

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	3
1 Теоретически анализ трафика корпоративных мультисервисных сетей	5
1.1 Обзор существующих корпоративных мультисервисных сетей	5
1.2 Основные преимущества корпоративных мультисервисных сетей	12
1.3 Классы и характеристика мультисервисного трафика	13
1.4 История развития средств анализа сетевого трафика	15
1.5 Выводы	25
2 Материалы и методы исследования трафика корпоративной мультисервисной сети.....	27
2.1 Сбор сведений о корпоративной мультисервисной сети	27
2.2 Средства и инструменты исследования трафика	30
2.3 Анализ и классификация сетевого трафика.....	37
2.3 Выводы	47
3 Результаты исследования трафика корпоративной мультисервисной сети.....	48
3.1 Анализ динамики трафика корпоративной мультисервисной сети.....	48
3.2 Прогноз изменения трафика на основе анализа корпоративной мультисервисной сети.....	57
3.3 Разработка рекомендаций по модернизации корпоративной мультисервисной сети.....	59
3.4 Выводы	62

ЗАКЛЮЧЕНИЕ	64
БИБЛИОГРАФИЧЕСКИЙ СПИСОК	66

ВВЕДЕНИЕ

Современные корпоративные сети предоставляют абонентам широкий спектр инфокоммуникационных услуг: передачу файлов, видеосвязь, IP-телефонию, работу с базами данных, просмотр веб-страниц, электронную почту и др., что позволяет сделать вывод о мультисервисной структуре трафика корпоративных сетей.

Мультисервисный трафик в соответствии с [1, 4, 12] имеет самоподобную структуру, а следовательно, задача оценки характеристик качества обслуживания абонентов и определения параметров работы сети не может быть основано на классических моделях систем массового обслуживания в соответствии с классификацией Кендалла-Башарина.

Для анализа и прогнозирования мультисервисного трафика в настоящее время широко используются средства имитационного моделирования и прогнозирования, такие как Opnet Modeller, Network Simulator, OmNet и др.

Таким образом, тема магистерской диссертации является актуальной и позволит на базе имитационного моделирования проводить анализ функционирования корпоративных сетей в широких пределах.

Целью магистерской диссертации является определение параметров функционирования корпоративной сети на основе исследования мультисервисного трафика средствами имитационного моделирования.

Объект исследования - мультисервисная корпоративная сеть.

Предмет исследования - характеристики и параметры трафика корпоративной мультисервисной сети.

Для достижения поставленной цели в магистерской диссертации решены следующие задачи исследования:

- Анализ структуры корпоративных мультисервисных сетей;
- Анализ характеристик и параметров мультисервисного трафика;

- Анализ средств и инструментов оценки параметров трафика корпоративных сетей;
- Имитационное моделирование корпоративной мультисервисной сети;
- Анализ результатов имитационного моделирования;
- Выработка практических рекомендаций по модернизации корпоративной мультисервисной сети на основе анализ трафика.

Структура магистерской диссертации включает введение, три главы и заключение.

1 Теоретически анализ трафика корпоративных мультисервисных сетей

1.1 Обзор существующих корпоративных мультисервисных сетей

В настоящее время, вне зависимости от вида деятельности предприятия, информационно-сетевая инфраструктура является основной инфраструктурой и реализуется посредством корпоративных мультисервисных сетей.

Корпоративная сеть – это совокупность программных и аппаратных компонентов, которые обеспечивают передачу и прием информации между удаленными приложениями и системами предприятия [1]. Корпоративные сети, как правило, не имеют единого центра обработки данных и относятся к классу децентрализованных или распределенных вычислительных сетей.

Корпоративная сеть является сложной системой и включает в себя различные компоненты:

- Персональные компьютеры пользователей корпоративной сети;
- Прикладное и системное программное обеспечение;
- Сетевое и коммутационное оборудование;
- Каналообразующее оборудование (модемы, работающие по волоконно-оптическому или медному кабелю, мультиплексоры, радиорелейные станции, станции широкополосного радиодоступа, станции спутниковой связи и т.д.).

Корпоративные сети могут располагаться в пределах одного города, нескольких городов или области, всего государства, а в крупных компаниях – в пределах континента.

Пример структуры корпоративной сети представлен на рисунке 1.1.

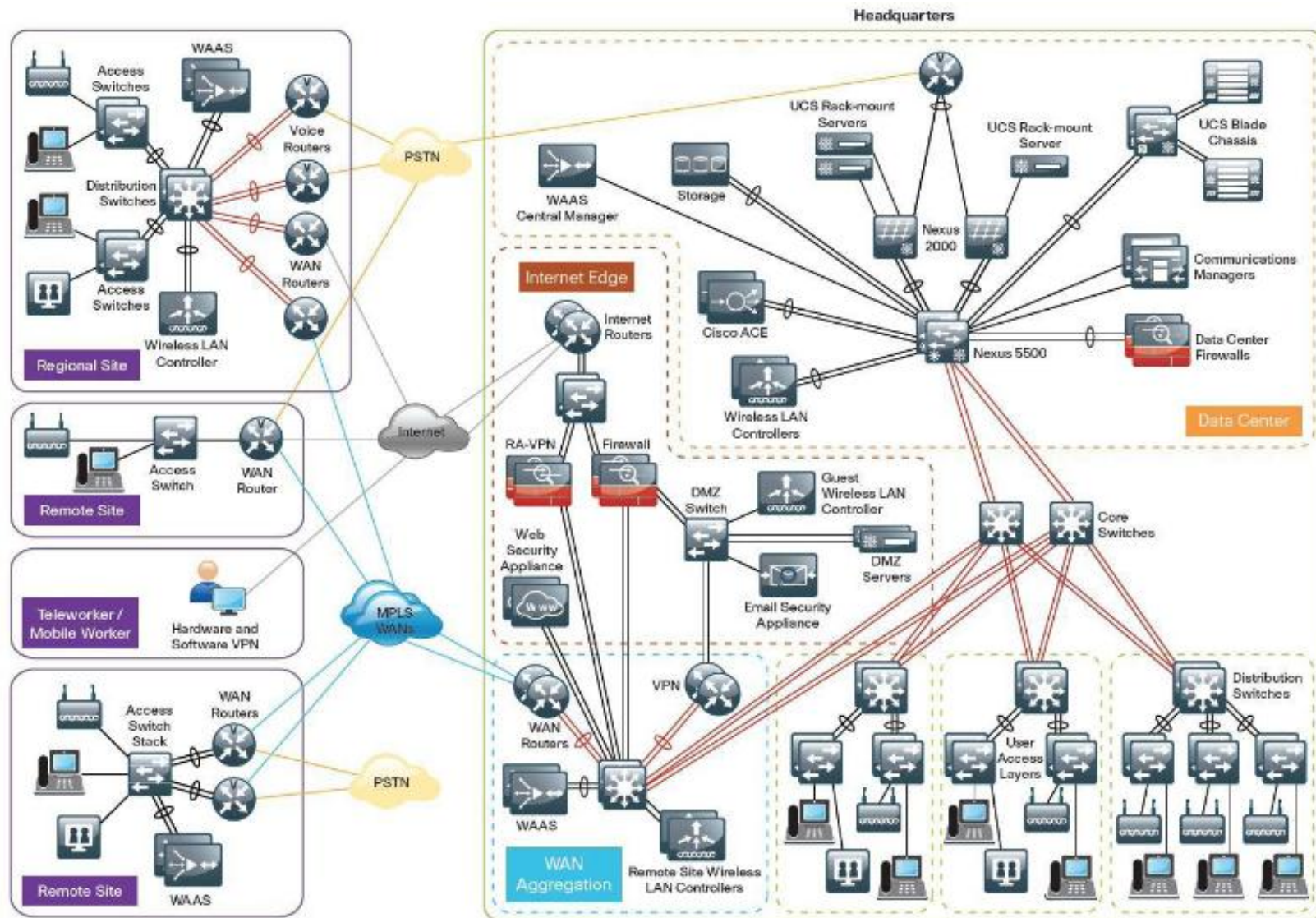


Рисунок 1.2 – Структура корпоративной сети

Корпоративные сети крупных компаний строятся, как правило, в соответствии с принципами построения сети Интернет:

- В сети отсутствует главный сервер, все терминальные устройства в сети являются одноранговыми;
- Основными стеком протоколов является стек TCP/IP;
- В сети используется общее адресное пространство [2].

Однако, корпоративным сетям также присущ основной принцип построения локальных вычислительных сетей: сеть занимает географически ограниченную область [4].

Для обеспечения работы пользователей корпоративной мультисервисной сети, при ее проектировании, должны выполняться следующие требования:

- Расширяемость – возможность относительного простого наращивания структурных элементов сети (терминальных устройств пользователей, телекоммуникационного и сетевого оборудования);
- Масштабируемость – возможность добавления узлов сети и увеличение протяженности соединительных линий без изменения всей архитектуры сети;
- Производительность – обеспечение нахождения основных параметров (скорость цифрового потока, задержка передачи, джиттер) в заданных пределах;
- Надежность – обеспечение бесперебойной работы сетевых элементов, а также безошибочная доставка данных между узлами сети;
- Управляемость – возможность централизованного управления сетью и мониторинга состояния сети;
- Безопасность – обеспечение данных, передаваемых по сети, от несанкционированного доступа.

Авторами в [2] предложен подход анализа корпоративных сетей на основе трехсторонней модели:

- Первая сторона – структурная;
- Вторая сторона – функциональная;
- Третья сторона – системно-техническая.

Рассматривая структурную сторону корпоративных сетей, можно прийти к выводу, что современные корпоративные сети являются совокупностью локальных вычислительных сетей, соединенных по смешанной топологии *иерархическая звезда* (общая топология сети имеет древовидную топологию, а терминальные устройства к коммутаторам подключаются по топологии «звезда») [3].

Анализ функциональной стороны корпоративных сетей показывает, что их главное предназначение – своевременная передача заданных объемов трафика между терминальными устройствами пользователей с целью обеспечения выполнения функций предприятия.

Системно-техническая сторона корпоративных сетей предполагает деление корпоративной сети на уровни (рисунок 1.2).



Рисунок 1.2 – Уровни корпоративной сети

Таким образом, в соответствии с иерархией уровней, корпоративная сеть представляет собой сложную систему, которая предоставляет пользователям услуги и сервисы в соответствии с перечнем задач и функций предприятия.

Анализ физической структуры сети целесообразно проводить, используя *иерархическую модель* корпоративной сети [5], которая включает три уровня:

- Уровень доступа – обеспечивает доступ пользователей к корпоративной сети;
- Уровень распределения – предоставляет доступ пользователей к услугам корпоративной сети;
- Уровень ядра – транспортный уровень, который объединяет уровни распределения в больших корпоративных сетях.

Наличие всех трех уровней в корпоративной сети является необязательным требованием и зависит от масштаба сети и решаемых задач предприятия. Например, для корпоративной сети небольшой организации (до 20 терминальных устройств пользователей) будет реализован только уровень доступа.

Иерархическая модель корпоративной сети представлена на рисунке 1.3.

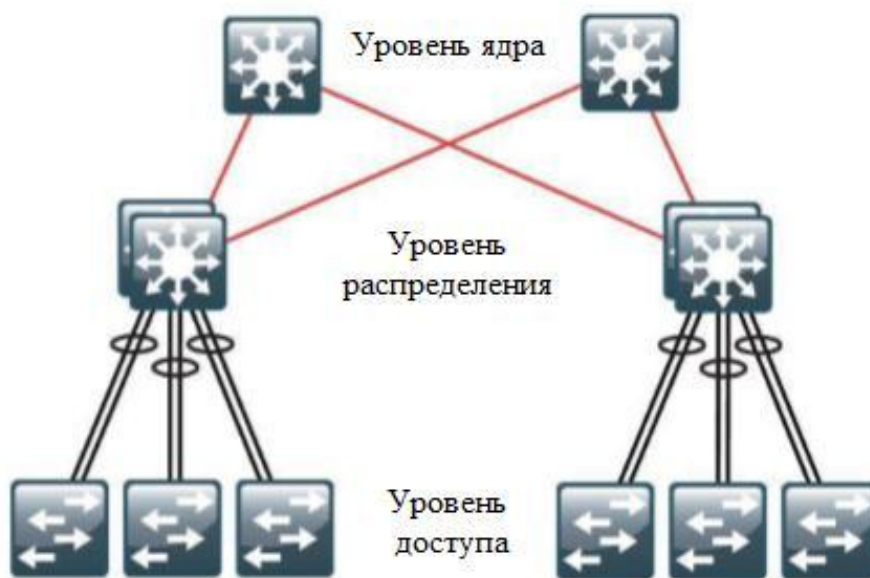


Рисунок 1.3 – Иерархическая модель корпоративной сети

Уровень доступа обеспечивает подключение различных терминальных устройств пользователей (персональных компьютеров, сетевых принтеров и сканеров, IP-телефонов, IP-камер) к корпоративной сети. Доступ может быть, как проводной (по медному или волоконно-оптическому кабелю), так и беспроводной (технологии IEEE 802.11 (WiFi), IEEE 802.16 (WiMAX), LTE). Пример сети на уровне доступа представлен на рисунке 1.4.



Рисунок 1.4 – Уровень доступа корпоративной сети

Главной задачей уровня агрегирования является объединение всех коммутаторов уровня доступа в единую сеть. Наличие уровня распределения позволяет в последующем масштабировать сеть за счет небольшого числа соединительных линий на верхних уровнях сети и обеспечивает более простую систему обслуживания и управления сетью, а также позволяет подключение корпоративной сети к другим сетям, например, к сети Интернет. Уровень распределения корпоративной сети представлен на рисунке 1.5.

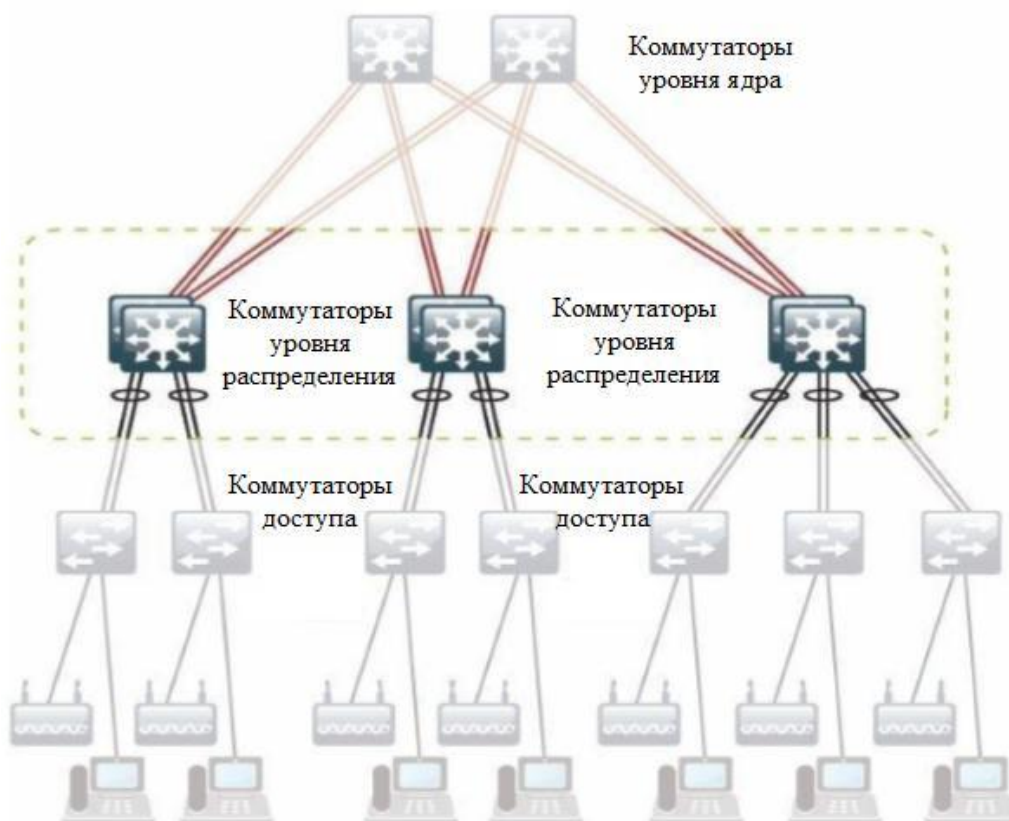


Рисунок 1.5 – Уровень распределения корпоративной сети

Устройства уровня ядра используются при необходимости объединения нескольких зданий предприятия в единую корпоративную сеть и решают задачу агрегирования мультисервисного трафика. Коммутаторы уровня ядра выделены на рисунке 1.6.

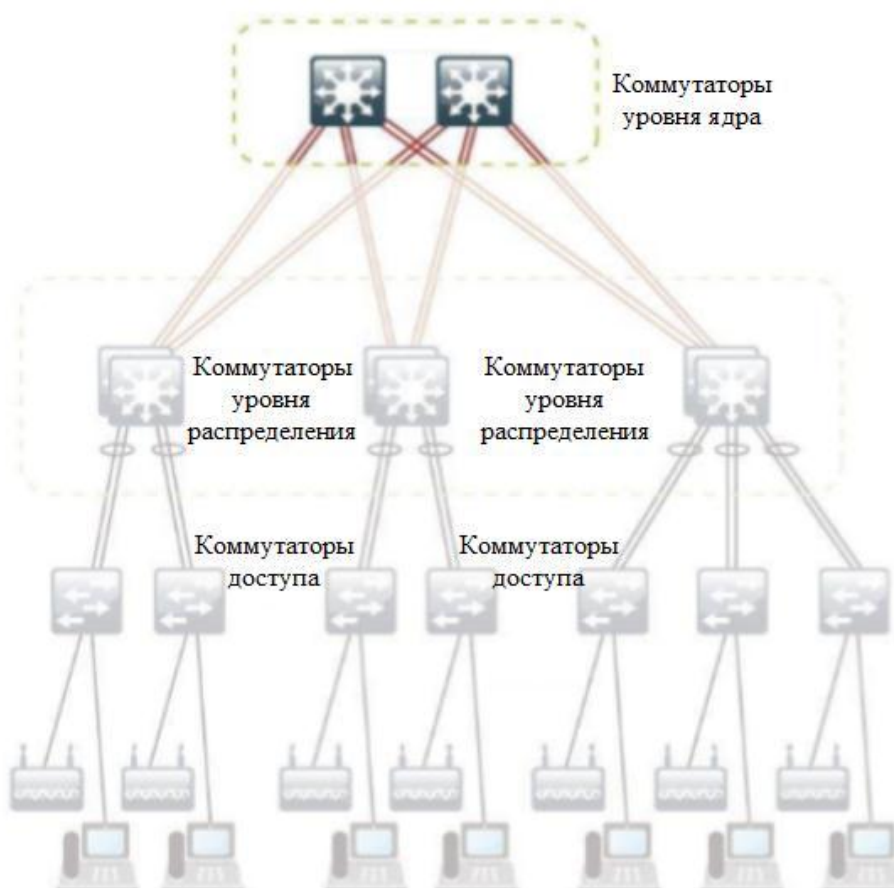


Рисунок 1.6 – Уровень ядра корпоративной сети

Сравнение двух корпоративных сетей без использования и с использованием уровня ядра представлено на рисунках 1.7, 1.8.

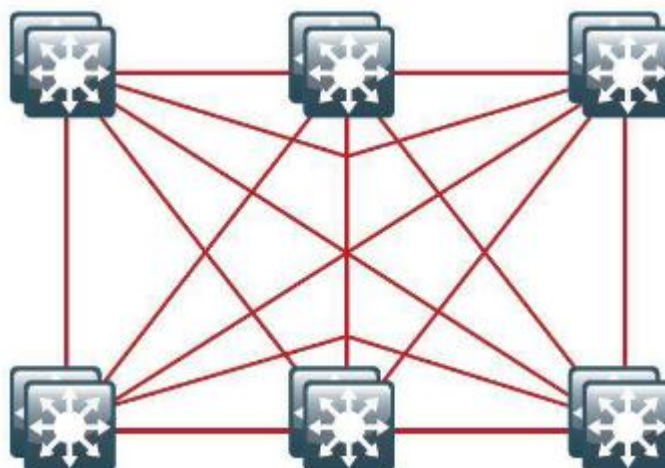


Рисунок 1.7 – Структура корпоративной сети без использование уровня ядра

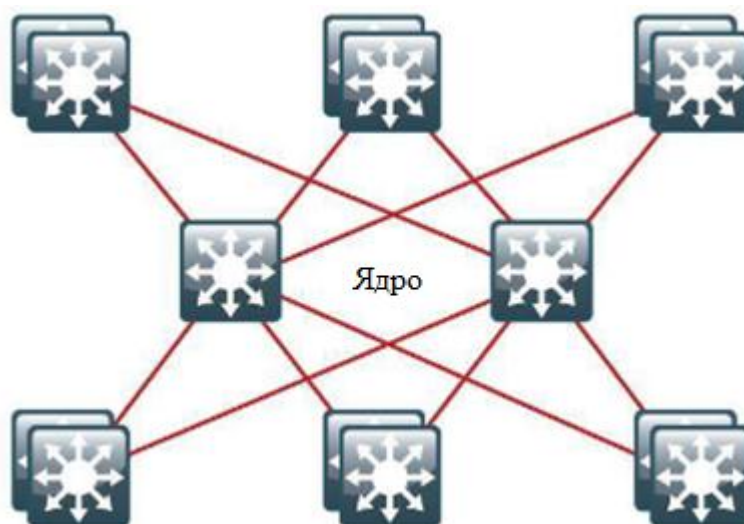


Рисунок 1.8 – Структура корпоративной сети с использованием уровня ядра

Из рисунков 1.7 и 1.8 следует, что наличие уровня ядра сокращает количество соединительных линий между офисами предприятия (коммутаторами уровня распределения).

1.2 Основные преимущества корпоративных мультисервисных сетей

Корпоративная сеть в настоящее время решает широкий спектр производственных задач предприятия, что обеспечивается возможностью передачи различных видов информации: голос, видео, работа сетевых приложений, интернет-коммерция и др.

Основными преимуществами корпоративных мультисервисных сетей являются:

- Быстрый доступ к информационным хранилищам единого информационного пространства предприятия;
- Возможность централизованного управления и анализа состояния производственных и бизнес-процессов предприятия;
- Обмен документами как внутри так и между отделами и службами предприятия;
- Централизованное управление ресурсами сети, контроль за характеристиками качества обслуживания абонентов;

- Разделение ресурсов – данное преимущество позволяет более экономно использовать ресурсы предприятия (например, принтером, подключенным к сети, могут пользоваться многие сотрудники предприятия);
- Разделение программных средств – данное преимущество характеризуется возможностью одновременного и параллельного использования программных средств сотрудниками предприятия.
- Обеспечение пользователей предприятия различными видами услуг.

1.3 Классы и характеристика мультисервисного трафика

Трафик, циркулирующий в пределах корпоративной сети является мультисервисным.

Пользователям корпоративной сети предоставляются следующие виды услуг:

- IP-телефония;
- Видеосвязь, видеоконференции;
- Доступ в сеть Интернет;
- Электронная почта;
- Корпоративные информационные порталы;
- Передача файлов.

В соответствии с рекомендациями МСЭ, характеристиками качества обслуживания являются:

- *Задержка передачи пакета* – время, затраченное на прохождение пакета от отправителя сообщения до получателя сообщения;
- *Вариация задержки передачи пакета (джиттер)* – отклонение максимального и минимального времени прохождения пакета от среднего времени прохождения;
- *Пропускная способность соединительной линии* – максимальная скорость передачи информации по данному каналу связи;

– *Вероятность приема пакета с ошибкой* – отношение количества пакетов, принятых с ошибками, к общему количеству пакетов;

– *Вероятность потери пакета* - отношение количества потерянных пакетов к общему числу пакетов.

Целью разбиения трафика на классы (группы) является обеспечение качества обслуживания пользователей сети.

В соответствии с рекомендацией МСЭ [5], в сетях с пакетной коммутацией различают восемь классов качества обслуживания пользователей. Классы качества обслуживания абонентов представлены в таблице 1.1.

Таблица 1.1 – Классы качества обслуживания

Характеристика	Класс качества обслуживания							
	0	1	2	3	4	5	6	7
Задержка передачи пакета, мс	<100	<400	<100	<400	<1000	-	<100	<400
Джиттер, мс	<50	<50	-	-	-	-	<50	<50
Вероятность приема пакета с ошибкой	$1 \cdot 10^{-3}$	$1 \cdot 10^{-3}$	$1 \cdot 10^{-3}$	$1 \cdot 10^{-3}$	$1 \cdot 10^{-3}$	-	$1 \cdot 10^{-5}$	$1 \cdot 10^{-5}$
Вероятность потери пакета	$1 \cdot 10^{-4}$	$1 \cdot 10^{-4}$	$1 \cdot 10^{-4}$	$1 \cdot 10^{-4}$	$1 \cdot 10^{-4}$	-	$1 \cdot 10^{-6}$	$1 \cdot 10^{-6}$

Услуги, предоставляемые пользователям корпоративной сети, можно распределить по классам качества обслуживания (таблица 1.2).

Таблица 1.2 – Распределение услуг по классам качества обслуживания абонентов

Класс качества обслуживания	Вид услуги	Способы обработки трафика
0	Реального времени, чувствительные к джиттеру, с повышенной степенью взаимодействия (VoIP)	Отдельная очередь с привилегированным уровнем обслуживания
1	Реального времени, чувствительные к джиттеру, интерактивные (VoIP)	
2	Данные транзакций с повышенной степенью интерактивности	Отдельная очередь, пониженный приоритет
3	Данные транзакций, интерактивные приложения	
4	Только с низкими потерями данных	Длинная очередь, пониженный приоритет
5	Традиционные приложения стандартных сетей IP	Отдельная очередь (самый низкий приоритет)

Таким образом, основными характеристиками качества обслуживания по которым классифицируется трафик являются: пропускная способность, задержка передачи пакета, джиттер, вероятность потери пакета и вероятность приема пакета с ошибкой. Исходя из таблицы 1.2, в мультисервисных сетях основной приоритет отдается сервисам реального времени (IP-телефония, видеосвязь и др.).

1.4 История развития средств анализа сетевого трафика

Анализатор трафика (сниффер) – специальное программное обеспечение для перехвата и последующего анализа сетевого трафика.

Анализаторы трафика захватывают пакеты трафика, проходящие через сетевую карту устройства на котором анализатор установлен. То есть терминальное устройство должно быть подключено к концентратору (хабу) либо на коммутаторе (switch) часть портов должны быть зеркальными для дублирования анализируемых пакетов.

История анализаторов трафика берет свое начало из первой половины девяностых годов двадцатого века, когда данное программное обеспечение начало широко использоваться хакерами для перехвата незашифрованной информации для последующего извлечения логинов и паролей к аккаунтам, финансовой и личной информации пользователей. В то время широкое использование концентраторов (доменов коллизии) способствовало незаконному завладению информацией пользователей.

В последующие годы анализаторы трафика начали активно использоваться в целях диагностики и решения ряда проблемных вопросов в мультисервисной сети:

- Обнаружение паразитного, вирусного, закольцованного трафика, который снижает эффективную пропускную способность на участках мультисервисной сети;
- Специализированные анализаторы трафика (*мониторы сетевой активности*) позволяют определять сетевые сканеры, троянские программы, флудеры, пиринговые клиенты и др.;

- Системные администраторы используют анализаторы трафика для локализации неисправности сетевых элементов, некорректной работы протоколов маршрутизации и др.;
- Инженерно-технический состав может использовать анализаторы трафика для оценки работоспособности сети и анализа характеристик качества обслуживания абонентов, для последующей модернизации сети или устранения ошибок ее проектирования;
- Восстановление данных (сбор пакетов, их сортировка и их реинкапсуляция в соответствии с уровнями модели взаимодействия открытых систем).

Наиболее популярными решениями в области анализа сетевого трафика являются свободно распространяемые и коммерческие программные продукты:

- Wireshark;
- Bro Network Security Monitor;
- Snort;
- Colasoft Capsa;
- ClearSight Analyzer.

Рассмотрим историю появления, основные возможности и архитектуру данных программных продуктов.

Анализатор трафика Wireshark.

Wireshark – это свободно распространяемый анализатор трафика, который поддерживает большое количество сетевых протоколов, фильтрацию, восстановление пакетов, анализ статистики. Первый выпуск программного продукта появился в 1998 году.

Интерфейс программы Wireshark представлен на рисунке 1.9.

Разработчиком программы является компания «The Wireshark Team». Программа распространяется по лицензии General Public License. Программа Wireshark разработана для операционных систем семейства Unix (Apple Mac OS, FreeBSD), Linux, Windows.

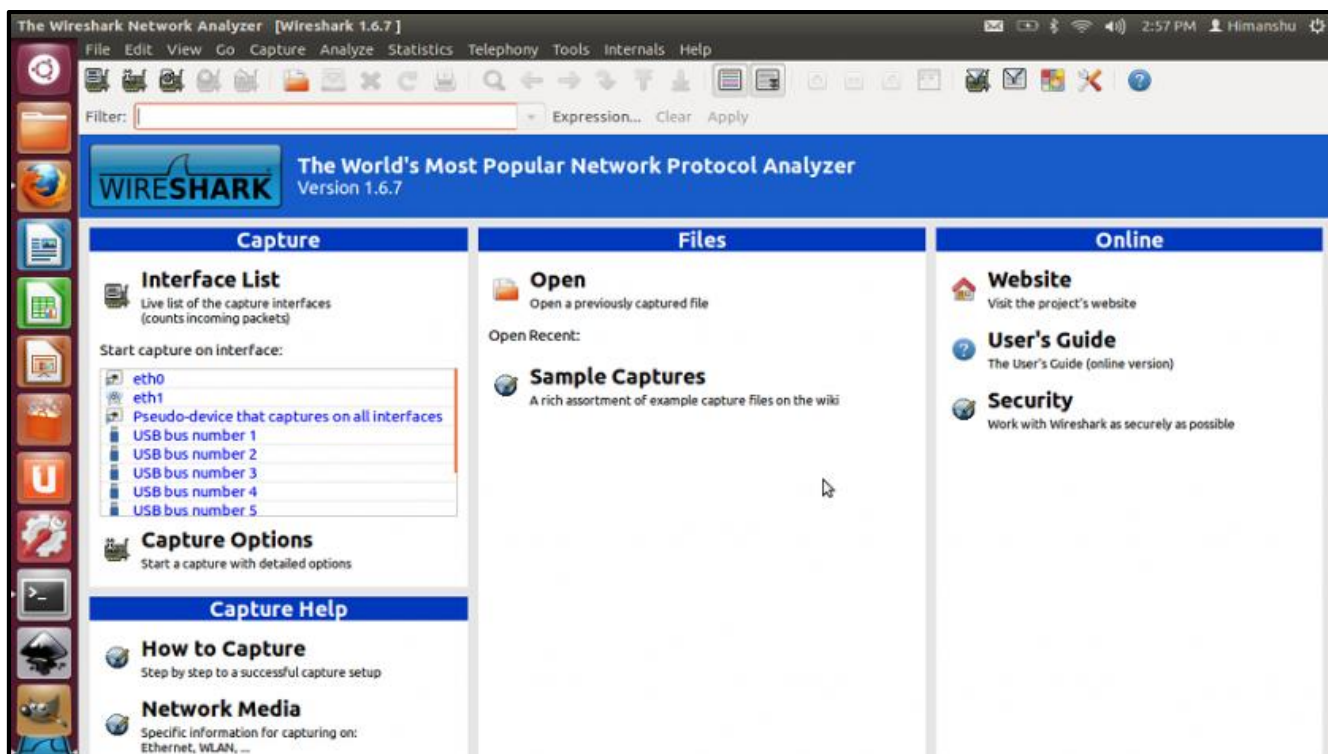


Рисунок 1.9 – Интерфейс анализатора трафика Wireshark

Программа Wireshark написана на языке C с использованием библиотеки libpcap (WinPcap). Программа Wireshark позволяет работать как с проводными так и с беспроводными адаптерами.

Архитектура программы Wireshark представлена на рисунке 1.10 [6].

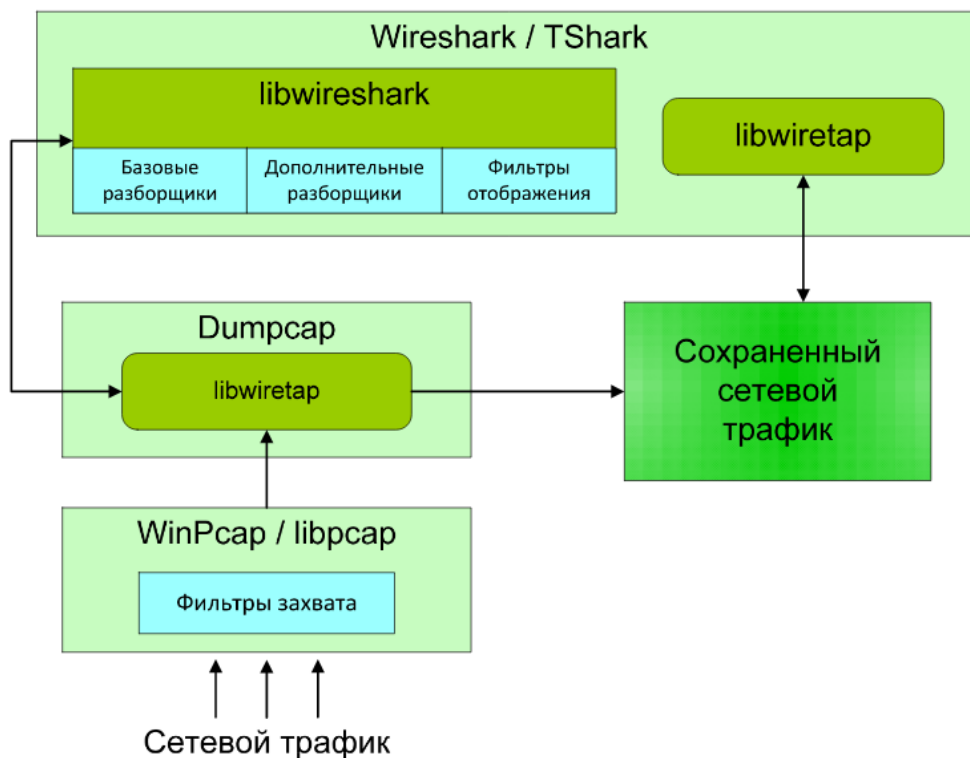


Рисунок 1.10 – Архитектура анализатора трафика Wireshark

Программа состоит из двух модулей:

- Библиотека, которая реализует процесс захвата сетевого трафика;
- Прикладное программное обеспечение, позволяющее производить фильтрацию пакетов по протоколам, графическое представление результатов анализа сетевого трафика, взаимодействие с операционной системой.

Библиотека `libpcap` (WinPcap) осуществляет взаимодействие с драйвером сетевой карты устройства. Программный модуль `Dumpcap` обеспечивает запись перехваченных пакетов в файл. Библиотека `libwireshark` реализует функции анализа перехваченного трафика, и визуализацию результатов.

Достоинства анализатора трафика Wireshark:

- Поддержка большинства современных протоколов различных стеков модели взаимодействия открытых систем;
- Возможность установки дополнительных программных модулей для определенных сетевых протоколов;
- Многокритериальная фильтрация пакетов сетевого трафика;
- Возможность восстановления сессии по протоколу TCP.

Недостатки анализатора трафика Wireshark:

- Поток пакетов, восстановленный программой, не является единым буфером памяти, а, следовательно, последующая обработка потоков является невозможной;
- Код программного модуля анализа трафика частично реализует функции визуализации результатов, что не позволяет логически разделить процессы анализа трафика и визуализации результатов.

Выявленные недостатки не позволяют применять программу Wireshark в сетях с многоуровневыми туннелями, а также не позволяют осуществлять эффективную работу с восстановленными потоками.

Анализатор трафика Bro Network Security Monitor (Bro).

История анализатора трафика Bro начинается с 1994 года. Разработана первая версия программы Верном Паксоном. Программа Bro позволяет проводить анализ

сетевого трафика в режиме реального. Анализатор разработан под операционные системы семейства Unix (Linux, FreeBSD, Mac OS). Интерфейс программы представлен на рисунке 1.11.

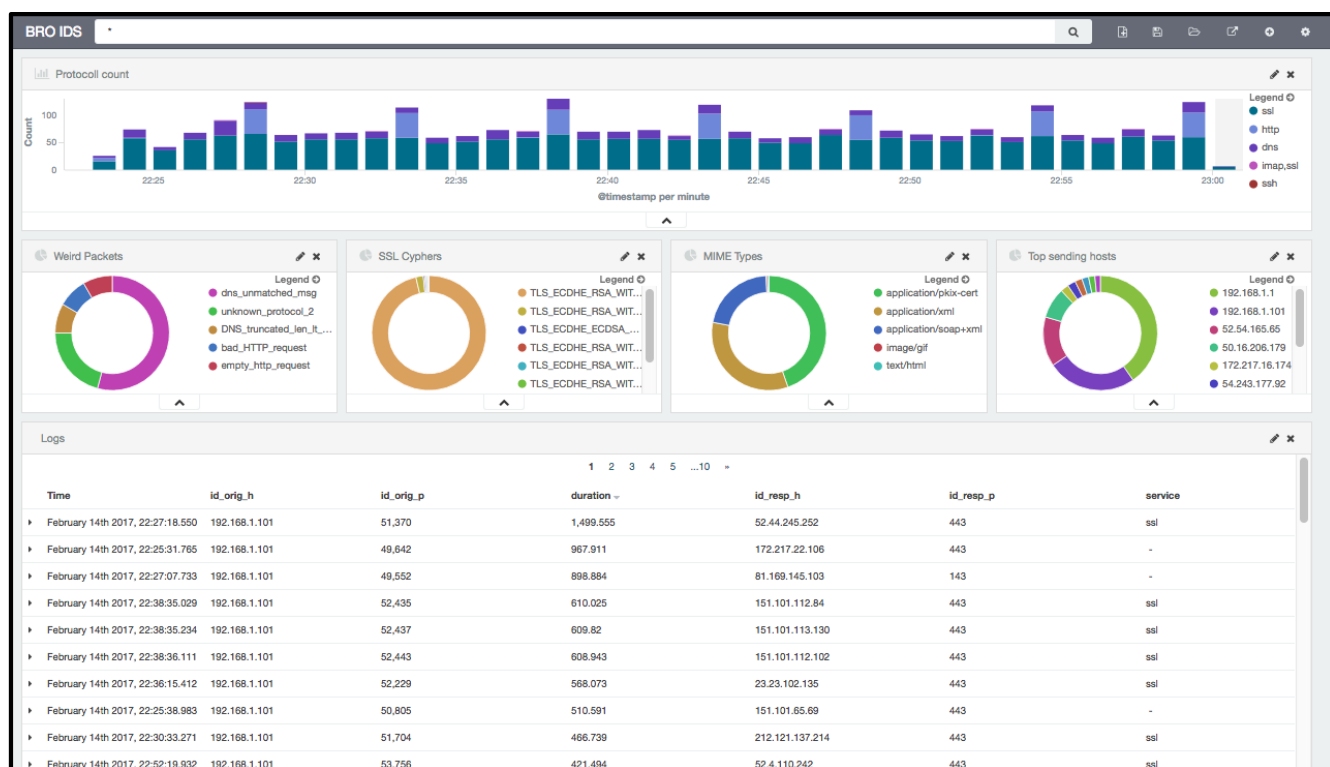


Рисунок 1.11 – Интерфейс анализатора трафика Bro Network Security Monitor

Архитектура программы представлена на рисунке 1.12.



Рисунок 1.12 – Архитектура анализатора трафика Bro Network Security Monitor

Архитектура анализатора трафика Bro состоит из двух программных модулей:

- Генератор событий (реализует функции анализа сетевого трафика и генерации событий);
- Обработчики событий (при помощи реализованного в программном продукте скриптового языка возможно проводить логирование процессов и событий, формировать предупреждения, а также осуществлять запуск других приложений при наступлении определенных событий указанных администраторам сети).

При помощи анализатора Bro можно анализировать трафик как в режиме реального времени, так и проводить отложенный анализ файлов с расширением .pcap.

Вместе с программным продуктом поставляется набор готовых скриптов под различные задачи. В скриптах условия по которому наступает действие может применяться как к заголовку пакета так и к его телу, что значительно расширяет круг решаемых задач данным анализатором трафика.

Программа Bro позволяет анализировать трафик в виртуальных частных сетях, однако, количество туннельных протоколов, реализованных для анализа в данной программе не велико.

Анализатор трафика Snort.

В основу логики работы анализатора трафика Snort положен метод сигнатурного поиска [8]. Разработчиком данного программного продукта является компания Sourcefire. Анализатор разработан для операционных систем семейства Linux, Windows, FreeBSD, Mac OS.

Анализатор трафика Snort поддерживает два режима работы:

- Анализ сетевого трафика в режиме реального времени;
- Анализ сохраненных в памяти сетевых трасс.

Анализ сетевого трафика в режиме реального времени обеспечивает вывод в консольное окно содержимого перехваченных пакетов, логирование (регистрация пакетов и их сохранение, анализ статистики сетевого трафика).

Интерфейс анализатора Snort представлен на рисунке 1.13.

The screenshot shows the 'Services / Snort / Alerts' interface. At the top, there are tabs for 'Snort Interfaces', 'Global Settings', 'Updates', 'Alerts' (selected), 'Blocked', 'Pass Lists', 'Suppress', 'IP Lists', 'SID Mgmt', 'Log Mgmt', and 'Sync'. Below the tabs is a 'Clear all interface log files' button. The 'Alert Log View Settings' section includes a dropdown for 'Interface to Inspect' (set to 'WAN'), an 'Auto-refresh view' checkbox, a text input for 'Alert lines to display' (set to '1000'), and a 'Save' button. Below this is an 'Alert Log Actions' section with 'Download' and 'Clear' buttons. The 'Alert Log View Filter' section is empty. The 'Last 1000 Alert Log Entries' section contains a table with the following data:

Date	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	SID	Description
2017-07-23 20:49:52	1	UDP	A Network Trojan was Detected	66.240.205.34	1066		16464	1:31136	MALWARE-CNC Win.Trojan.ZeroAccess inbound connection
2017-07-22 06:15:49	2	UDP	Potentially Bad Traffic	163.172.17.76	54465		5060	140:26	(spp_sip) Method is unknown
2017-07-21 09:26:30	2	UDP	Potentially Bad Traffic	163.172.22.169	52428		5060	140:26	(spp_sip) Method is unknown
2017-07-21 01:03:28	2	UDP	Potentially Bad Traffic	163.172.17.76	46834		5060	140:26	(spp_sip) Method is unknown
2017-07-20 20:36:37	2	UDP	Potentially Bad Traffic	163.172.22.169	54788		5060	140:26	(spp_sip) Method is unknown
2017-07-20 08:31:30	2	UDP	Potentially Bad Traffic	163.172.17.76	59571		5060	140:26	(spp_sip) Method is unknown

Рисунок 1.13 – Интерфейс анализатора трафика Snort

Архитектура программы представлена на рисунке 1.14.

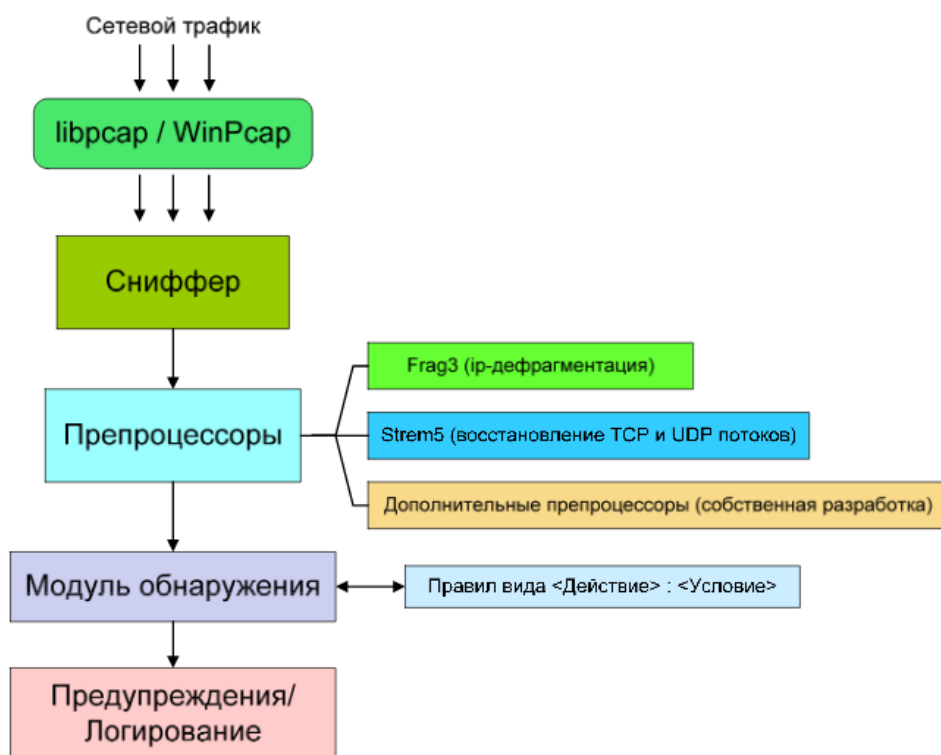


Рисунок 1.14 – Архитектура анализатора трафика Snort

Основным отличием архитектуры анализатора трафика Snort является наличие двух основных компонентов: процессоров и модуля обнаружения. Задача процессоров состоит в разборе различных сетевых протоколов. В программу можно добавлять пользовательские процессоры. Модуль обнаружения определяет заданные пользователем шаблоны событий и выполняет заданные действия при их обнаружении. Модуль обнаружения работает в соответствии с правилами, которые включают заголовки и опции.

Анализатор трафика Colasoft Capsa.

Данный анализатор трафика предназначен для диагностики работоспособности сети. Разработчиком Colasoft Capsa является Colasoft. Colasoft Capsa распространяется по лицензии, однако существует бесплатная ограниченная версия программы. Анализатор разработан для семейства операционных систем Windows и работает как с проводными, так и с беспроводными сетевыми картами.

Интерфейс анализатора Colasoft Capsa представлен на рисунке 1.15.



Рисунок 1.15 – Интерфейс анализатора трафика Colasoft Capsa

Архитектура программы представлена на рисунке 1.16. Логически программа состоит из нескольких модулей. Модуль перехвата данных

взаимодействует с сетевым драйвером и передает перехваченные пакеты анализатору для разбора содержимого пакетов в режиме реального времени.

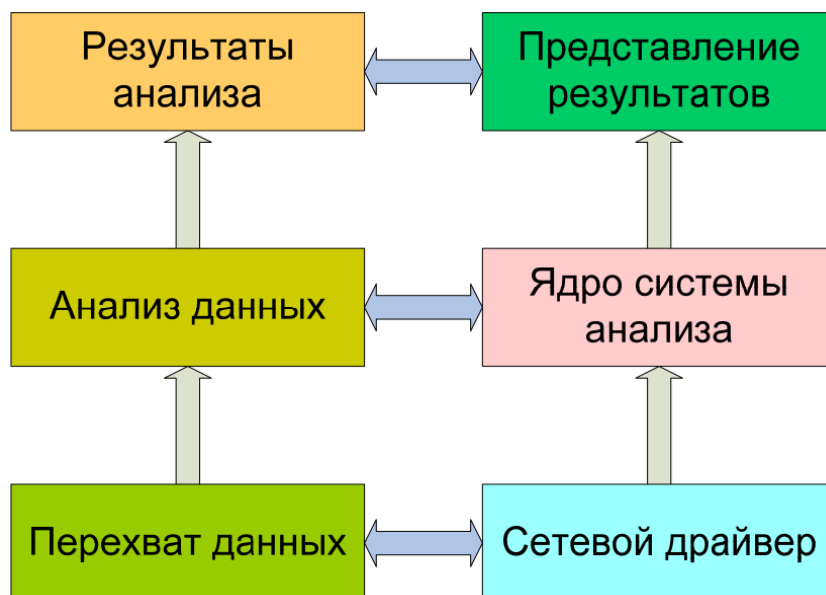


Рисунок 1.16 – Архитектура анализатора трафика Colasoft Capsa

Процесс анализа трафика анализатором Colasoft Capsa представлен на рисунке 1.17.

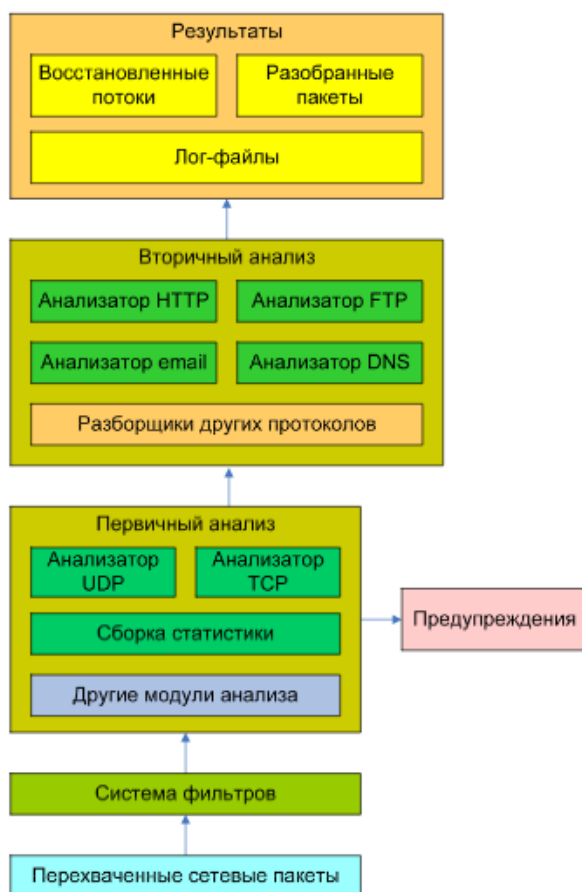


Рисунок 1.17 – Процесс анализа трафика в программе Colasoft Capsa

Перехваченные пакеты анализатором трафика проходят систему пользовательских фильтров и поступают на программный блок первичного анализа, который проводит разбор кадров и пакетов на канальном, сетевом и транспортном уровнях модели взаимодействия открытых систем.

Вторичный анализ обеспечивает разбор пакетов на прикладном уровне семиуровневой модели. Анализатор трафика поддерживает более трехсот протоколов прикладного уровня.

Главной особенностью и одновременно достоинством анализатора трафика Colasoft Capsa является многопоточность.

Анализатор трафика ClearSight Analyzer.

Анализатор трафика ClearSight Analyzer является программно-аппаратным модулем комплекса Network Time Machine, архитектура которого представлена на рисунке 1.18.

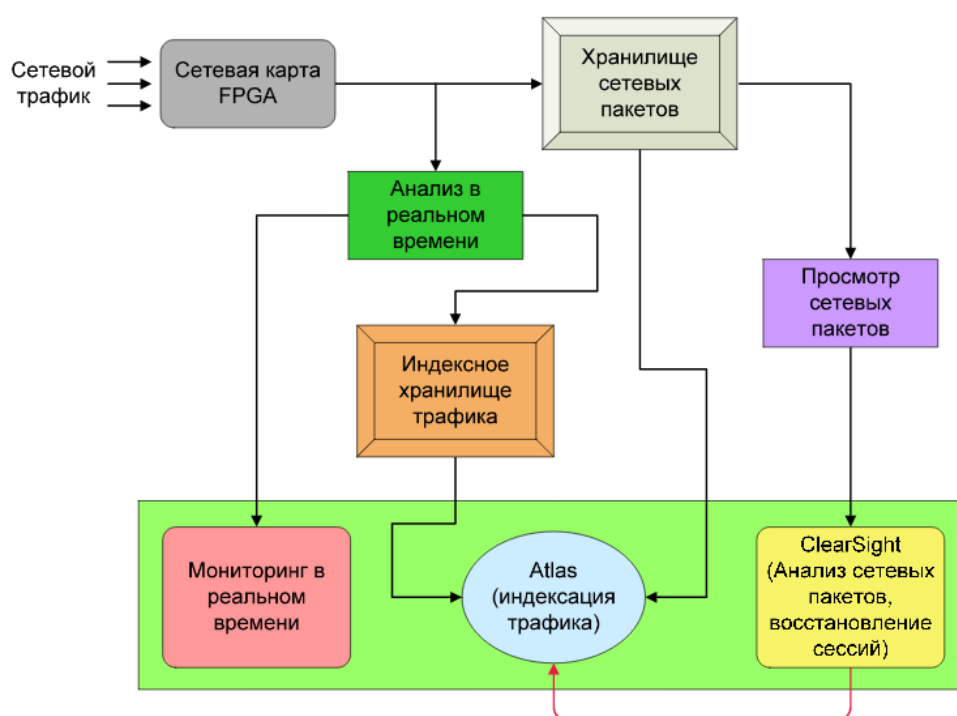


Рисунок 1.18 – Архитектура Network Time Machine

Исследуемый трафик поступает на сетевую карту FPGA программно-аппаратного комплекса и далее может анализироваться либо в режиме реального времени, либо поступать в хранилище сетевых пакетов (область долговременной памяти на жестком диске). При анализе в режиме реального времени может

проводится индексация трафика по различным характеристикам при помощи программного модуля Atlas. За счет программно-аппаратной реализации комплекса повышается анализ трафика в режиме реального времени на высокоскоростных каналах связи (до 20 Гбит/с). Интерфейс программы представлен на рисунке 1.19.

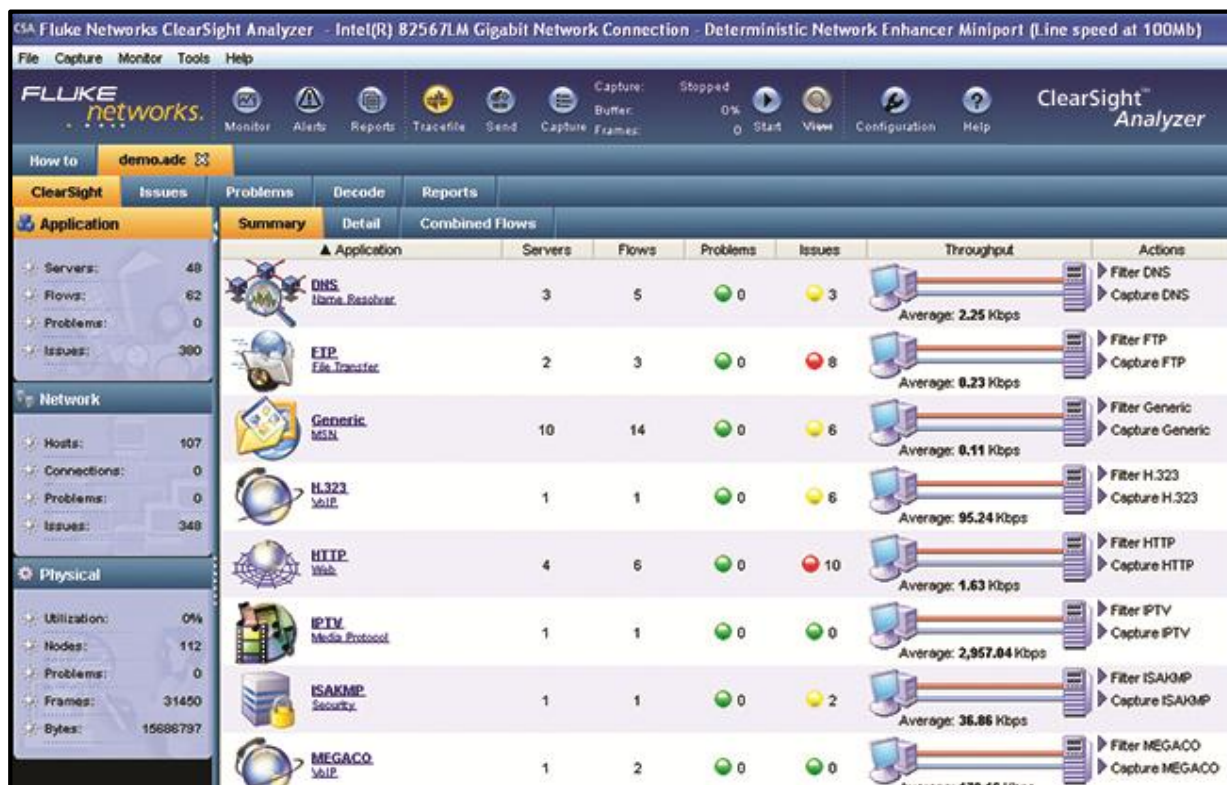


Рисунок 1.19 – Интерфейс программы ClearSight Analyzer

Таким образом, анализаторы трафика разных производителей решают схожий круг задач и имеют несущественные отличия. Весь перечень проанализированных программных продуктов можно разделить на две группы: анализаторы трафика используемые в небольших сетях и анализаторы трафика больших телекоммуникационных сетей. Для корпоративных сетей наиболее подойдут анализаторы для небольших сетей, например, WireShark.

1.5 Выводы

1. Современные корпоративные сети имеют трехуровневую архитектуру и строятся на базе стека протоколов TCP/IP.
2. Трафик корпоративных сетей является мультисервисным и в соответствии с принципом конвергенции формируется на выходе большого

количества терминального оборудования пользователей (как старого так и нового поколения, подключенного через систему IP-шлюзов).

3. Основными характеристиками качества обслуживания абонентов являются: пропускная способность, задержка передачи пакетов, джиттер, вероятность потери пакетов и вероятность приема пакета с ошибкой. Классы трафика в соответствии с рекомендациями МСЭ определяются системой данных характеристик. Основной приоритет при обработке мультисервисного трафика отдается сервисам реального времени (видеосвязь, IP-телефония и др.).

4. Средства анализа трафика достаточно широко представлены на рынке программного обеспечения и решают задачи: сбора, анализа, восстановления, хранения трафика, а также выполнение действий при наступлении определенных сетевых событий.

2 Материалы и методы исследования трафика корпоративной мультисервисной сети

2.1 Сбор сведений о корпоративной мультисервисной сети

Для анализа трафика корпоративной мультисервисной сети рассмотрена реальная корпоративная сеть предприятия ОАО «Стройинвест Групп». Предприятие «Стройинвест Групп» осуществляет проектирование и строительство промышленных объектов, складских комплексов и помещений, административных, офисных и развлекательных зданий, оздоровительных комплексов и специализированных лабораторий.

Также рассматриваемая компания оказывает услуги по проведению строительных экспертиз конструкций и инженерных систем.

Штат компании составляет 580 человек. Офисы предприятия располагаются в трех административных зданиях, которые располагаются на расстоянии трех километров друг от друга.

Корпоративная мультисервисная сеть предприятия строится на базе технологии SHDSL и состоит из:

- 520 рабочих станций пользователей;
- Структурированную кабельную систему на основе кабеля витая пара;
- Десять коммутаторов второго уровня модели OSI;
- Один маршрутизатор;
- Четыре сервера (сервер баз данных, сервер электронной почты, файловый сервер, сервер IP-телефонии);
- Оборудование видеонаблюдения.

Связь между офисами организуется при помощи SHDSL-модемов. При помощи ADSL-модема осуществляется доступ в сеть Интернет. Для повышения безопасности информации используется услуга VPN-сервиса на стороне провайдера.

Структура мультисервисной сети организации и схематичное расположение сетевых элементов на плане здания представлено на рисунках 2.1-2.3.

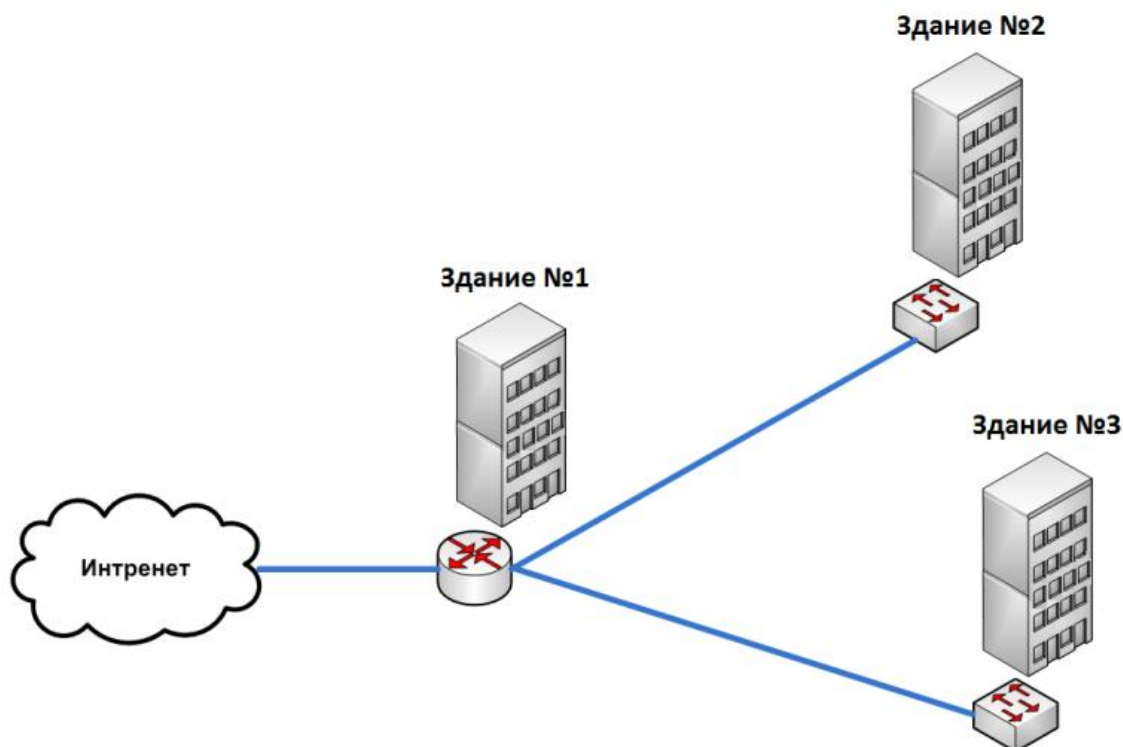


Рисунок 2.1 – Обобщенная схема сети ОАО «Стройинвест Групп»

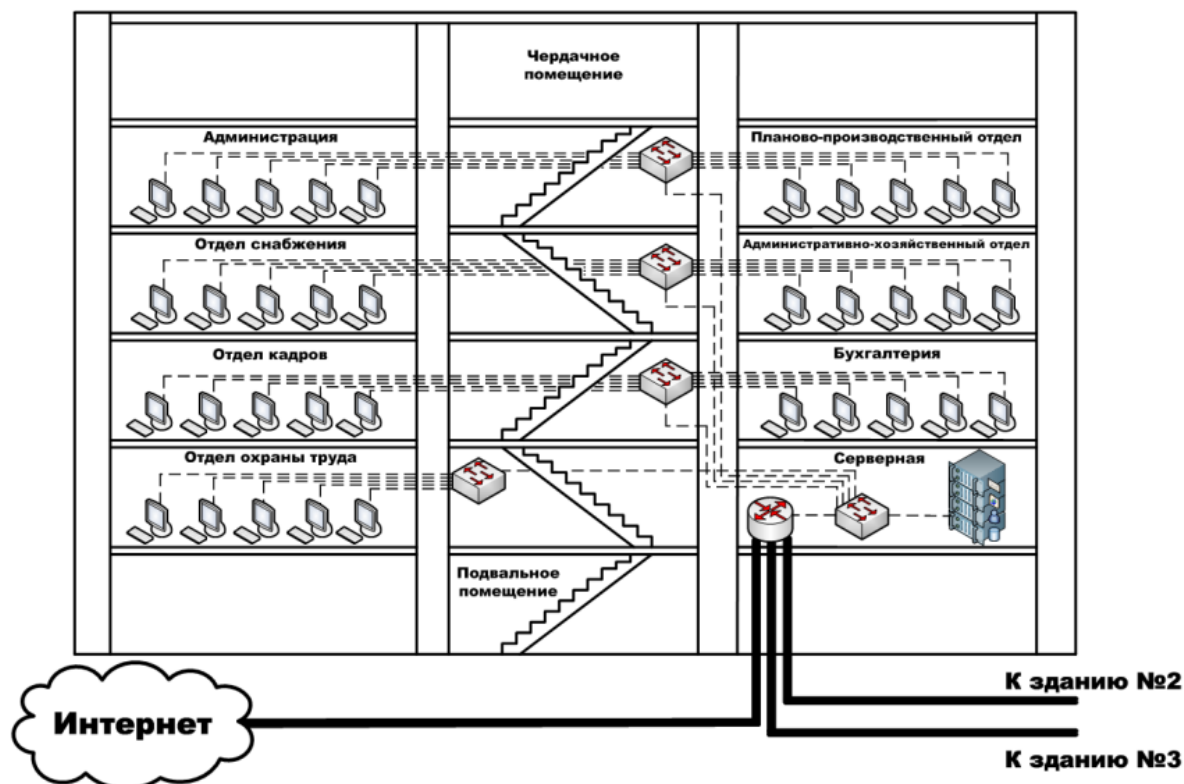


Рисунок 2.2 – Схема сети здания №1

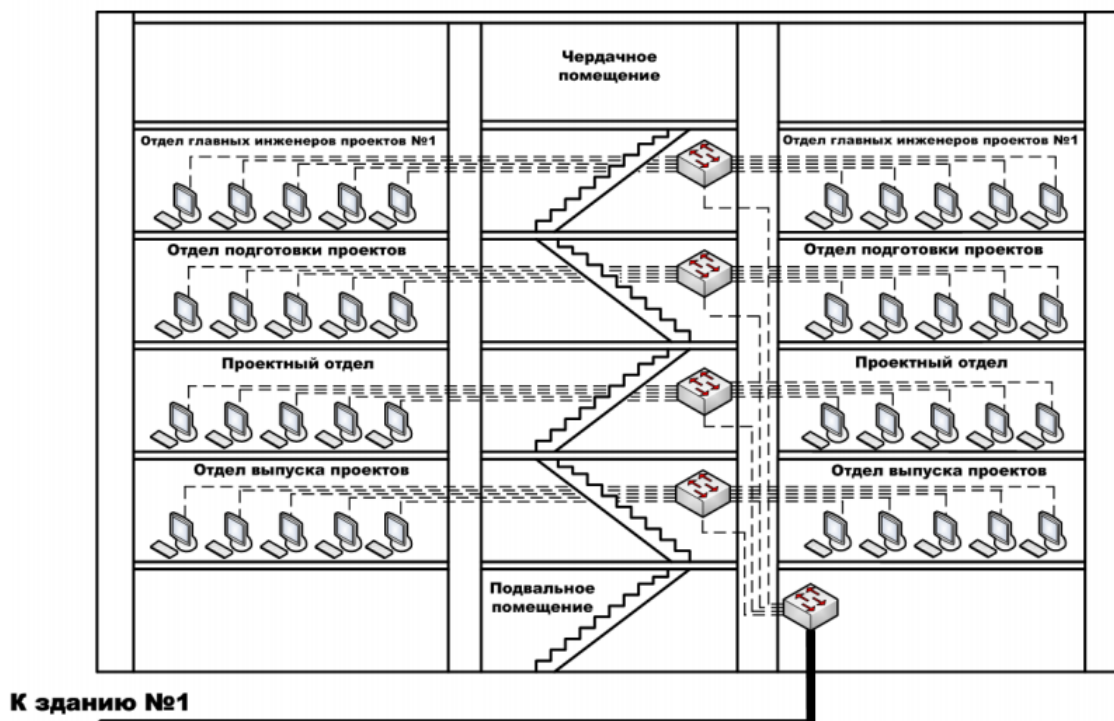


Рисунок 2.3 – Схема сети здания №2

Схема сети здания №3 аналогична схеме сети здания №2.

Анализ структуры сети предприятия показал, что используемая сетевая инфраструктура не способна удовлетворить возрастающие потребности пользователей. Используемое на предприятии каналобразующие оборудование (ADSL-модемы) не может увеличить пропускную способность на данных расстояниях и используемых типах кабелей. Перегрузки коммутационного и серверного оборудования повышают частоту выхода из строя данного оборудования и, как следствие, расходы предприятия. Также участились жалобы пользователей на низкую скорость доступа в сеть, большое время отклика ресурсов (баз данных, электронной почты, сервиса IP-телефонии) корпоративной мультисервисной сети.

Анализ структуры телекоммуникационной сети позволил предъявить к ней следующий набор требований:

- Обеспечение отказоустойчивости сети и ее отдельных элементов;
- Обеспечение надежности сети предприятия;
- Обеспечение требуемой производительности сети;

- Обеспечение масштабируемости сети и гибкости ее составных элементов;
- Обеспечение требуемого уровня информационной безопасности сети;
- Повышение пропускной способности ядра сети;
- Модернизация структурированной кабельной системы;
- Обновление коммутационного и серверного оборудования, включая программное обеспечение.

2.2 Средства и инструменты исследования трафика

Для решения задач оценки интенсивности трафика в исследуемой сети, а также для оценки основных характеристик качества обслуживания пользователей: задержки передачи пакетов, времени отклика на запросы пользователя и других характеристик использован анализатор трафика Wireshark.

После запуска сетевого анализатора Wireshark главное окно программы имеет вид, представленный на рисунке 2.4.

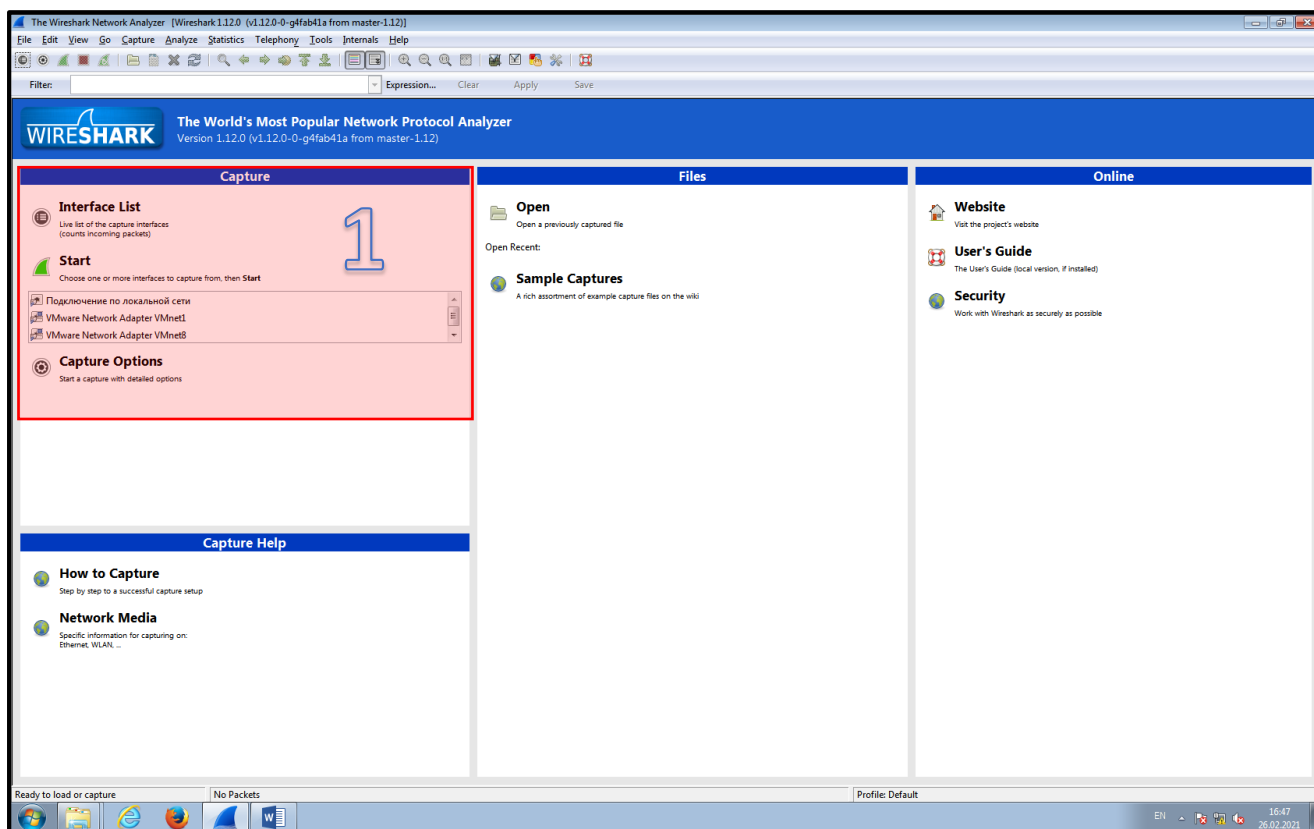


Рисунок 2.4 – Главное окно программы Wireshark

Для захвата пакетов в режиме реального времени необходимо выбрать сетевую карту, установленную на компьютере (элемент 1 на рисунке 2.4).

Для открытия уже сохраненного файла с информацией о принятых пакетах, необходимо перейти в раздел меню «Файл» и выбрать пункт «Открыть» (рисунок 2.5).

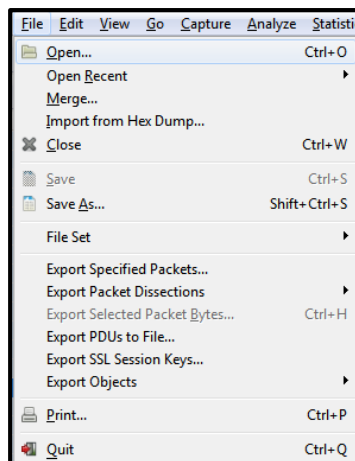


Рисунок 2.5 – Меню «Файл» главного окна программы Wireshark

После открытия файла окно программы примет вид, представленный на рисунке 2.6.

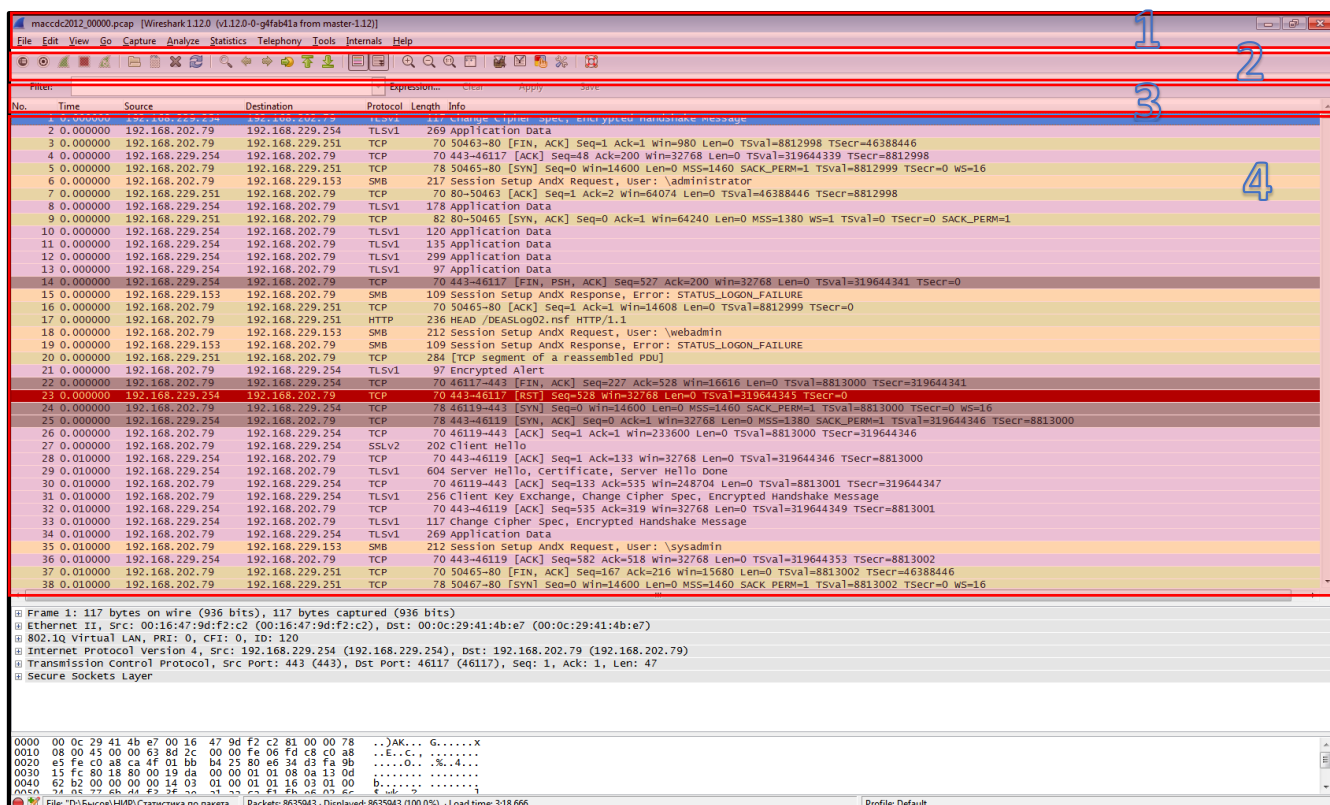


Рисунок 2.6 – Главное окно программы Wireshark с информацией о пакетах

Главное окно программы Wireshark включает панель меню и панель быстрого доступа элементы 1 и 2 соответственно на рисунке 2.6. Под панелью быстрого доступа находится панель для настройки фильтров (элемент 3 на рисунке 2.6). Под панелью фильтров находится панель с информацией о принятых пакетах (элемент 4 на рисунке 2.6). В таблице данной панели представлена следующая информация:

- Условный номер принятого пакета (№);
- Время регистрации пакета (Time);
- IP-адрес узла-источника (Source);
- IP-адрес узла назначения (Destination);
- Протокол (Protocol);
- Длина пакета (Length);
- Дополнительная информация о принятом пакете (Info).

Далее следует панель с детальной информацией по выделенному пакету (рисунок 2.7).

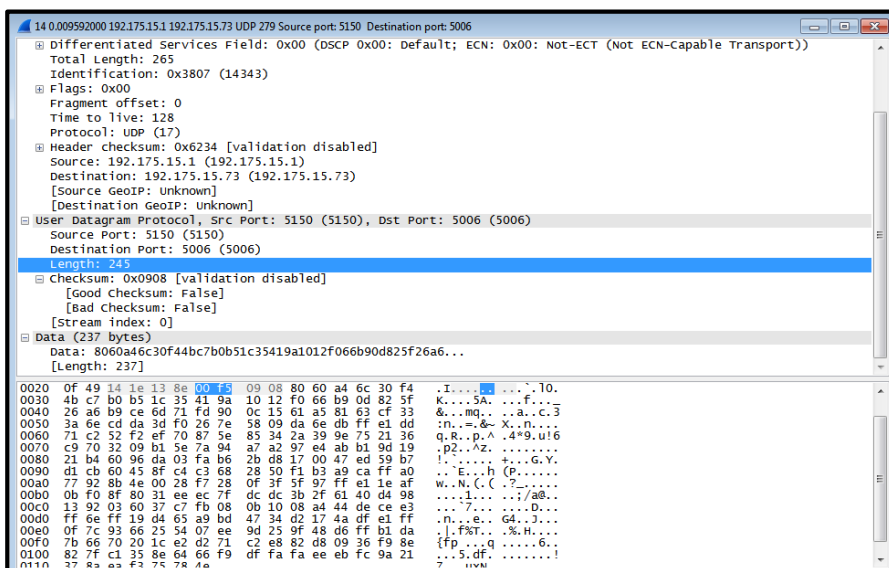


Рисунок 2.7 – Панель программы с детальной информацией о структуре пакета

В панели представлено содержимое пакета в соответствии с эталонной моделью взаимодействия открытых систем. Информация о пакетах представлена в виде дерева, ветви которого можно раскрывать для просмотра содержимого пакета на определенном уровне. Нижняя часть панели содержит дамп пакетов в шестнадцатеричной форме.

Панель «Меню» содержит пункты с интуитивно понятным назначением (рисунок 2.8).

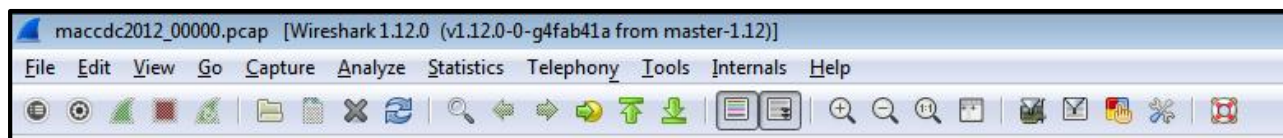


Рисунок 2.8 – Панель «Меню» и панель быстрого доступа

Для просмотра информации по пакетам используется пункт меню «Statistics» (рисунок 2.9).

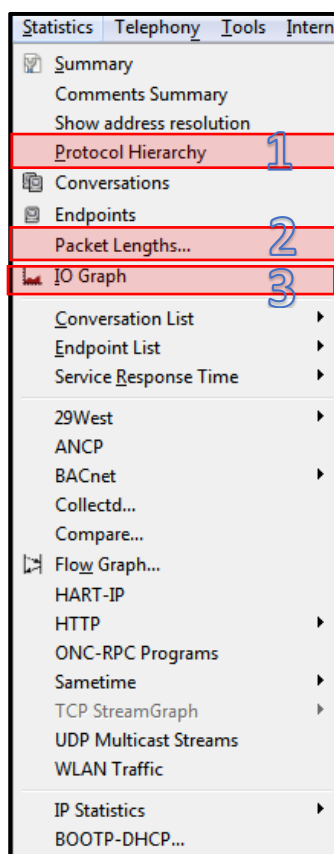


Рисунок 2.9 – Содержание пункта меню «Statistics»

Первым используемым пунктом является пункт «Иерархия протоколов» (пункт 1 на рисунке 2.9). Обзор статистики в соответствии с данным пунктом представлено на рисунке 2.10.

Пункт «Иерархия протоколов» содержит информацию об абсолютном и процентном отношении принятых байт и пакетов определенного протокола, а также скорость следования пакетов данного протокола. Информация представляется таблично. Колонка «Протокол» имеет древовидную структуру с различной детализацией.

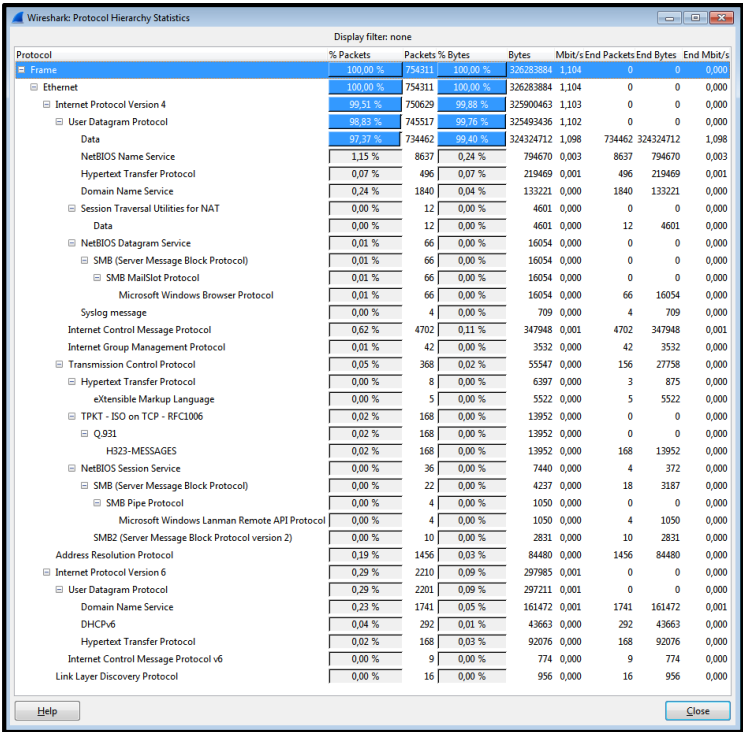


Рисунок 2.10 – Пример окна «Иерархия протоколов»

Следующим важным пунктом для обобщенного анализа длин принятых пакетов является пункт «Длина пакетов» (элемент 2 на рисунке 2.11). Пример окна «Длина пакетов» представлено на рисунке 2.11.

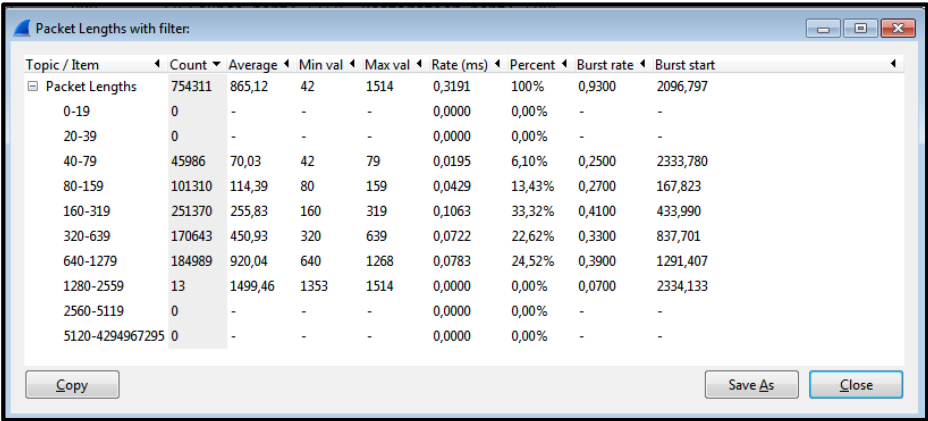


Рисунок 2.11 – Пример окна «Длина пакетов»

Для построения зависимости интенсивности мультисервисного трафика от времени используется пункт меню «График интенсивности» (элемент 3 на рисунке 2.9). Сетевой анализатор позволяет строить зависимости интенсивности трафика измеряемой как в бит/с (рисунок 2.12), так и - пакет/с (рисунок 2.13).

Мультисервисный трафик имеет пульсирующий характер, причем амплитуда пульсаций имеет достаточно большое значение относительно среднего значения.

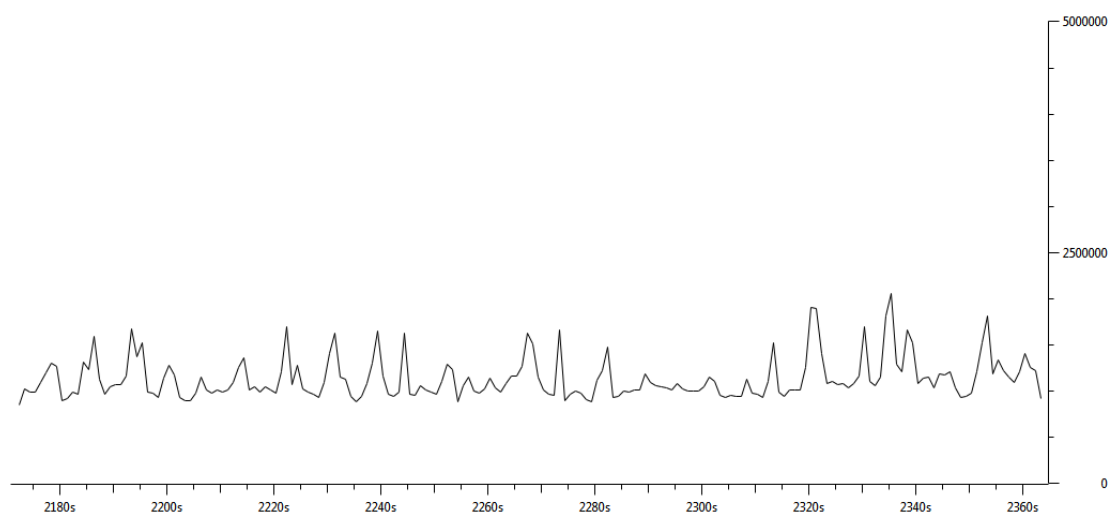


Рисунок 2.12 – Зависимость интенсивности мультисервисного трафика (бит/с) от времени

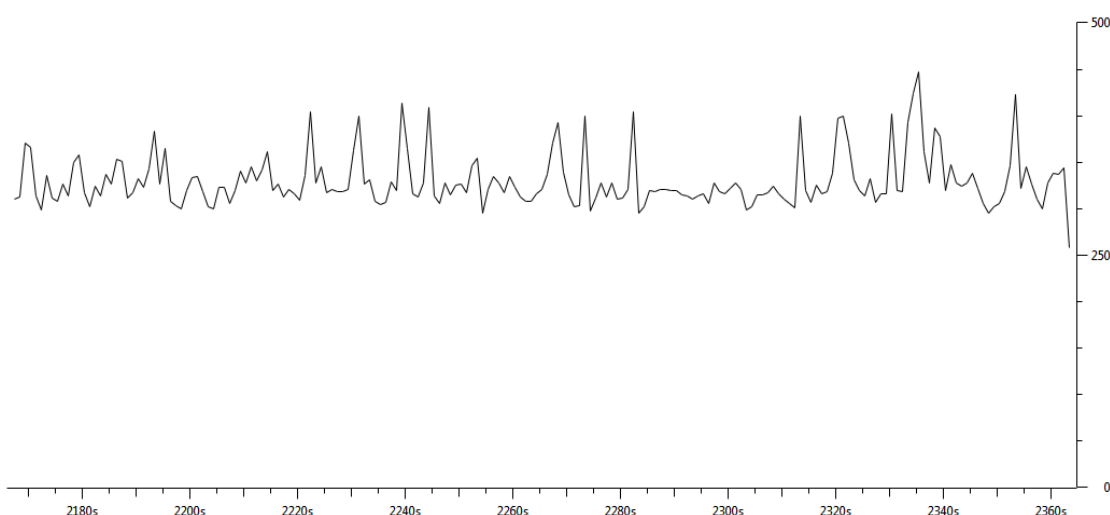


Рисунок 2.13 – Зависимость интенсивности мультисервисного трафика (пакет/с) от времени

Для исследования характеристик определенной группы пакетов используется панель «Фильтр» (рисунок 2.14).



Рисунок 2.14 – Панель «Фильтр»

В программе можно как встроенные фильтры (рисунок 2.15), так и создавать пользовательские фильтры. Создание пользовательских фильтров основано на использовании операторов сравнения и логических операторов.

Основные операторы сравнения представлены в таблице 2.1.

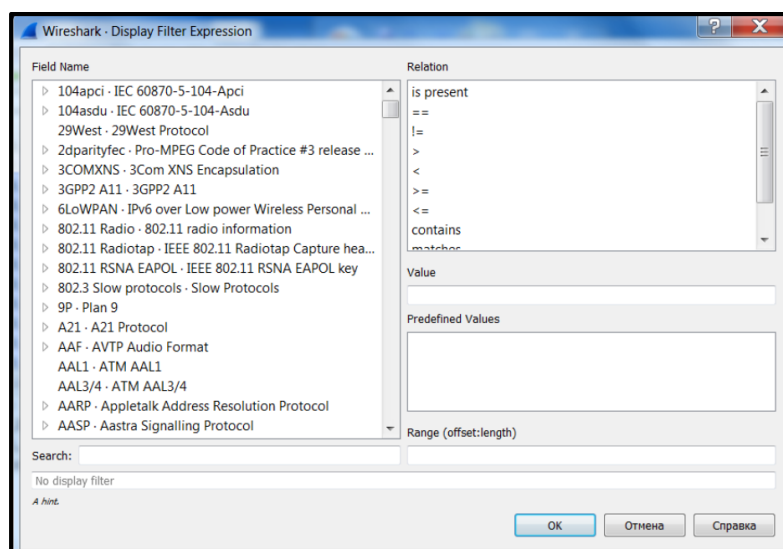


Рисунок 2.15 – Встроенные фильтры программы Wireshark

Таблица 2.1 – Основные операторы сравнения

Оператор сравнения	Пояснение
tcp.ack	Подтверждения (ACK) протокола TCP
udp.port	Порт источника или получателя в сегменте протокола UDP
ip.proto	Обозначение протокола, который был инкапсулирован в пакет IP
tcp.srcport	Порт источника в сегменте протокола TCP
tcp.dstport	Порт получателя в сегменте протокола TCP
dns.resp.name	Имя сетевого ресурса в DNS ответе
dns.qry.name	Имя сетевого ресурса в DNS запросе
tcp.port	Порт источника или получателя в сегменте протокола TCP
ip.addr	Сетевой адрес источника или получателя в пакете протокола IP
ip.src	Сетевой адрес источника в пакете протокола IP
ip.dst	Сетевой адрес получателя в пакете протокола IP
eth.addr	Физический адрес источника или получателя в кадре протокола Ethernet
eth.src	Физический адрес источника в кадре протокола Ethernet
eth.dst	Физический адрес получателя в кадре протокола Ethernet
eth.len	Длина кадра протокола Ethernet

Для создания комбинированных фильтров используются логические операторы. Логические операторы и примеры их применения представлены в таблице 2.2.

Таблица 2.2 – Основные логические операторы

Логический оператор	Значение	Пример
>	больше	tcp.srcport>2000 - отобразить только те сегменты протокола TCP, в которых порт источника больше 2000
<	меньше	tcp.srcport<200 - отобразить только те сегменты протокола TCP, в которых порт источника меньше 2000
==	равно	ip.addr==10.10.0.27 - отображение пакетов с IP-адресом 10.10.0.27 источника или получателя
!=	не равно	ip.dst!=255.255.255.255 - не отображать широковещательные пакеты
&&	логическое «и»	ip.src==10.10.0.27&&ip.dst10.10.0.30 - отобразить только сообщения, отправленные устройством с IP-адресом 10.10.0.27 для устройства с IP-адресом 10.10.0.30.

Таким образом, программа Wireshark имеет широкие возможности по исследованию мультисервисного трафика в корпоративных сетях. Для анализа трафика сетевой анализатор должен быть установлен на компьютер, который можно подключать в различных точках сети для регистрации трафика. Как правило анализаторы трафика устанавливаются в ядре мультисервисной сети для исследования агрегированных потоков трафика. Технически задача подключения регистрирующего компьютера решается путем перевода одного из интерфейсов коммутатора в режим «Зеркало» для параллельного захвата пакетов трафика без разрыва соединения.

2.3 Анализ и классификация сетевого трафика

В результате исследования трафика мультисервисной сети получены интенсивности трафика в ядре сети. Зависимость интенсивности трафика выраженной в бит/с и пакет/с представлены на рисунках 2.16 и 2.17 соответственно.

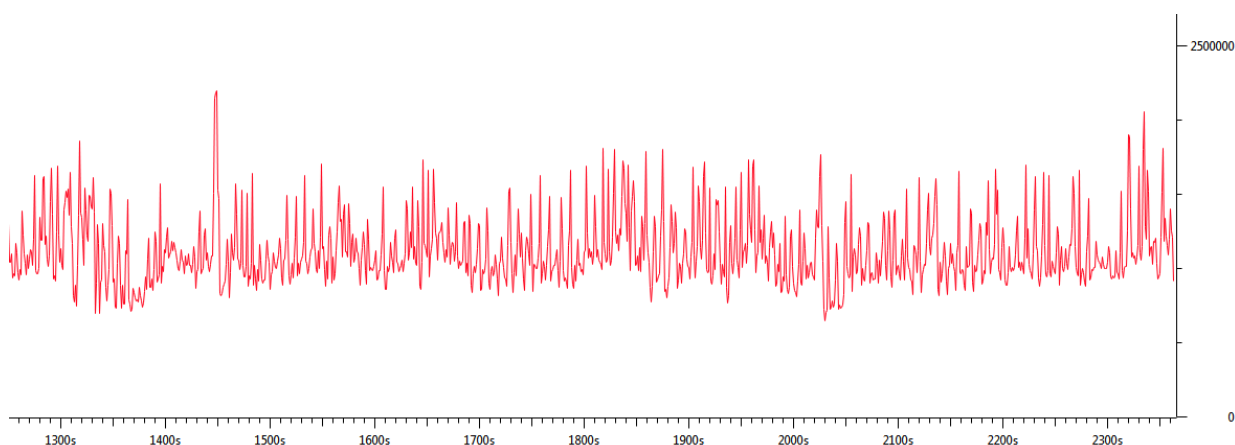


Рисунок 2.16 – Интенсивность мультисервисного трафика (бит/с)

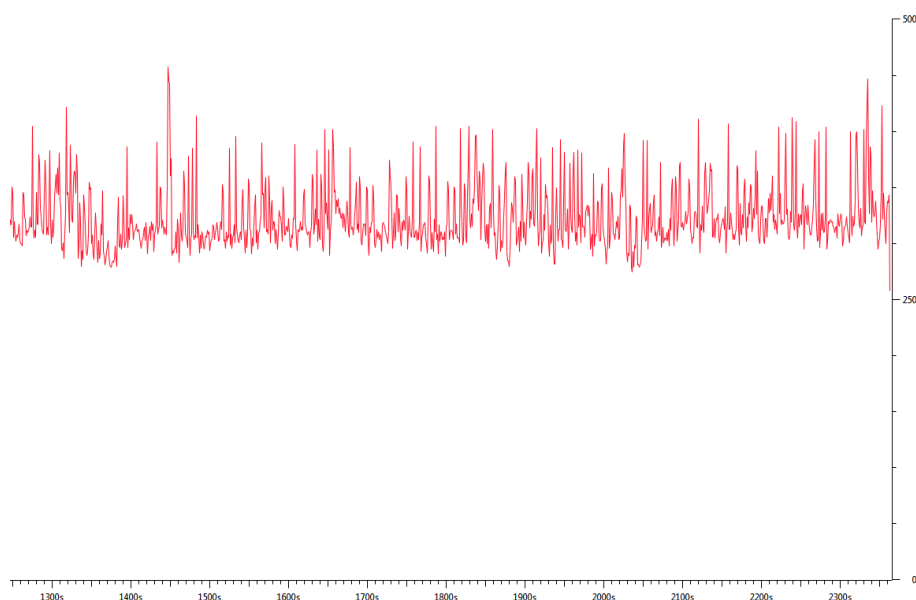


Рисунок 2.17 – Интенсивность мультисервисного трафика (пакет/с)

Для оценки среднего значения интенсивности мультисервисного трафика, проведено усреднение данных в программе. Среднее значение интенсивности, измеренное в бит/с и пакет/с представлено на рисунках 2.18 и 2.19 соответственно.

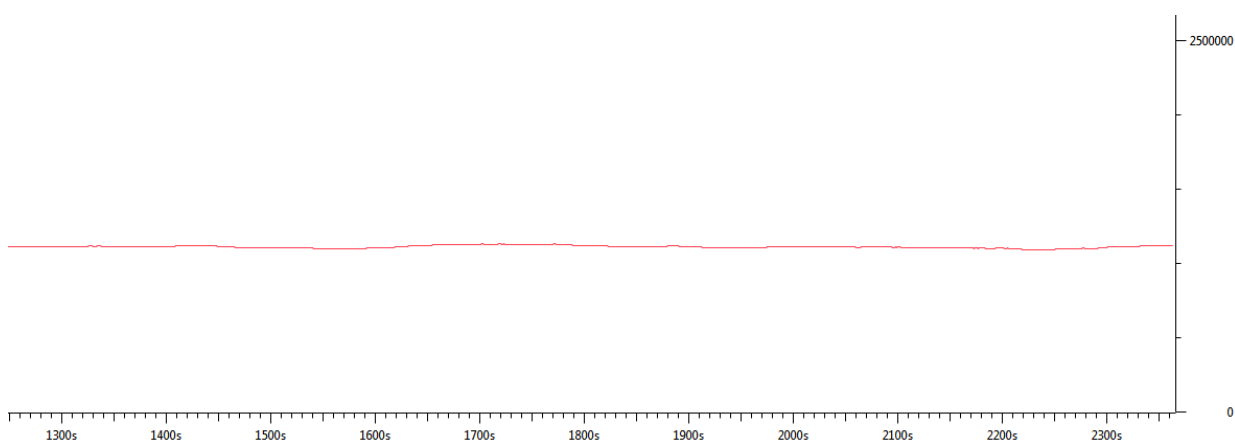


Рисунок 2.17 – Среднее значение интенсивности трафика (бит/с)

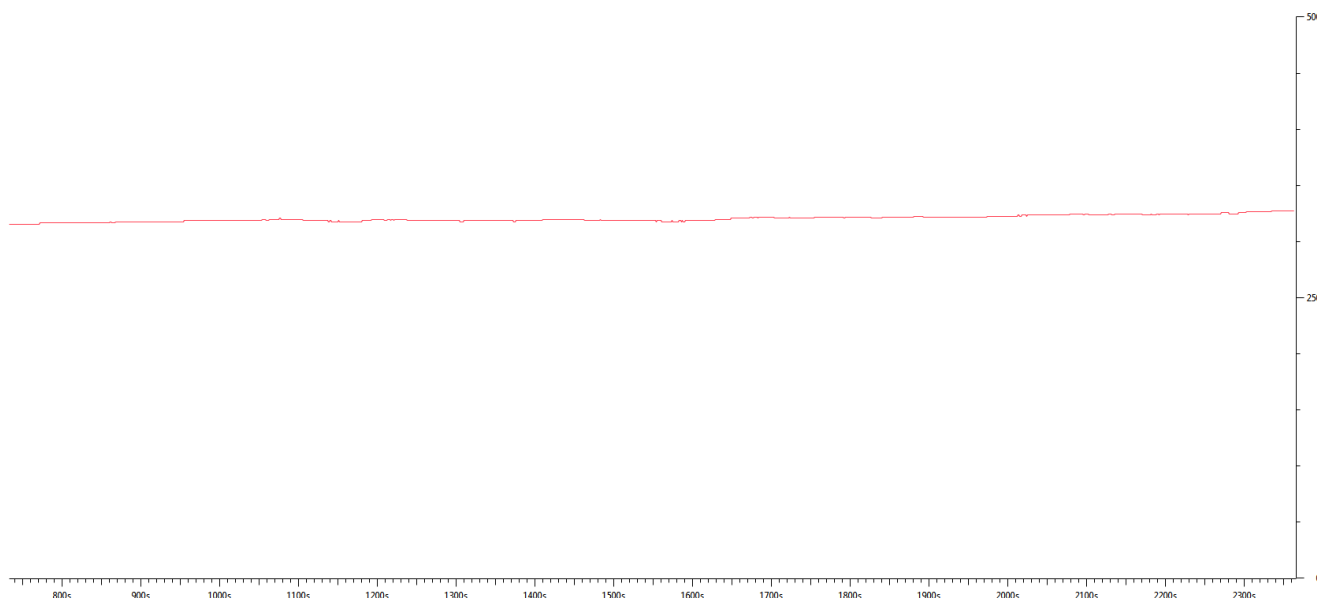


Рисунок 2.18 – Среднее значение интенсивности трафика (пакет/с)

На рисунках 2.15 и 2.16 показано, что из-за наличия входных и выходных буферов у коммутационных устройств пакеты следуют группами (пачками), что приводит к наличию пульсаций. Наблюдаемые пульсации имеют относительно невысокую длительность, однако, достаточно высокую амплитуду относительно среднего значения. Наличие пульсаций предполагает наличие существенного запаса по пропускной способности линий связи.

На рисунках 2.17 и 2.18 показано, что среднее значение интенсивности мультисервисного трафика составляет 1,2 Мбит/с или 330 пакетов/с.

Для дальнейшего анализа объемов трафика в зависимости от типа протокола транспортного уровня ЭМВОС. данные полученные в разделе «Иерархия протоколов» меню «Статистики» программы Wireshark перенесены в редактор Microsoft Office Excel. Структура мультисервисного трафика на транспортном уровне представлена на рисунке 2.19.

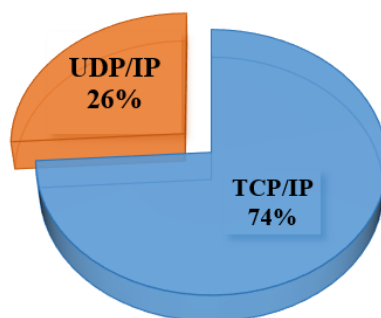


Рисунок 2.19 – Структура трафика на транспортном уровне

На рисунке 2.19 показано, что преобладающую часть пакетов на транспортном уровне передается в соответствии с протоколом гарантированной доставки пакетов (TCP). Однако существенную долю занимают пакеты, переданные в соответствии с протоколом транспортного уровня негарантированной доставки пакетов (UDP). Наличие 26% данных пакетов можно объяснить используемыми сервисами в сети, а именно системой видеонаблюдения (пакеты данного сервиса передаются, как правило, в соответствии с протоколом UDP для снижения средней задержки передачи пакетов).

Дальнейший анализ проведен в соответствии с используемыми приложениями внутри стеков TCP/IP и UDP/IP.

Распределение пакетов в соответствии со стеком UDP/IP представлено на рисунке 2.20.

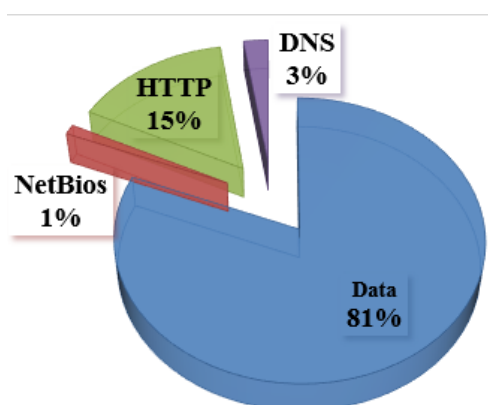


Рисунок 2.20 – Структура трафика в соответствии со стеком протоколов UDP/IP

На рисунке 2.20 показано, что 81% занимают передаваемые данные, к которым относится подвижное изображение (видеопоток), голосовая информация. Данный видео и аудио поток формируют IP-камеры системы видеонаблюдения. Следующим по объему является трафик, переданный в соответствии с протоколом HTTP (15%).

Протокол HTTP (Hypertext Transfer Protocol) является протоколом прикладного уровня ЭМВОС. Данный протокол используется для работы с веб-ресурсами. Основной программой для работы в соответствии с протоколом HTTP на стороне клиента является веб-браузер. В исследуемой корпоративной мультисервисной сети сотрудники пользуются доступом в сеть Интернет, а также

доступом к корпоративному сайту, размещенного на веб-сервере. Процесс обмена в системе «клиент-сервер» в соответствии с протоколом HTTP представлено на рисунке 2.21.

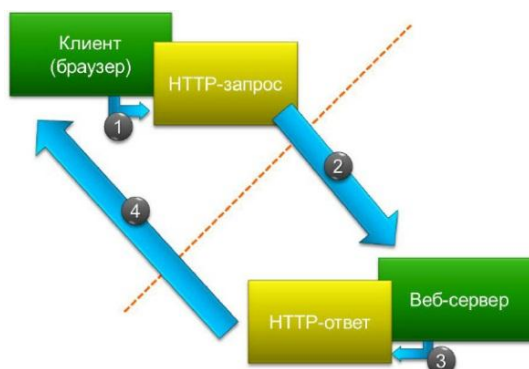


Рисунок 2.21 – Процесс обмена в соответствии с протоколом HTTP

Протокол DNS (Domain Name System – система доменных имен). Протокол прикладного уровня ЭМВОС, который предназначен для преобразования известного доменного имени (например, mail.ru) в IP-адрес сервера, на котором находится веб-ресурс. Организация работы службы DNS представлена на рисунке 2.22.

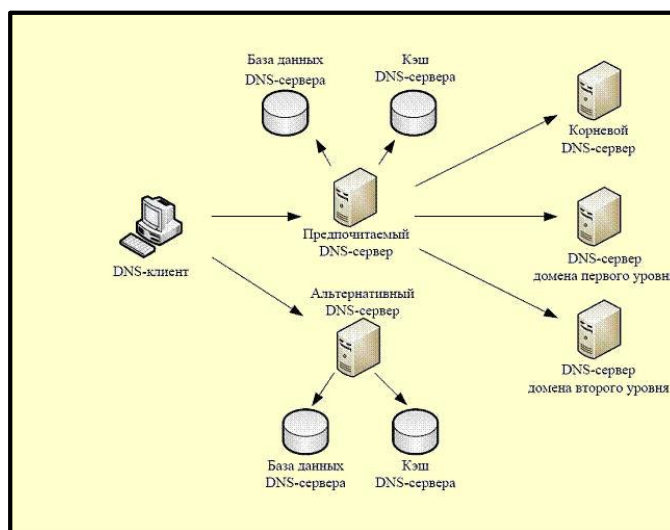


Рисунок 2.22 – Организация службы DNS

Протокол NetBIOS (Network Basic Input/Output System) – протокол сеансового уровня ЭМВОС, разработанный для локальных вычислительных сетей, построенных на базе компьютеров семейства IBM/PC. Является универсальным протоколом-интерфейсом взаимодействия (API) для управления сетевыми операциями ввода/вывода.

Распределение пакетов в соответствии со стеком TCP/IP представлено на рисунке 2.23.

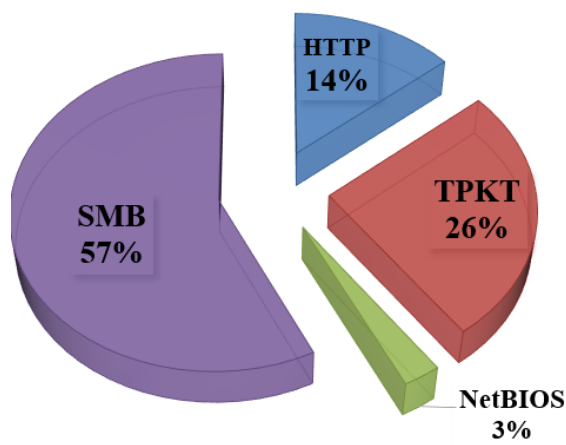


Рисунок 2.23 – Структура трафика в соответствии со стеком протоколов TCP/IP

На рисунке 2.20 показано, что 57% занимают пакеты, переданные в соответствии с протоколом SMB (Server Message Block) – протокол сетевого уровня ЭМВОС, который обеспечивает доступ к сетевым ресурсам: файлам, принтерам, сканерам, а также для межпроцессорного взаимодействия.

Протокол HTTP также может передаваться в соответствии с протоколом транспортного уровня TCP, о чем свидетельствует статистика в результате регистрации мультисервисного трафика. Похожая ситуация и с протоколом NetBIOS (3%), который также поддерживает оба протокола транспортного уровня.

Протокол TRKT сеансовый протокол контроля передачи для протокола прикладного уровня RDP (Remote Desktop Protocol) – протокол удаленного рабочего стола. Данный протокол используется для обеспечения удаленной работы пользователей с сервером, на котором реализуется услуга терминальных подключений.

Дальнейший анализ проведен для длин пакетов, передаваемых в мультисервисной корпоративной сети. Диаграмма распределения длин пакетов в соответствии со стеком TCP/IP представлена на рисунке 2.24.

Большая часть пакетов в передаваемом трафике имеют длину в диапазоне от 40 до 319 байт. Средняя длина пакетов равна 302 байта.

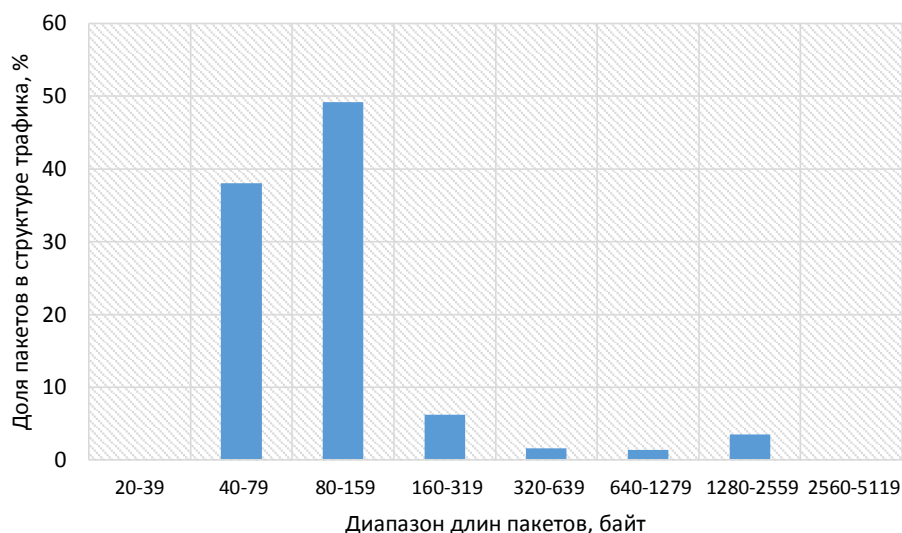


Рисунок 2.24 – Диаграмма длин пакетов трафика в соответствии со стеком протоколов TCP/IP

Диаграмма распределения длин пакетов в соответствии со стеком UDP/IP представлена на рисунке 2.25.

Распределение длин пакетов в соответствии со стеком UDP/IP имеет более равномерную структуру. Средняя длина пакетов равна 871 байт.

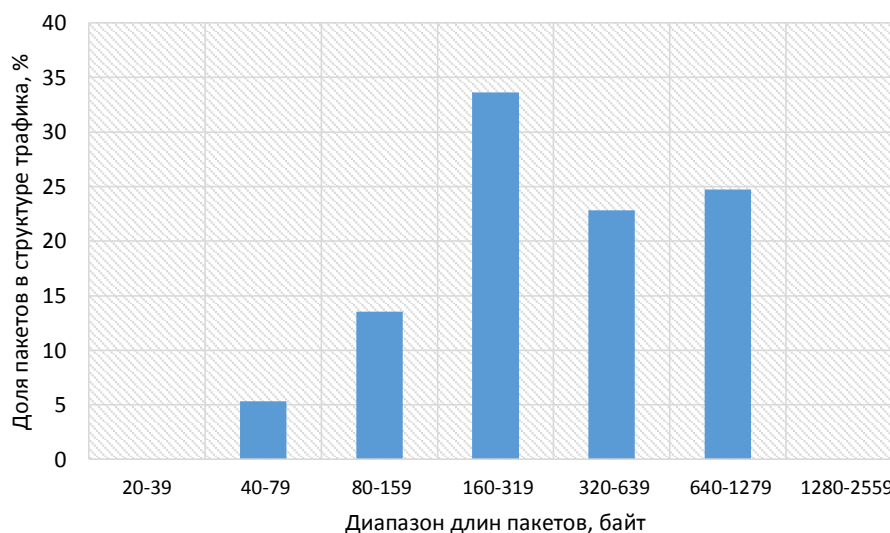


Рисунок 2.25 – Диаграмма длин пакетов трафика в соответствии со стеком протоколов UDP/IP

Пакеты определенных протоколов прикладного уровня (например, UDP) имеют более однородную структуру распределения длин пакетов (рисунок 2.26).

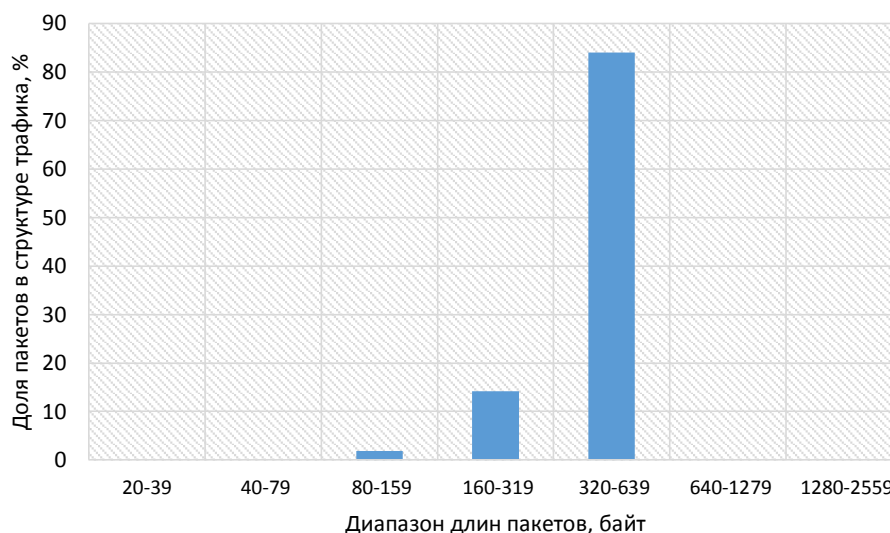


Рисунок 2.26 – Диаграмма длин пакетов трафика в соответствии со стеком протоколов HTTP/UDP/IP

Большинство пакетов (84%) имеют длину в диапазоне от 320 до 639 байт, что можно объяснить принципом работы протокола UDP. То есть, при негарантированной доставке пакетов и отсутствии логического соединения между отправителем и получателем, нет механизма изменения длин пакетов в зависимости от качества передачи по каналам связи.

Для сравнения проанализирован тот же протокол прикладного уровня (HTTP), но при передаче в соответствии со стеком TCP/IP (рисунок 2.27).

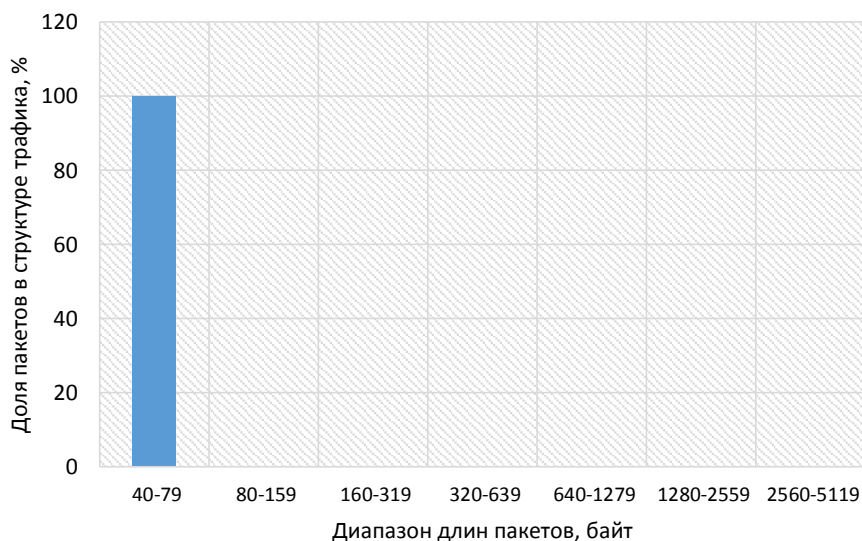


Рисунок 2.26 – Диаграмма длин пакетов трафика в соответствии со стеком протоколов HTTP/TCP/IP

На рисунке 2.26 показано, что протокол транспортного уровня управляет длиной сегмента в зависимости от условий передачи (например, пакеты с длиной в диапазоне от 320 до 639 байт отсутствуют).

Отдельно исследовано распределение длин пакетов в соответствии с протоколом ICMP (Internet Control Message Protocol) - протокол межсетевых управляющих сообщений. Распределение длин пакетов в соответствии с протоколом ICMP представлено на рисунке 2.27.

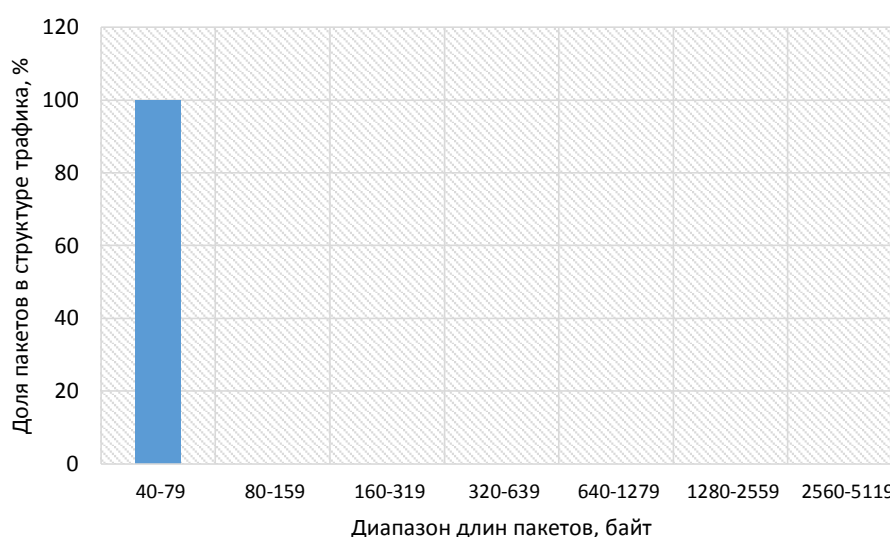


Рисунок 2.27 – Диаграмма длин пакетов в соответствии с протоколом ICMP

Пакеты протокола ICMP имеют фиксированную длину. Длина ICMP-пакета равна 74 байта.

Также проведено исследование пакетов, переданных в соответствии с протоколом ARP (Address Resolution Protocol) – протокола разрешения адресов. Распределение длин пакетов в соответствии с протоколом ARP представлено на рисунке 2.28. Средняя длина ARP-пакетов равна 58 байт.

Учитывая факт одновременной поддержки двух протоколов сетевого уровня (IPv4 и IPv6) на большинстве современных терминальных и сетевых устройств, проведен анализ распределения длин пакетов данных протоколов. Распределение длин пакетов в соответствии с протоколом IPv4 и IPv6 представлено на рисунках 2.29 и 2.30 соответственно.

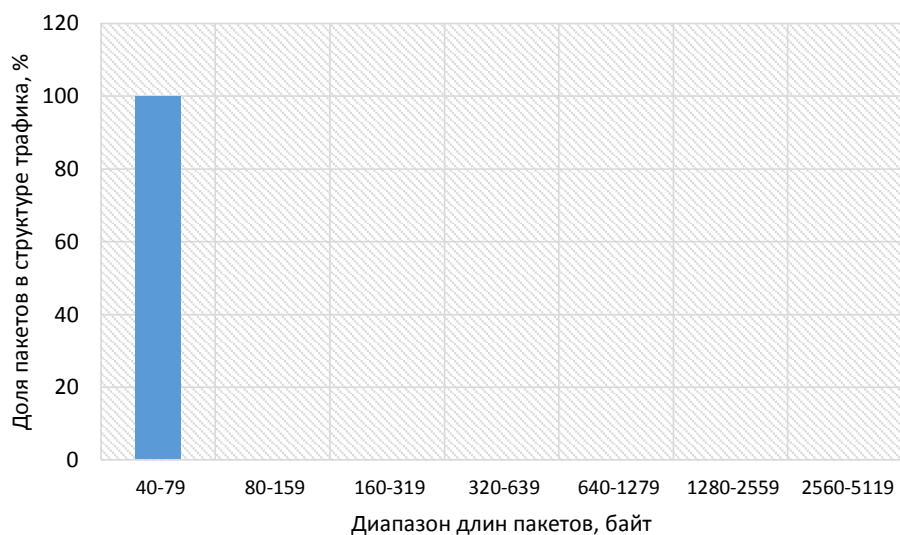


Рисунок 2.28 – Диаграмма длин ARP-пакетов

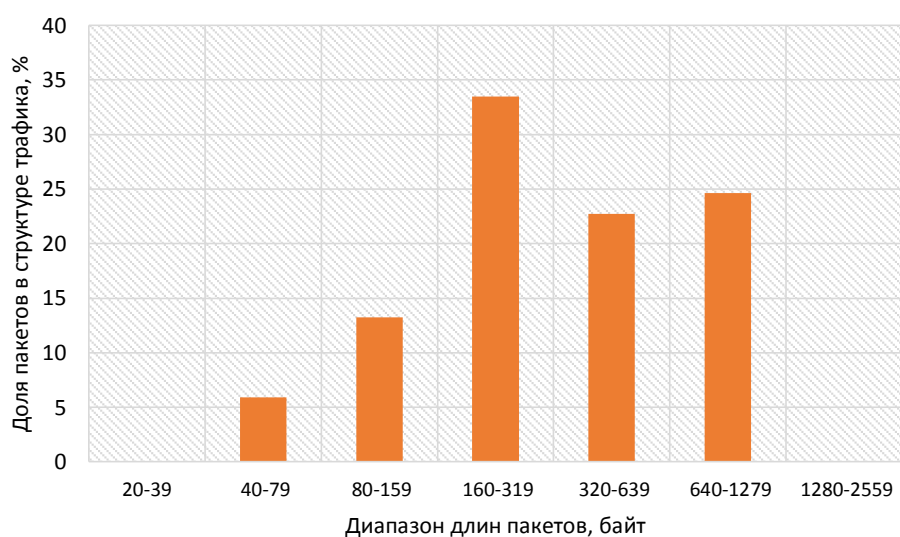


Рисунок 2.29 – Диаграмма длин пакетов IPv4

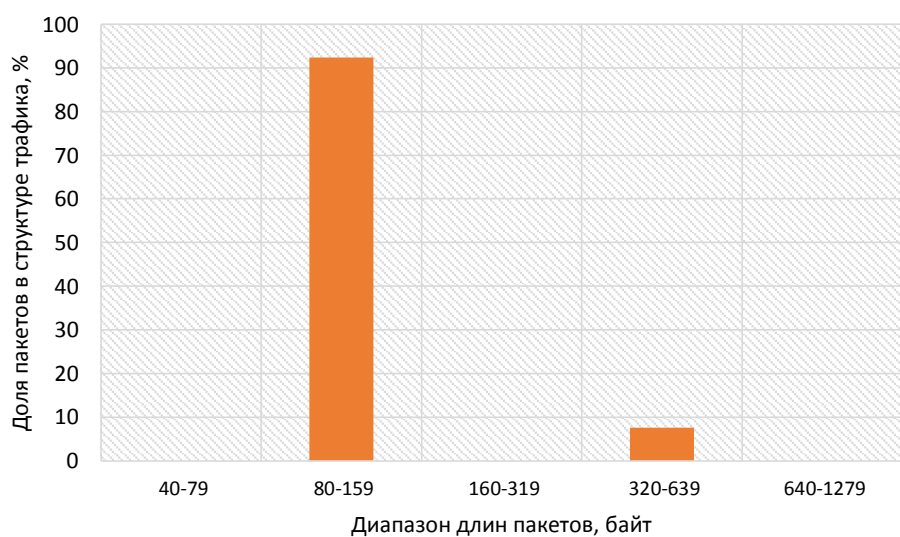


Рисунок 2.30 – Диаграмма длин пакетов IPv6

Распределение длин пакетов в соответствии с протоколом IPv4 носит достаточно предсказуемый характер, а именно, большинство протоколов вышестоящих уровней (от транспортного до прикладного) используют на сетевом уровне протокол IP и определяют необходимую длину пакета на данном уровне. Средняя длина пакета IPv4 равна 434 байта.

Для пакетов IPv6 наблюдается иная картина (рисунок 2.30): распределение длин большинства пакетов соответствует диапазону от 80 до 159 байт, что можно объяснить небольшим количеством прикладных процессов, которые используют в качестве протокола сетевого уровня IPv6. Таким образом, применение шестой версии протокола IP в исследуемой корпоративной сети носит ограниченный характер. Средняя длина пакета IPv6 равна 134 байта.

2.3 Выводы

5. Рассматриваемая корпоративная мультисервисная сеть строится на достаточно низкоскоростной технологии SHDSL (в сравнении с волоконно-оптическими линиями связи).

6. В настоящей главе проведен сбор и анализ мультисервисного трафика при помощи программы WireShark. На основе данного программного продукта проведена оценка интенсивности трафика и средней интенсивности трафика.

7. Получены данные о структуре мультисервисного трафика на всех уровнях эталонной модели взаимодействия открытых систем. Определены соотношения доли различных протоколов в общей структуре трафика.

8. Проведен анализ распределения длин пакетов на сетевом и транспортном уровне, а также исследованы особенности передачи протокола HTTP в зависимости от используемого протокола транспортного уровня.

3 Результаты исследования трафика корпоративной мультисервисной сети

3.1 Анализ динамики трафика корпоративной мультисервисной сети

Для анализа и прогнозирования мультисервисного трафика корпоративной сети создана имитационная модель в сетевом симуляторе Opnet Modeller. Сетевой симулятор Opnet Modeller имеет интуитивно понятный интерфейс, богатую библиотеку сетевых и терминальных устройств, каналообразующего оборудования. Интерфейс программы с рабочей областью для создания модели представлен на рисунке 3.1.

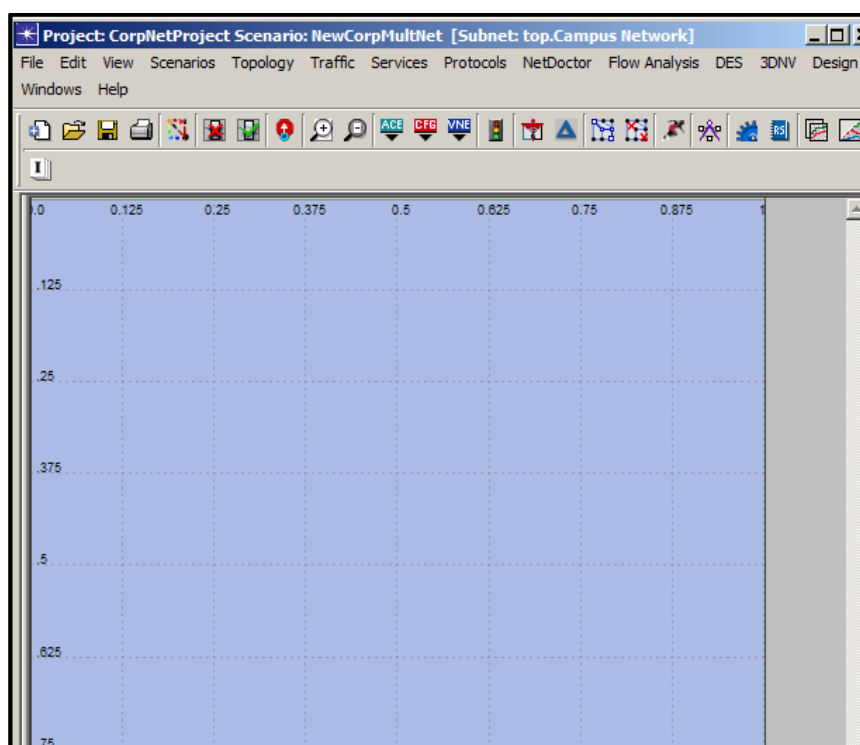


Рисунок 3.1 – Интерфейс программы Opnet Modeller

На рабочую область, которая по размерам соответствует площади занимаемой зданиями трех офисов компании, добавлены сетевые элементы из библиотеки элементов Opnet Modeller (рисунок 3.2). Для реализации имитационной модели корпоративной мультисервисной сети использованы следующие объекты библиотеки элементов:

- Маршрутизатор;

- Три коммутатора третьего уровня;
- Четыре сервера (сервер баз данных, сервер электронной почты, файловый сервер, сервер IP-телефонии);
- Четыре SHDSL-модема;
- Сеть доступа (коммутаторы доступа, терминальные устройства пользователей) представлена элементом LAN, создающим адекватную нагрузку на коммутационные устройства корпоративной сети;
- Соединительные линии (для соединения терминальных и коммутационных устройств настроена спецификация 100Base-TX технологии Fast Ethernet, а для соединения SHDSL-модемов использована линия связи на основе медного кабеля с пропускной способностью 6 Мбит/с).

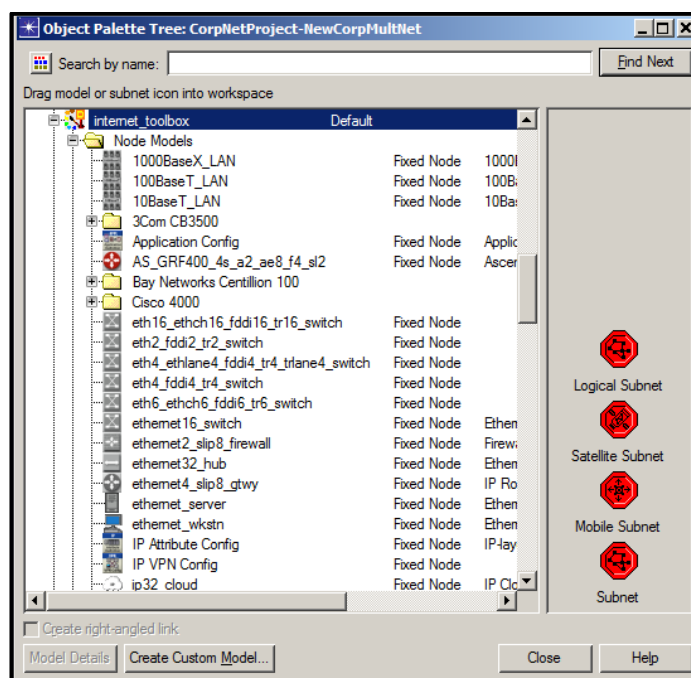


Рисунок 3.2 – Библиотека элементов сетевого симулятора Ornet Modeller

Структура мультисервисной корпоративной сети в симуляторе Ornet Modeller представлена на рисунке 3.3.

В качестве исходных данных для проведения имитационного моделирования использованы результаты анализа трафика корпоративной сети, представленные в пункте 2.3 магистерской диссертации. Настройка основных элементов имитационной модели сети представлена на рисунках 3.4-3.6.

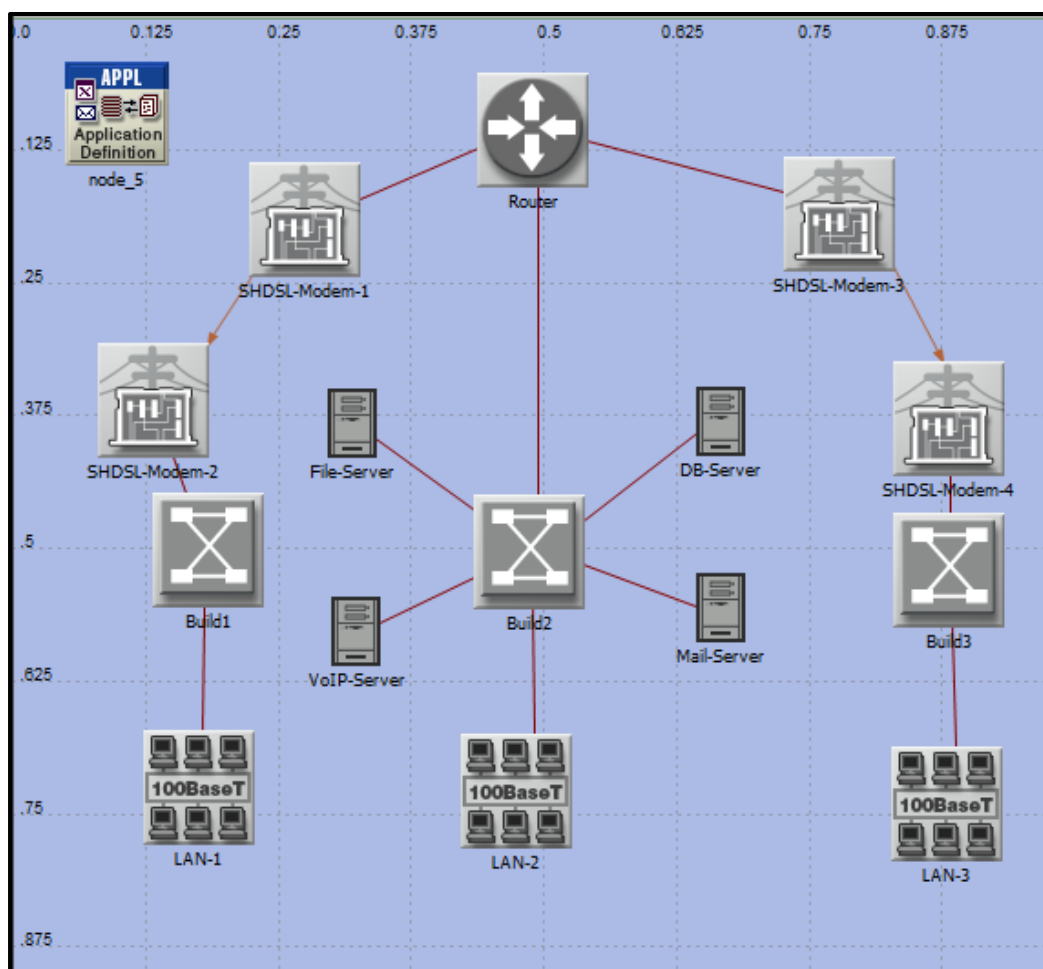


Рисунок 3.3 – Структура сети в сетевом симуляторе Opnet Modeler

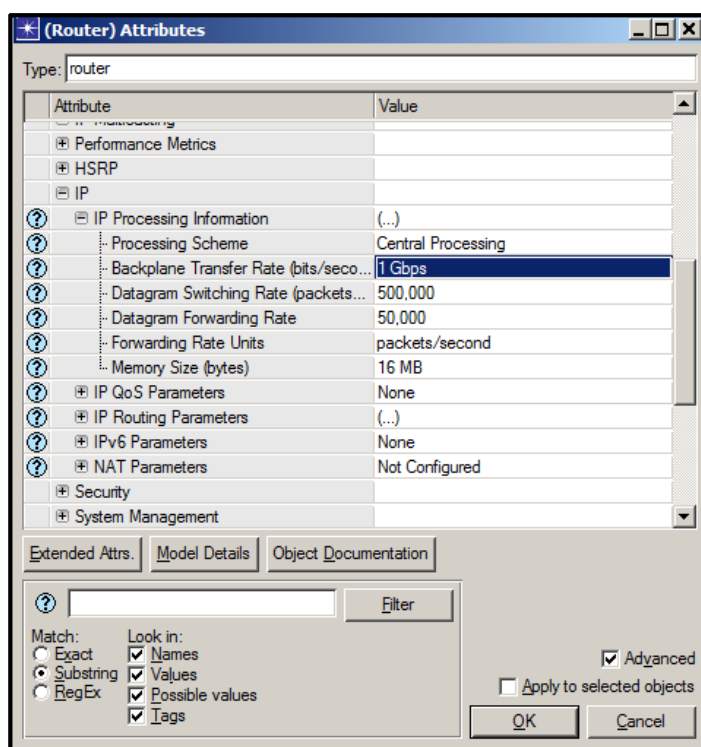


Рисунок 3.4 – Параметры имитационной модели маршрутизатора

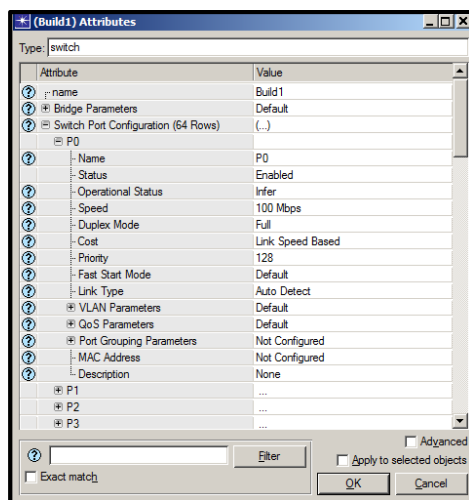


Рисунок 3.5 – Параметры имитационной модели коммутатора

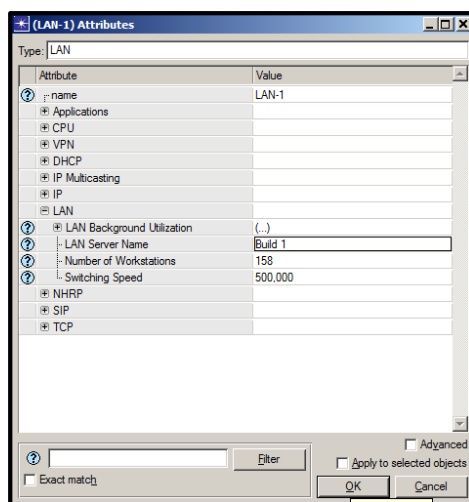


Рисунок 3.6 – Параметры имитационной модели сети доступа (элемент LAN)

Для анализа основных параметров функционирования сети проведен расчет полезной пропускной способности между офисами компании с учетом что полная пропускная способность равна 6 Мбит/с.

Значение полезной пропускной способности зависит от размера Ethernet-кадра на канальном уровне: чем меньше размер Ethernet-кадра, тем большую долю пропускной способности занимает заголовок Ethernet-кадра, который имеет фиксированную длину. Наиболее эффективно пропускная способность будет расходоваться в сетях с однородным трафиком, в которой длина Ethernet-кадров будет максимальной.

Служебная информация Ethernet-кадра равна 18 байт. Размер поля данных лежит в интервале от 46 до 1500 байт. Таким образом, размер Ethernet-кадра лежит в диапазоне от 64 байт (18+46) до 1518 байт (18+1500).

Доля полезной информации для Ethernet-кадра минимальной длины равна:

$$\gamma_{min} = \frac{46}{64} = 0.72.$$

Доля полезной информации для Ethernet-кадра максимальной длины равна:

$$\gamma_{max} = \frac{1500}{1518} = 0.99.$$

Определим частоту следования кадров минимального и максимального размеров.

Длина кадра минимальной длины вместе с преамбулой составляет 72 байта (64+8), что соответствует 576 битам информации. Межкадровый интервал составляет 96 бит, следовательно, период следования кадров равен 672 бита (576+96). Скорости 6 Мбит/с будет соответствовать время 112 мкс. Тогда частота следования кадров равна

$$\mu' = \frac{1}{112 \cdot 10^{-6}} = 8929 \frac{\text{кадр}}{\text{с}}.$$

Длина кадра максимальной длины вместе с преамбулой составляет 1526 байта (1518+8), что соответствует 12208 битам информации. Межкадровый интервал составляет 96 бит, следовательно, период следования кадров равен 12304 бита (12208+96). Скорости 6 Мбит/с будет соответствовать время 2051 мкс. Тогда частота следования кадров равна

$$\mu'' = \frac{1}{2051 \cdot 10^{-6}} = 488 \frac{\text{кадр}}{\text{с}}.$$

Определим полезную пропускную способность в соответствии с выражением

$$B_{\Pi} = V_{\kappa} \cdot 8 \cdot \mu.$$

Для кадра минимальной длины $V_{\kappa min} = 46$ байт полезная пропускная способность равна

$$B_{\Pi min} = V_{\kappa min} \cdot 8 \cdot \mu' = 46 \cdot 8 \cdot 8929 = 3.29 \text{ Мбит/с}.$$

Для кадра минимальной длины $V_{k\min} = 46$ байт полезная пропускная способность равна

$$B_{п\max} = V_{к\max} \cdot 8 \cdot \mu'' = 1500 \cdot 8 \cdot 488 = 5.86 \text{ Мбит/с.}$$

Таким образом, полезная пропускная способность соединительных линий между офисами мультисервисной корпоративной сети составляет от 3.29 до 65.86 Мбит/с.

Далее определим значения полезной пропускной способности при помощи эксперимента на участке реальной сети исследуемой организации

Для формирования кадров минимальной длины по сети отправлялись тысяча файлов размером 1 байт каждый, что соответствует формированию одной тысяче кадров. Далее произведена оценка времени затрачиваемого на пересылку файлов при помощи программы WireShark.

Полезная пропускная способность составила

$$B_{пр\min} = 3.21 \frac{\text{Мбит}}{\text{с}}.$$

Для формирования кадров максимальной длины по сети отправлялся один файл размером 10 Мбайт. Далее произведена оценка времени затрачиваемого на пересылку файлов при помощи программы WireShark.

Полезная пропускная способность составила

$$B_{пр\max} = 5.69 \frac{\text{Мбит}}{\text{с}}.$$

Рассчитанные и измеренные значения полезной пропускной способности для кадров минимальной и максимальной длины представлены в таблице 3.1.

В соответствии с таблицей 3.1 относительная ошибка определения полезной пропускной способности на участке корпоративной мультисервисной сети организации между офисами составила 2.4 % и 2.9 % для кадров минимальной и максимальной длины соответственно.

Таким образом, результаты проведенного эксперимента подтверждают расчетные данные.

Таблица 3.1 – Полезная пропускная способность мультисервисной корпоративной сети

Размер кадра (полезная информация), байт	Полезная пропускная способность		
	Рассчитанное значение, Мбит/с	Измеренное значение, Мбит/с	Ошибка, %
46	3.29	3.21	2.4
1500	5.86	5.69	2.9

Так как на участке сети между офисами образовалось так называемое «бутылочное горлышко» с полезной пропускной способностью от 3.3 до 5.9 Мбит/с, а в рамках подсетей офисов реализована технология Fast Ethernet, целесообразно определить *коэффициент загруженности сети*.

В соответствии с определением в [7] коэффициент загруженности сети равен отношению нагрузки на сеть к максимально пропускной способности сети.

Зная полезную пропускную способность, внесем данные изменения в имитационную модель, а далее на основе нее определим коэффициент загруженности сети.

Загрузка WAN-соединения (участок сети от маршрутизатора в офисе № 2 до ADSL-модема, через который осуществляется доступ в сеть Интернет) представлен на рисунке 3.7.

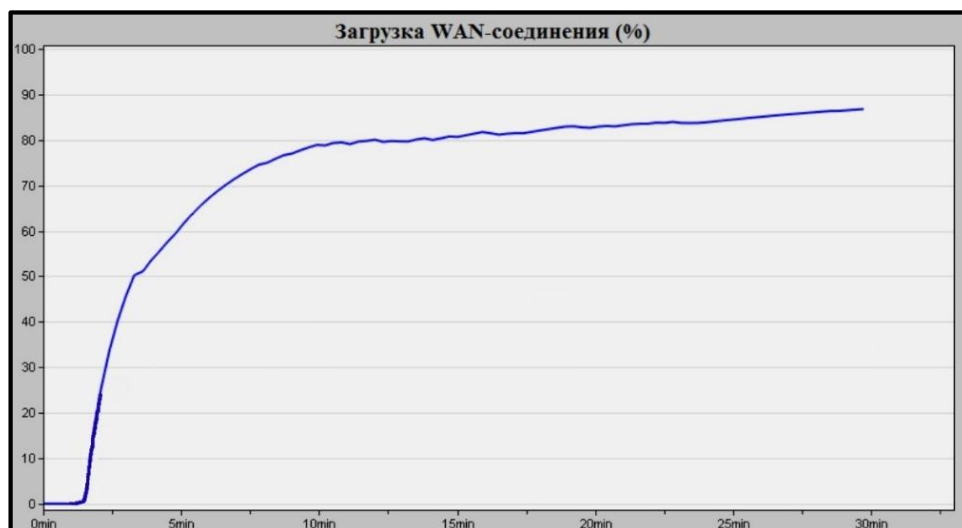


Рисунок 3.7 – Загрузка WAN-соединения

На рисунке 3.7 показано, что на десятой минуте моделирования (когда большинство пользователей начинают работать с сетью Интернет) нагрузка на WAN-соединение увеличивается до 80% и продолжает расти до 90%. С учетом пульсирующего характера пакетного трафика 80-90% загрузки WAN-соединения не позволит всем пользователям корпоративной мультисервисной сети получить доступ в сеть Интернет.

Загрузка соединения между зданиями 1 и 2 (линия связи между двумя SHDSL-модемами) представлена на рисунке 3.8.

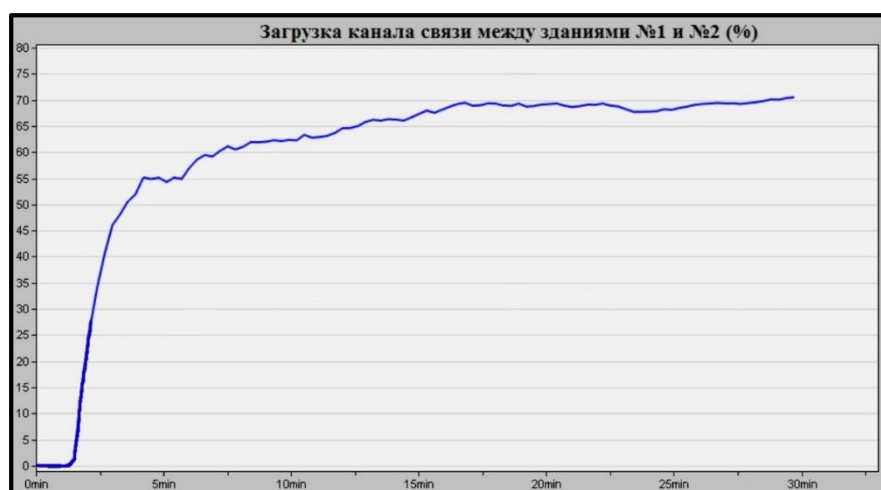


Рисунок 3.8 – Загрузка соединения между зданиями 1 и 2

Зависимость, представленная на рисунке 3.8 имеет ту же тенденцию, как и на рисунке 3.7, что можно объяснить структурой сети (ADSL-модем для доступа в сеть Интернет располагается в здании 2).

Высокая загрузка соединительных линий указывает на большое время предоставления услуг пользователям корпоративной мультисервисной сети. Для оценки времени предоставления различных услуг пользователям сети на основе имитационной модели проведена оценка времени отклика сети для следующих приложений:

- Загрузка веб-страницы (доступ в сеть Интернет);
- Электронная почта;
- Приложение баз данных;
- Работа с FTP-сервером.

Время отклика для данных типов приложений представлено на рисунках 3.9-3.12 соответственно.



Рисунок 3.9 – Среднее время отклика веб-страницы



Рисунок 3.10 – Среднее время отклика приложения электронной почты



Рисунок 3.11 – Среднее время отклика приложения базы данных



Рисунок 3.12 – Среднее время отклика приложения FTP-сервера

Таким образом, время отклика для данной группы приложений составляет единицы, десятки секунд, что для современных требований пользователей является недопустимым качеством обслуживания.

3.2 Прогноз изменения трафика на основе анализа корпоративной мультисервисной сети

На основе анализа корпоративной мультисервисной сети проведен анализ загрузки маршрутизатора в широких. Анализ загрузки маршрутизатора проводился на основе имитационной модели, при этом учитывались и оценивались следующие параметры:

- Пропускная способность канала связи;
- Скорость обслуживания кадров;
- Среднее время обслуживания кадра;
- Загрузка маршрутизатора;
- Вероятность отсутствия кадра в маршрутизаторе.

Результаты моделирования представлены в таблице 3.2.

На основе данных имитационного моделирования построены зависимости загрузки маршрутизатора корпоративной сети от пропускной способности канала связи и вероятности отсутствия кадров от пропускной способности. Полученные зависимости представлены на рисунках 3.13 и 3.14 соответственно.

Таблица 3.2 – Результаты имитационного моделирования

Пропускная способность канала связи, Мбит/с	Скорость обслуживания кадров, бит/с	Среднее время обслуживания кадра, мс	Загрузка маршрутизатора	Вероятность отсутствия кадра в маршр.
1	2,42	413,4	0,657	0,343
5	12,2	82,68	0,154	0,846
9	21,77	45,93	0,067	0,933
13	31,45	31,8	0,078	0,922
17	41,12	24,32	0,055	0,945
21	50,8	19,69	0,049	0,951
25	60,47	16,54	0,045	0,955
29	70,15	14,26	0,036	0,964
33	79,83	12,53	0,041	0,959
37	89,5	11,17	0,034	0,966
41	99,18	10,08	0,029	0,971
45	108,85	9,19	0,021	0,979
49	118,53	8,44	0,018	0,982
53	128,21	7,8	0,01	0,99
57	137,88	7,25	0,007	0,993

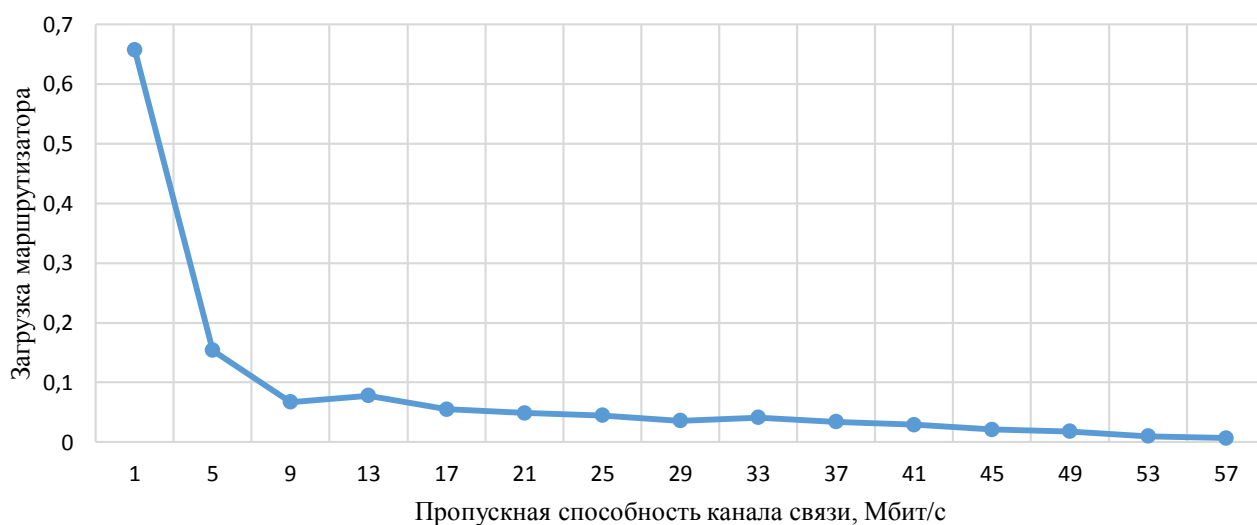


Рисунок 3.13 – Зависимость загрузки маршрутизатора от пропускной способности канала связи

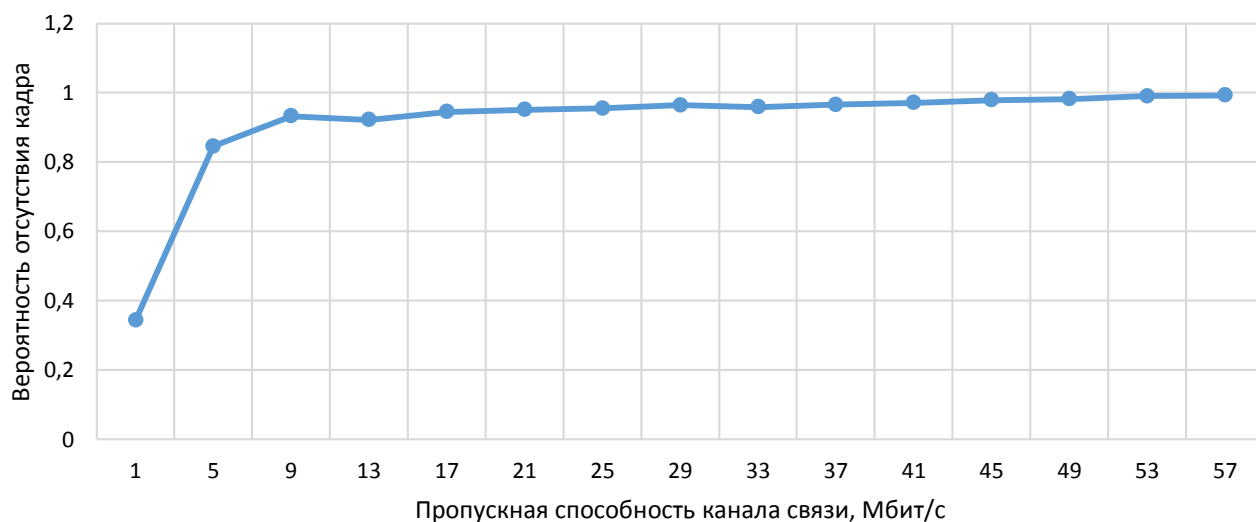


Рисунок 3.14 – Зависимость вероятности отсутствия кадра в маршрутизаторе от пропускной способности канала связи

На рисунках 3.13 и 3.14 показано, что требуемая загрузка трафика (для самоподобного трафика данный показатель не должен превышать 10-15% [17]) и соответственно вероятность отсутствия кадров в маршрутизаторе будут достигаться при пропускной способности соединительных линий между зданиями, а также между маршрутизатором и сетью Интернет равной не менее 9 Мбит/с.

Из проводных технологий доступа в сеть Интернет, наиболее рационально модернизировать сеть при помощи технологии пассивных оптических сетей доступа PON и способа доведения оптического кабеля до пользователя (FTTx).

3.3 Разработка рекомендаций по модернизации корпоративной мультисервисной сети

Для анализа применения технологии PON в имитационной модели SHDSL модемы заменены на оборудование сетей PON (модем ONT). При данном подходе пропускная способность может достигать 100 Мбит/с.

На основе имитационной модели проведена оценка параметров:

- Загрузка WAN-соединения;
- Загрузка линии связи между зданиями один и два;
- Среднее время отклика веб-страницы;

- Среднее время отклика приложения электронной почты;
- Среднее время отклика приложения базы данных;
- Среднее время отклика FTP-сервера.

Указанные параметры оценивались до модернизации сети и после модернизации. Зависимости представлены на рисунках 3.15-3.20.

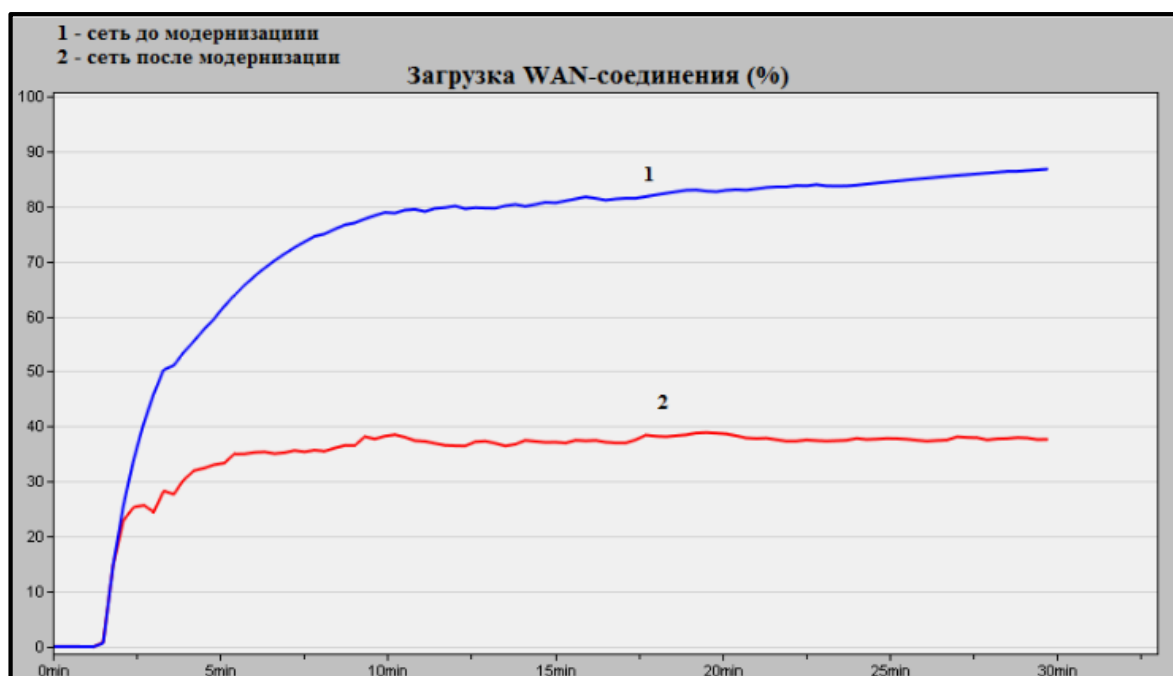


Рисунок 3.15 – Загрузка WAN-соединения

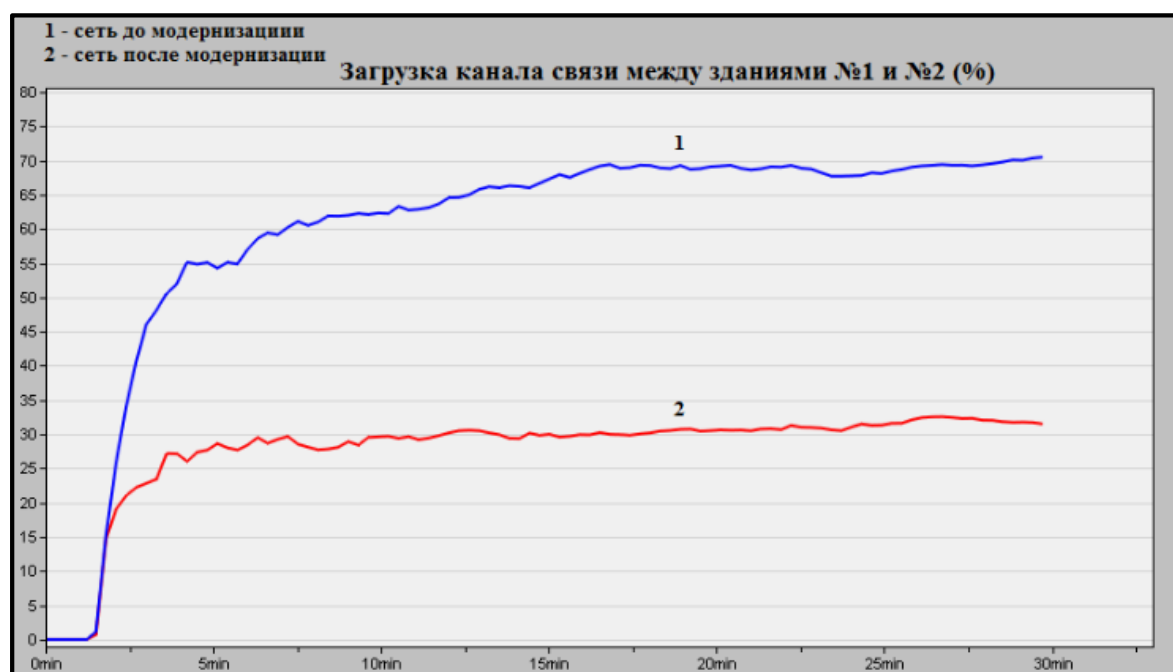


Рисунок 3.16 – Загрузка соединения между зданиями 1 и 2



Рисунок 3.17 – Среднее время отклика веб-страницы



Рисунок 3.18 – Среднее время отклика приложения электронной почты



Рисунок 3.19 – Среднее время отклика приложения базы данных



Рисунок 3.20 – Среднее время отклика приложения FTP-сервера

Модернизация сети при помощи технологий PON и FTТх позволила снизить загрузку WAN-соединения с 85% до 37% (рисунок 3.15), при этом загрузка линии связи между зданиями снизилась с 70% до 32% (рисунок 3.16).

Для услуг, предоставляемых пользователям сети, достигнуты следующие показатели:

- Среднее время отклика веб-страницы снизилось с 11,8 секунд до 1.7 секунд (рисунок 3.17);
- Среднее время отклика приложения электронной почты снизилось с 8.8 секунд до 1 секунды;
- Среднее время отклика приложений баз данных снизилось с 5 секунд до 0.55 секунды;
- Среднее время отклика FTP-сервера снижено с 13.8 секунды до 0.8 секунды.

3.4 Выводы

1. Анализ динамики трафика на основе имитационной модели мультисервисной корпоративной сети показал, что основные параметры функционирования сети (загрузка WAN-соединения, загрузка линии связи между зданиями 1 и 2) достигают 80-90%. С учетом пульсирующего характера трафика

при данной загрузке большинство пользователей сети получают отказ в обслуживании.

2. Для оценки качества предоставляемых услуг на основе имитационной модели получены значения для параметров, характеризующих качество предоставления услуг пользователям: среднее время отклика веб-страницы, среднее время отклика для приложений электронной почты, баз данных и FTP-сервера. Значения данных параметров достигают критичных значений.

3. Применение технологии пассивных оптических сетей позволило повысить пропускную способность WAN-соединения и соединений между зданиями до 100 Мбит/с, что привело к снижению загрузки WAN-соединения с 85% до 37%, загрузку линии связи между зданиями - с 70% до 32%.

ЗАКЛЮЧЕНИЕ

Анализ структуры корпоративных мультисервисных сетей показал, что она имеет трехуровневую архитектуру и строится на базе стека протоколов TCP/IP. Основными технологиями канального и физического уровня корпоративных сетей являются технологии семейства Ethernet, IEEE 802.11 (WiFi), xDSL, FTTx и PON.

Необходимость использования нескольких сервисов абонентами приводит к мультисервисной структуре пакетного трафика, имеющего пачечную структуру, что приводит к пульсирующему характеру трафика и требующего существенных запасов каналов связи по пропускной способности.

Основными характеристиками качества обслуживания абонентов являются: пропускная способность, задержка передачи пакетов, джиттер, вероятность потери пакетов и вероятность приема пакета с ошибкой. Классы трафика в соответствии с рекомендациями МСЭ определяются системой данных характеристик. Основной приоритет при обработке мультисервисного трафика отдается сервисам реального времени (видеосвязь, IP-телефония и др.).

Современные средства анализ трафика имеют широкий спектр функций для оценки параметров работы корпоративной сети, сбора статистики, механизмов оценки содержимого пакетов с целью обеспечения безопасности сети.

Анализ трафика корпоративной мультисервисной сети компании «Стройинвест Групп» при помощи программного обеспечения Wireshark позволил определить основные параметры ее функционирования, а также получить исходные статистические данные для последующего имитационного моделирования корпоративной мультисервисной сети в сетевом симуляторе Opnet Modeller.

При помощи программы Wireshark проведено исследование структуры трафика в соответствии со стеками протоколов UDP/IP и TCP/IP.

В третьей главе магистерской диссертации построена имитационная модель корпоративной мультисервисной сети в сетевом симуляторе Opnet Modeller и проведена оценка основных параметров ее функционирования и качества

предоставления услуг пользователям. Анализ данных имитационной модели показал, что загрузка WAN-соединения и загрузка линии связи между зданиями 1 и 2 достигают 80-90%.

Среднее время отклика для исследуемой группы приложения (веб-страницы, электронная почта, работа с базами данных и FTP-сервером) составляет единицы - десятки секунд, что для современных требований пользователей является недопустимым качеством обслуживания.

Для решения задачи обеспечения качества обслуживания пользователей предложена модернизация сети при помощи технологий FTTx и PON. Результаты модернизации оценены на основе имитационной модели в сетевом симуляторе Opnet Modeller. Таким образом, в результате модернизации корпоративной мультисервисной сети привело к снижению:

- Загрузки WAN-соединения с 85% до 37%;
- Загрузки линии связи между зданиями с 70% до 32%;
- Среднего времени отклика веб-страницы с 11,8 секунд до 1.7 секунд;
- Среднего времени отклика приложения электронной почты с 8.8 секунд до 1 секунды;
 - Среднего времени отклика приложений баз данных 5 секунд до 0.55 секунды;
- Среднего времени отклика FTP-сервера с 13.8 секунды до 0.8 секунды.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Алиев, Т. И. Основы моделирования дискретных систем / Т.И. Алиев. – СПб : СПбГУ ИТМО, 2009. – 363 с.
2. Алиев, Т. И. Сети ЭВМ и телекоммуникации / Т. И. Алиев. – СПб : СПбГУ ИТМО, 2011. – 400 с.
3. Бакланов, И. Г. NGN : принципы построения и организации / И. Г. Бакланов; под ред. Ю. Н. Чернышова. – М. : Эко - Трендз, 2008. – 400 с.
4. Буров, А. А. Исследование влияния методов маршрутизации на качество обслуживания в мультисервисных сетях связи, функционирующих в экстремальных условиях : автореф. дис. ... канд. техн. наук : 05.12.13 / А. А. Буров; Сибирский гос. ун-т телекоммуникаций и информатики. – Новосибирск, 2009. – 23 с.
5. Васильев, К. К. Математическое моделирование систем связи : учеб. пособие / К. К. Васильев, М. Н. Служивый. – Ульяновск : УлГТУ, 2008. – 169 с.
6. Вегешна, Ш. Качество обслуживания в сетях IP / Ш. Вегешна. – М. : Изд. дом «Вильямс», 2003. – 368 с.
7. Гладцын, В. А. Средства моделирования вычислительных сетей : учеб. пособие / В. А. Гладцын, В. В. Яновский. – СПб. : Изд. СПбГЭТУ «ЛЭТИ», 2001. – 128 с.
8. Гольдштейн, Б. С. IP-телефония / Б. С. Гольдштейн, А. В. Пинчук, А. Л. Суховицкий. – М. : Радио и связь, 2001. – 336с.
9. Гончаров, А. А. Исследование условий обеспечения гарантированного качества обслуживания в сети Интернет : автореф. дис. ... канд. техн. наук : 05.12.13 / А. А. Гончаров ; Моск. физ.-техн. ин-т. – М., 2007. – 22 с.
10. Городецкий, А. Я. Информатика. Фрактальные процессы в компьютерных сетях : учеб. пособие / А. Я. Городецкий, В. С. Заборовский. – СПб. : СПбГТУ, 2000. – 102 с.

11. Гургенидзе, А. Т. Мультисервисные сети и услуги широкополосного доступа / А. Т. Гургенидзе, В. И. Кореш. – М. : Наука и техника, 2003. – 390 с.
12. Крылов, В. В. Теория телетрафика и ее приложения / В. В. Крылов. – СПб. : БХВ-СПб., 2005. – 288 с.
13. Куроуз, Дж. Компьютерные сети / Дж. Куроуз, К. Росс. – 2-е изд. – СПб. : Питер, 2004. – 765 с.
14. Кучерявый, А. Е. Пакетная сеть связи общего пользования / А. Е. Кучерявый, Л. З. Гильченко, А. Ю. Иванов. – СПб. : Наука и техника, 2004. – 272 с.
15. Лившиц, Б. С. Теория телетрафика / Б. С. Лившиц, А. П. Пшеничников, А. Д. Харкевич. – М. : Связь, 1979. – 224 с.
16. Меликов, А. З. Телетрафик : модели методы, оптимизация / А. З. Меликов, Л. А. Пономаренко, В. В. Паладюк. – Киев : Политехника, 2007. – 256 с.
17. Никитюк, Л. А. Элементы синтеза и анализа телекоммуникационных сетей : учеб. пособие / Л. А. Никитюк. – Одесса : УГАС им. А. С. Попова, 2000. – 44 с.
18. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы: учебник / В. Г. Олифер, Н. А. Олифер. – 5-е изд. – СПб. : Питер, 2015. – 992 с.
19. Осин, А. В. Влияние самоподобности речевого трафика на качество обслуживания в телекоммуникационных сетях : автореф. дис. ... канд. техн. наук : 05.12.13 / А. В. Осин ; Моск. гос. ун-т сервиса – М., 2005. – 20 с.
20. Основные рекомендации в телефонной коммутации и сигнализации : Рекомендация Q.9. – Женева : МСЭ, 2005. – 26 с.
21. Паничев, В. В. Компьютерное моделирование / В. В. Паничев, Н. А. Соловьев. – Оренбург : ГОУ ОГУ, 2008. – 130 с.
22. Петров, В. В. Структура телетрафика и алгоритм обеспечения качества обслуживания при влиянии эффекта самоподобия : дис. ... канд. техн. наук: 05.12.13 / В. В. Петров. – М., 2004. – 198 с.

23. Рвачева, Н. В. Методика моделирования для трафика данных пропускной способности телекоммуникационной сети / Н. В. Рвачева // Системы обработки информации. – 2010. – № 1(82). – С. 123–133.
24. Самарский, А. А. Математическое моделирование. Идеи. Методы. Примеры / А. А. Самарский, А. П. Михайлов. – 2-е изд. – М. : ФИЗМАТЛИТ, 2005. – 320 с.
25. Степанов, С. Н. Основы телетрафика мультисервисных сетей / С. Н. Степанов. – М. : Эко-Трендз, 2010. – 392 с.
26. Столингс, В. Современные компьютерные сети / В. Столингс. – СПб. : Питер, 2003. – 783 с.
27. Сухов, А. М. Научные основы анализа качества интернет трафика : автореф. дис. ... докт. техн. наук : 05.13.13 / А. М. Сухов ; Самарский гос. аэрокосм. ун-т им. академика С. П. Королева – Самара, 2007. – 35 с.
28. Таненбаум, Э. Архитектура компьютера / Э. Таненбаум. – 6-е изд. – СПб. : Питер, 2016. – 816 с.
29. Таненбаум, Э. Современные операционные системы / Э. Таненбаум. – 3-е изд. – СПб. : Питер, 2011. – 1120 с.
30. Танненбаум, Э. Компьютерные сети / Э. Таненбаум. – 5-е изд. – СПб. : Питер, 2012. – 960 с.
31. Требования к сетевым показателям качества для служб, основанных на протоколе IP : Рекомендация Y.1541. – Женева : МСЭ, 2006. – 16 с.
32. Филимонов, А. Ю. Построение мультисервисных сетей Ethernet / А. Ю. Филимонов. – СПб. : БХВ-Петербург, 2007. – 592 с.
33. Цыбаков, Б. С. Модель телетрафика на основе самоподобного случайного процесса / Б. С. Цыбаков // Радиотехника. – 1999. – № 5. – С. 24-31.

34. Шелухин, О. И. Моделирование информационных систем : учеб. пособие / О. И. Шелухин, А. М. Тенякшев, А. В. Осин; под ред. О. И. Шелухина. – М. : Радиотехника, 2005. – 368 с.