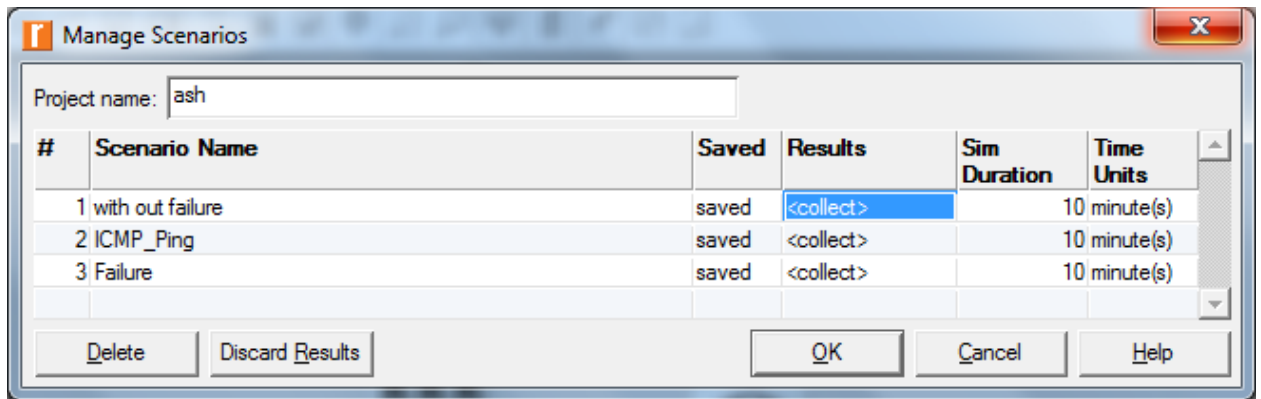


Рисунок 3.39 – Столбец «Результаты»

3. Нажимаем «ОК», чтобы запустить три моделирования.
4. После завершения трех симуляционных прогонов, по одному для каждого сценария, нажмите «Закреть».

### 3.4.3 Просмотр результатов

Теперь будем сравнивать количество обновлений:

для того чтобы сравнить результаты всех сценариев нужно выполнять следующие действия

1. Выбираем сравнить результаты (Compare Results) в меню результатов (Results) а затем выбираем Stacked Statistics как показано на рисунке 3.40.

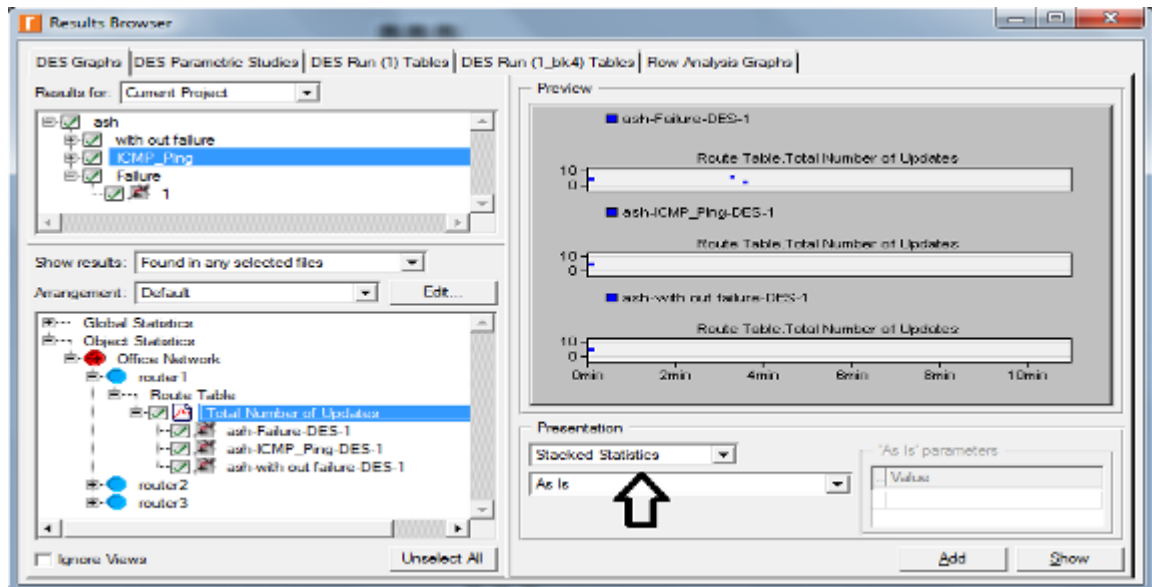


Рисунок 3.40 – Меню результатов

2. Выбираем статистику общего количества обновлений (total number of updates) для 1-ого маршрутизатора и показываем графики со сбоем в канале связи и без сбоя.

3. Должны получиться два графика, по одному для каждого сценария. Щелкаем правой кнопкой мыши по каждому графику и выбираем draw style → bar chart.

Полученные графики должны выглядеть следующим образом (рисунок 3.41).

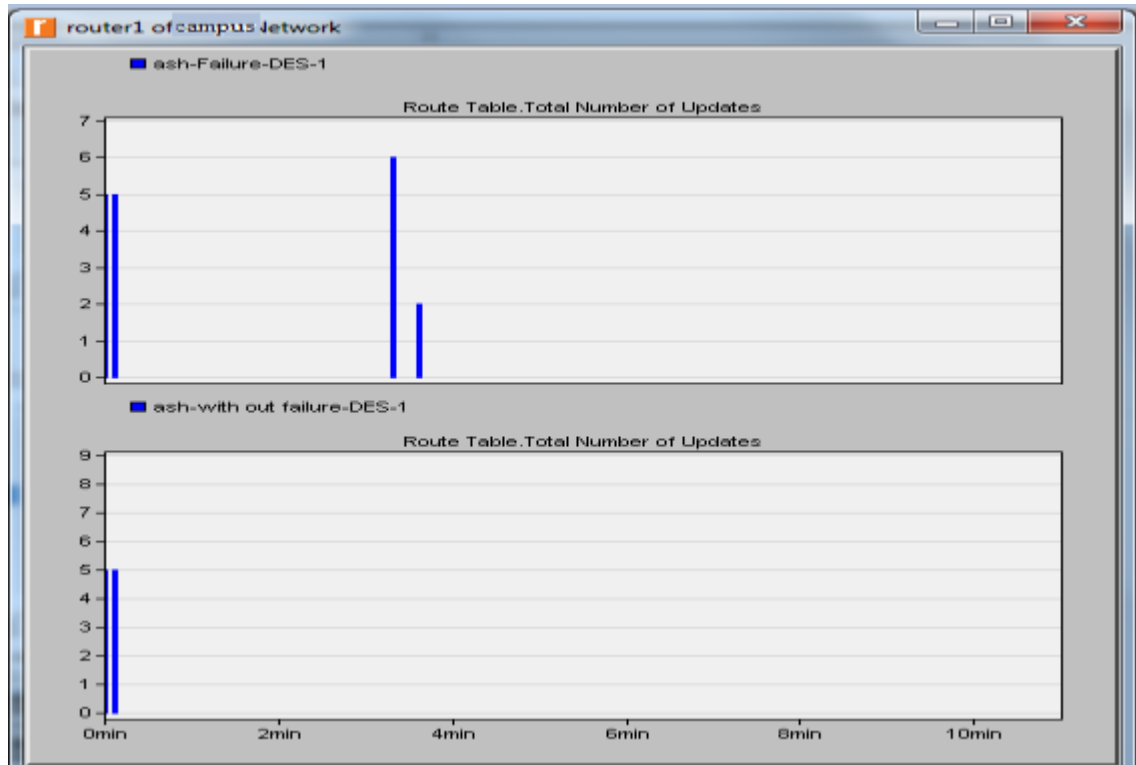


Рисунок 3.41 – Количество обновлений коммутатора

### 3.5 IP-адресация для интерфейса

Перед проверкой содержимого таблиц маршрутизации, необходимо определить информацию об IP-адресе для всех интерфейсов в сети. Напоминаю, что эти IP-адреса присваиваются автоматически во время моделирования, и мы устанавливаем характеристики режима IP адресации интерфейса для экспорта этой информации в файл.

1. Заходим на файл где сохранена вся информация о назначении IP-адреса, как на рисунке 3.42 показано, в нашем случае выбран сценарий, который без сбоя (without failure), так же есть сценарии, которые со сбоем (failure).



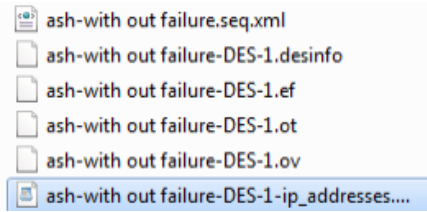


Рисунок 3.42 – Сценарии

2. Ниже приведена часть содержимого файла. Она показывает IP-адреса, назначенные интерфейсам `router_1` в моделируемой сети. Например, интерфейс `router_1`, который подключен к `net_11`, имеет IP-адрес 192.0.0.1. (замечание: результат может изменяться из-за различного расположения узлов). Маска подсети, связанная с этим интерфейсом, указывает, что адрес подсети, к которой подключен интерфейс, – это 192.0.0.0 (то есть «логическое И» IP-адреса интерфейса и маски подсети).

```
Node Name: campus Network.router1 ←
```

Iface Name	IP Address	Subnet Mask	Connected Link
IF0 →	192.0.0.1	255.255.255.0	campus Network.net11 <-> router1 ↓
IF1	192.0.1.1	255.255.255.0	campus Network.router1 <-> net12
IF10	192.0.2.1	255.255.255.0	campus Network.router3 <-> router1
IF11	192.0.3.1	255.255.255.0	campus Network.router1 <-> router2
LB0	192.0.4.1	255.255.255.0	Not connected to any link.

Рисунок 3.43 – Файл с информацией об IP-адресе

На рисунке 3.44 представлена схема сети, которую реализовали в работе.

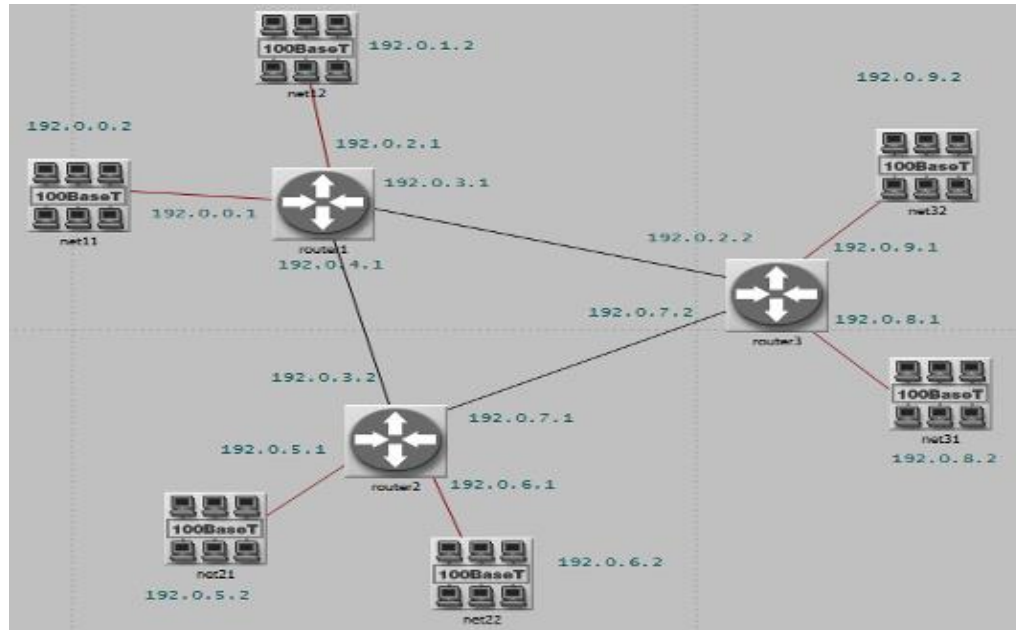


Рисунок 3.44 – Реализованная схема сети

### 3.6 Получение отчета Ping

Чтобы проверить содержимое отчета ping для 1-ого роутера выполняем следующие шаги:

1. Перейдем к сценарию ICMP\_Ping. → Переходим в меню «Результаты». → открываем журнал моделирования → выбираем PING REPORT для сети и получаем отчет, как показано на рисунке 3.45.

	IP Address	Hop Delay	Node Name	MPLS Label	MPLS EXP
1	192.0.2.1	0.000	router1		
2	192.0.8.1	0.000	router3		
3	192.0.2.2	0.000	router3		
4	192.0.2.1	0.000	router1		
5					
6	Total Response Time: 0.000 seconds				

Рисунок 3.45 – Отчет Ping

### 3.7 Сравнение содержимого таблиц маршрутизации

Чтобы проверить содержимое таблиц маршрутизации в 1-ом роутере для сценариев without Failure и Failure нужно делать следующее:

1. Нажимаем на Ctrl + 1, чтобы перейти к сценарию без сбоя (without Failure) → Переходим в меню «Результаты» → Открываем журнал моделирования, затем отрываем таблицу пересылок IP-адресов, как показано на рисунке 3.46.

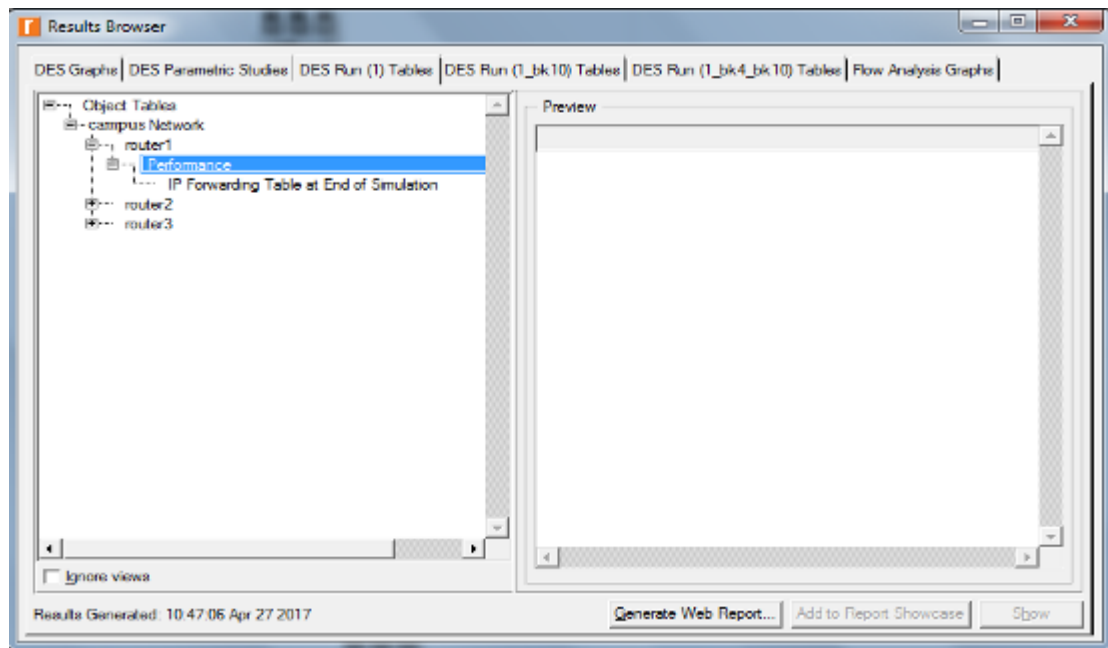


Рисунок 3.46 – Проверка содержимого таблиц маршрутизации

2. Выполняем предыдущий шаг для сценария со сбоем. Ниже приведено частичное содержимое таблиц маршрутизации первого роутера для обоих сценариев (рисунки 3.47 и 3.48).

	Destination	Source Protocol	Route Preference	Metric	Next Hop Address	Next Hop Node	Outgoing Interface	Outgoing LSP	Insertion Time (secs)
1	192.0.0.0/24	Direct	0	0	192.0.0.1	campusNetwork.router1	IF0	N/A	0.000
2	192.0.1.0/24	Direct	0	0	192.0.1.1	campusNetwork.router1	IF1	N/A	0.000
3	192.0.2.0/24	Direct	0	0	192.0.2.1	campusNetwork.router1	IF10	N/A	0.000
4	192.0.3.0/24	Direct	0	0	192.0.3.1	campusNetwork.router1	IF11	N/A	0.000
5	192.0.4.0/24	Direct	0	0	192.0.4.1	campusNetwork.router1	LB0	N/A	0.000
6	192.0.5.0/24	RIP	120	1	192.0.3.2	campusNetwork.router2	IF11	N/A	8.655
7	192.0.6.0/24	RIP	120	1	192.0.3.2	campusNetwork.router2	IF11	N/A	8.655
8	192.0.7.0/24	RIP	120	1	192.0.2.2	campusNetwork.router3	IF10	N/A	6.863
9	192.0.8.0/24	RIP	120	1	192.0.2.2	campusNetwork.router3	IF10	N/A	6.863
10	192.0.9.0/24	RIP	120	1	192.0.2.2	campusNetwork.router3	IF10	N/A	6.863
11									
12	Gateway of last resort is not set								
13									

Рисунок 3.47 – Таблица маршрутизации первого роутера сценарии без сбоя

	Destination	Source Protocol	Route Preference	Metric	Next Hop Address	Next Hop Node	Outgoing Interface	Outgoing LSP	Insertion Time (secs)
1	192.0.0.0/24	Direct	0	0	192.0.0.1	campusNetwork.router1	IF0	N/A	0.000
2	192.0.1.0/24	Direct	0	0	192.0.1.1	campusNetwork.router1	IF1	N/A	0.000
3	192.0.2.0/24	Direct	0	0	192.0.2.1	campusNetwork.router1	IF10	N/A	0.000
4	192.0.4.0/24	Direct	0	0	192.0.4.1	campusNetwork.router1	LB0	N/A	0.000
5	192.0.5.0/24	RIP	120	2	192.0.2.2	campusNetwork.router3	IF10	N/A	216.863
6	192.0.6.0/24	RIP	120	2	192.0.2.2	campusNetwork.router3	IF10	N/A	216.863
7	192.0.7.0/24	RIP	120	1	192.0.2.2	campusNetwork.router3	IF10	N/A	6.863
8	192.0.8.0/24	RIP	120	1	192.0.2.2	campusNetwork.router3	IF10	N/A	6.863
9	192.0.9.0/24	RIP	120	1	192.0.2.2	campusNetwork.router3	IF10	N/A	6.863
10									
11	Gateway of last resort is not set								
12									

Рисунок 3.48 – Таблица маршрутизации первого роутера для сценарии со сбоем

В результате разработаны логические схемы на примере беспроводной кампусной сети университета города Сана и беспроводной телекоммуникационной кампусной сети главного корпуса этого же университета. Собраны имитационные модели в программе OPNET Modeler. Сформированы топологии сети, продемонстрированы работоспособность модели и построены графические зависимости процесса передачи трафика. Также были рассмотрены таблицы маршрутизации и адресация интерфейса.

## ЗАКЛЮЧЕНИЕ

В ходе выполнения диссертационной работы была разработана имитационная модель беспроводной телекоммуникационной кампусной сети в программной среде OPNET Modeler 17.5 для государственного технологического университета города Сана Республики Йемена.

В диссертации решены следующие задачи:

– рассмотрены общие понятия беспроводной сети, классификация беспроводных сетей, а также общие характеристики основных стандартов беспроводных сетей. Выбраны наиболее применимые для построения сети университета: беспроводные локальные сети (WLAN — Wireless Local Area Networks). Технология — Wi-Fi;

– рассмотрены средства имитационного моделирования: OPNET Modeler, NS2, NS3, OMNeT++ и Cisco Packet Tracer. Для разработки имитационной модели корпоративной сети была выбрана программа OPNET Modeler;

– разработаны логические схемы на примере беспроводной кампусной сети университета города Сана и беспроводной телекоммуникационной кампусной сети главного корпуса этого же университета. Собраны имитационные модели в программе OPNET Modeler. Сформированы топологии сети, продемонстрированы работоспособность модели и построены графические зависимости процесса передачи трафика. Также были рассмотрены таблицы маршрутизации и адресация интерфейса.

## СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Григорьев, В.А. Системы и сети радиодоступа [Текст] / В.А. Григорьев, О.И. Лагутенко, Ю.А. Распаев. – Москва: ЭкоТрендз, 2005.
2. Балонин, Н. А., Сергеев М. Б. Беспроводные персональные сети на алгоритмы маршрутизации [Электронный ресурс] / Н. А. Балонин, М. Б. Сергеев. – Режим доступа : <http://citforum.ru/nets/ito/2.shtml> (Дата обращения: 18.05.2016).
3. Методы маршрутизации [Электронный ресурс]. – Режим доступа : <http://sga-informatika.ru/1006012/232-102-routing-methods> (Дата обращения: 20.05.2016).
4. Олифер, В.Г. Компьютерные сети. Принципы, технологии, протоколы : учебник для вузов [Текст] / В.Г. Олифер, Н.А. Олифер. – 4-е изд. – Санкт-Петербург : «Питер», 2014. –944 с.
5. Радке, Хорст Дитер. Wireless Law Easy [Текст] / Хорст Дитер Радке, Йеремиас Радке.– изд-во: НТ Пресс, 2014, 320 с.
6. Семенов, Ю.А. Протоколы и ресурсы Интернет [Текст] / Ю.А. Семенов. – Москва: Радио и связь, 2011. – 320 с.
7. Тарасов, В.Н. Проектирование и моделирование сетей ЭВМ в системе OPNET Modeler [Текст] / В.Н. Тарасов [и др.]. – Самара, 2008.
8. Лоу, А.М. Имитационное моделирование. Классика CS [Текст] / А.М. Лоу, В.Д. Кельтон – 3-е изд. – Санкт-Петербург : Питер; Киев: Издательская группа BHV, 2005. – 847 с.
9. OPNET [Электронный ресурс]. – Режим доступа : <http://www.riverbed.com/products/performance-management-control/opnet.html> (Дата обращения : 20.05.2017).
10. Sommerville, I. Software Engineering, Fourth Edition [Текст] / I. Sommerville. – Addison-Wesley Publishing Company, 1992.

11. Адлер, Ю.П. Статистические методы в имитационном моделировании [Текст] / Ю.П. Адлер. – Москва: Мир, 1990.
12. Калашников, В.В. Организация моделирования сложных систем [Текст] / В.В. Калашников. – Москва : Высшая школа, 1990.
13. Максимей, И. В. Имитационное моделирование на ЭВМ [Текст] / И.В. Максимей. – Москва : Радио и связь, 1988.
14. Павловский, Ю.Н. Имитационные модели и системы [Текст] / Ю.Н. Павловский. – Москва : Высшая школа, 1990.
15. Поляк, Ю.Г., Филимонов В.А. Статистическое машинное моделирование средств связи [Текст] / Ю.Г. Поляк, В.А. Филимонов. – Москва : Радио и связь, 1988.
16. Атре, Ш. Структурный подход к организации баз данных [Текст] / Ш. Атре. – Москва : Финансы и статистика, 1983.
17. Pidd, M. Computer Simulation in Management Science» [Текст] / M. Pidd. – John Wiley & Sons, 1992.
18. Robinson, S. Successful Simulation: A Practical Approach to Simulation Projects [Текст] / S. Robinson. – McGraw-Hill International (UK) Ltd, 1994.