

Министерство образования и науки Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н. Г. ЧЕРНЫШЕВСКОГО»

Кафедра математической
кибернетики и компьютерных наук

АНАЛИЗ СТРЕССОУСТОЙЧИВОСТИ СЕТЕВОГО ОБОРУДОВАНИЯ
АВТОРЕФЕРАТ БАКАЛАВРСКОЙ РАБОТЫ

студента 4 курса 411 группы
направления 02.03.02 — Фундаментальная информатика и информационные
технологии
факультета КНиИТ
Плодистого Петра Дмитриевича

Научный руководитель
доцент, к. ф.-м. н.

В. М. Соловьёв

Заведующий кафедрой
к. ф.-м. н.

С. В. Миронов

Саратов 2016

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	3
1 Основное содержание работы	5
ЗАКЛЮЧЕНИЕ	13
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ	14

ВВЕДЕНИЕ

Темой работы является анализ стрессоустойчивости телекоммуникационного оборудования, эта тема актуальна в связи с бурным ростом и усложнением компьютерных сетей, то есть растут не только сами сети, но и увеличивается число технологий, которое используется для управления функционированием сети.

В качестве материала для исследований выступает компьютерная сеть, а частности алгоритмы взаимодействия между узлами в этой сети, т.е. протоколы сетевого уровня.

Первостепенное значение в современной сети отдается требованиям производительности, безопасности передачи данных, отказоустойчивости и расширяемости. Нарушения любого из этих требований может повлечь за собой потерю важной информации, финансовые затраты и простои в работе, что приведет к огромным убыткам крупных компаний. Вследствие этого контроль системным администратором и обслуживающим персоналом за нормальной работой сети, без вспомогательных инструментов становится все сложнее и сложнее. На производительность сети во многом влияет используемое сетевое оборудование. Из-за этого при проектировании и расширении сети отдельное внимание уделяется подбору подходящего сетевого оборудования. К оборудованию предъявляются те же требования, что и к сети. Целью работы стало изучение возможности анализа стрессоустойчивости компьютерной сети при помощи имитационного моделирования. При проектировании сети большое внимание уделяется выбору подходящего сетевого оборудования. К оборудованию те же как и к сети предъявляются требования. Один из способов определить, отвечает ли сетевое оборудование всем этим требованиям – это анализ стрессоустойчивости оборудования. Наилучший метод, с точки зрения эффективности анализа стрессоустойчивости – это покупка экземпляра сетевого оборудования и его тестирования в конкретных условиях, но это требует больших финансовых затрат. Альтернативой является использование имитационной модели – это наименее финансово затратный метод.

Задачей при выполнении данной работы стало создание имитационной модели сети с хабом и имитационной модели коммутатора а также их тестирование на стрессоустойчивость.

Дипломная работа представлена введением, четырьмя разделами, заклю-

чением, списком использованных источников и приложением (листингом программы).

Раздел 1 представляет собой описание необходимости тестирования телекоммуникационного оборудования, на стрессоустойчивость

Раздел 2 представляет собой описание методов тестирования телекоммуникационного оборудования, на стрессоустойчивость

Раздел 3 представляет собой теоретического описание имитационной модели

Раздел 4 представляет собой практическую реализацию имитационных моделей сети, а так же тестирование их на стрессоустойчивость.

1 Основное содержание работы

Раздел 1. Анализ современного телекоммуникационного оборудования

В первой главе работы описывается положение в сфере мониторинга телекоммуникационного оборудования на текущий момент времени. В настоящее время большое внимание уделяется вопросу управления сетью, так как чем больше компьютерная сеть, тем сложнее ей управлять. На данный момент имеется огромное количество решений данной проблемы. Существуют продукты, специально разработанные для конкретных задач (например, мониторинг доступности телекоммуникационного оборудования по какому-либо протоколу), а так же есть целые комплексы программных решений по централизованному управлению сети.

У любой крупной сети есть система централизованного управления, которая имеет собственный специфичный функционал. К сожалению нет систем, выполняющих ряд функций, которые определены международными стандартами. Описание функционала для управляющей сети содержится в рекомендации ITU-T X.700 и в стандарте ISO 7498-4. В данных стандартах системы управления сетью разделены на пять функциональных групп:

- управление конфигурацией сети и именованием;
- обработка ошибок;
- анализ производительности и надежности;
- управление безопасностью;
- учет работы сети.

Первой задачей является определение конфигурацией сети (количество рабочих станций, серверов, коммутаторов и т.д.), а так же определить их сетевые адреса, идентификаторы (имена) и пр. Существуют множество программных продуктов занимающихся решением этой задачи (например: HP IMC Service Health Manager, NetK, LANState и другие). Все они используют протокол SNMP для построения карты сети.

Задача подсистемы обработки ошибок – это выявление, определение и устранение последствий сбоев в работе сети. На этом этапе выполняется сбор, фильтрация и анализ ошибок возникающих в процессе работы сети.

На практике же, как правило, производится только сбор логов с сетевого оборудования, а фильтрацией занимается системный администратор.

Система для анализа производительности и надежности, должна производить оценку накопленной статистической информации, включающую в себя такие параметры, как время реакции системы, пропускная способность реального или виртуального канала связи между двумя конечными абонентами сети, интенсивность трафика в отдельных сегментах и каналах сети, вероятность искажения данных при их передаче через сеть, а также коэффициент готовности сети или ее определенной транспортной службы.

Управление безопасностью сети включает в себя контроль целостности и отсутствие несанкционированного доступа к данным извне, при хранении и передаче. Основные службы которые выполняют эти требования – это процедуры аутентификации пользователей, назначение и проверка прав доступа к ресурсам сети, распределение и поддержка ключей шифрования, управления полномочиями и т. п.

Для учета работы сети используются приложения для регистрации различных ресурсов сети: устройств, каналов и т.п.

Описанная система управления позволит организовать работу сети. Основными принципами функционирования этой сети является мониторинг и анализ. Однако анализ надежности выполняется на основе статических данных, что не всегда удобно, так как эти данные не всегда можно собрать, потому что мы не можем заранее перевести сеть в необходимое нам состояние. Одним из решений данной проблемы является использование средств моделирования.

Раздел 2. Методы моделирования вычислительной сети

В данной главе описываются методы моделирования сети. Цель моделирования сети заключается в определении наиболее подходящей топологии для будущей сети, выбор сетевого оборудования, определение рабочих характеристик и возможная модернизации. На моделях производится тестирование сети в различных стрессовых ситуациях, таких как broadcast-шторм или воссоздать режим коллапса, что не возможно в работающей сети.

В процессе моделирования выясняются следующие параметры:

- предельные пропускные способности различных фрагментов сети и зависимости потерь пакетов от загрузки отдельных станций и внешних каналов;
- время отклика основных серверов и самых различных режимах работы;
- влияние установки новых серверов на перераспределение информационных потоков;
- решение оптимизации топологии при возникновении узких мест в сети;
- выбор того или иного типа сетевого оборудования или режима его работы;
- выбор внутреннего протокола маршрутизации и его параметров;
- определение предельно допустимого числа пользователей того или иного сервера;
- оценка необходимой полосы пропускания внешнего канала для обеспечения требуемого уровня QOS;
- оценка влияния мультимедийного трафика на работу локальной сети.

Возможны два способа моделирования сети: аналитический и симуляционный.

Аналитический метод представляет собой совокупность математических соотношений, связывающие между собой входные и выходные характеристики сети. Данный метод позволяет достаточно точно определить задержки, время передачи и время обслуживания, однако не для каждой конфигурации сети возможно построить аналитическую модель, в первую очередь это относится к сетевому оборудованию.

Симуляционное моделирование используется для выявления в системе критических элементов. Для этого типа моделирования характерно использование специализированных языков симулирования, для него

так же необходимо априорно знать относительно статические свойства системы как в целом, так и её составляющих. При данном подходе необходимо сформировать модель, затем отладить и проверить на корректность работы. Во время проверки на корректность происходит сравнение расчетных данных с экспериментальными.

Симуляционная модель представляет собой программный продукт, позволяющий имитировать события, происходящие в реальной сети: процессы генерации сообщений приложениями, задержки, связанные с обработкой сообщений, пакетов и кадров внутри операционной системы, разбиение сообщений на пакеты и кадры определенных протоколов, процесс обработки поступающих пакетов маршрутизатором, процесс получения доступа компьютером к разделяемой сетевой среде и т.д. Симуляционная модель может поддерживать эмуляцию довольно большого числа сетевого оборудования. Благодаря этому нет необходимости приобретать экземпляры сетевого оборудования. Работа этого оборудования эмулируется с помощью программных средств, они в достаточно точной мере воспроизводят особенности этого оборудования, а также учитывают его основные параметры. Также данная модель позволяет эмулировать различные стрессовые ситуации внутри сети: обрыв линии связи, выход из строя того или иного экземпляра сетевого оборудования и т.п. Еще один плюс использования симуляционной модели – это возможность ускорить происходящие события в системе. Благодаря этому за несколько минут работы программы можно воспроизвести работу сети за несколько дней или недель.

Ещё одним преимуществом имитационной модели является возможность эмулировать сети как какого-то конкретного, так и различных типов, а также объединять их. Результатом работы имитационной модели являются собранные статистические данные о наиболее важных характеристиках сети: времени реакции, коэффициенте использования каналов и узлов, вероятности потерь пакетов и т.п.

Имитационная модель является сложной структурой, состоящей из различных подмоделей: различного сетевого оборудования, различных протоколов 2-го и 3-го уровня модели OSI, сред передачи данных и т.д. Остановимся подробнее на сетевом оборудовании, а именно на мостах, коммутаторах и маршрутизаторах.

Раздел 3. Создание имитационной модели сети

При создании крупной компьютерной сети нельзя использовать одну разделяемую среду. Несмотря на использование такой скоростной технологии, как Gigabit Ethernet, невозможно это не из-за ограничения по максимально допустимому количеству узлов в разделяемой среде, а из-за используемых протоколов обмена и характера рабочей нагрузки. В сети средних размеров (около 100 узлов), работающей по одной разделяемой среде, скорее всего будут плохо передаваться данные, если она вообще будет работать.

Технологии Ethernet присущ экспоненциальный рост величины задержек доступа при увеличении коэффициента нагрузки сети. Такая сеть будет нормально работать при нагрузке до 50%, при большей нагрузке возрастает влияние коллизий, а при загрузке близкой к 100% сеть вообще перестанет работать.

Для того что-бы снизить нагрузку на сеть, а так же уменьшить влияние коллизий на передачу данных, сеть необходимо разделить на несколько сегментов. Для этого используются различные дополнительные сетевые устройства, такие как хабы, коммутаторы и маршрутизаторы.

Остановимся более подробнее на коммутаторах. Существует три основных схемы этого устройства(не редко все три технологии совмещаются в одном устройстве):

- коммутационная матрица;
- общая шина;
- разделяемая многовходовая память.

Для исследования характеристик коммутаторов при асинхронной внешней нагрузке существует имитационная модель коммутатора. модель коммутатора . В состав данной модели входят следующие подмодели:

- модель рабочей нагрузки;
- модель блока генерации пакетов;
- модель управления передачей пакетов;
- модель блока буферизации пакетов;
- модель коммутационной матрицы.

Модель рабочей нагрузки предназначена для имитации процесса поступления пакетов, передаваемых в другой сегмент сети. Нагрузка на каждый порт имитируется собственным независимым источником требований. Для преоб-

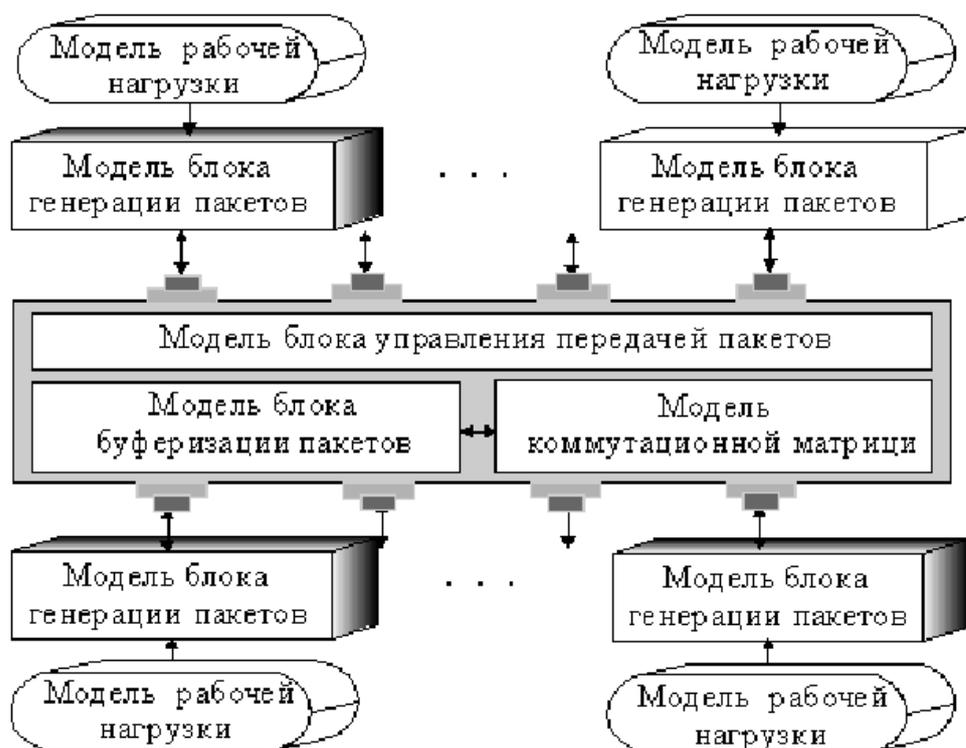


Рисунок 1 – Схема имитационной модели коммутатора

разования требований в пакеты используются стандартные механизмы упаковки требований в пакеты. Дальнейшая их транспортировка осуществляется согласно правилам передачи кадров в моделях сетей пакетной коммутации. При этом модель рабочей нагрузки обеспечивает имитацию нагрузки на все порты, модель блока генерации пакетов – преобразование исходной заявки в множество кадров, используемых для транспортировки исходного сообщения.

Модели компонентов механизма управления коммутацией предназначены для моделирования аппаратных задержек, возникающих при обмене данными между портами коммутатора. В эту группу входят модель управления передачей пакетов, модель блока буферизации пакетов и модель коммутационной матрицы. По сути, эти подмодели имитируют работу коммутатора. При этом модель управления передачей пакетов предназначена для имитации процессов обмена информацией между входным и выходным портами. Модель буферизации пакетов предназначена для проверки доступности выходного порта и записи пакета в промежуточный буфер в случае его занятости. При освобождении последнего с помощью механизмов управления моделируется процесс передачи пакета из буфера в соответствующий выходной порт. Имитация транзитной задержки выполняется с помощью модели коммутационной матрицы.

Раздел 4. Реализация моделей сети

Данный раздел состоит из двух частей, в первой описывается метод коллективного доступа с опознаванием несущей и обнаружением коллизий, создано приложение реализующее эту модель, а так же представлено тестирование и сравнение полученных данных с практическими результатами.

Входными данными для приложения являются количество устройств в сети и размер пакета при передаче данных. Результатом работы программы является время передачи данных каждым хостом и общее число потерянных пакетов и общее число коллизий.

Тесты модели показали, что при увеличении размера кадра в сети увеличивается количество коллизий и потерянных пакетов, что в реальной сети может привести к сбоям в работе сети или к её неработоспособности.

Также были проведены тесты по выявлению зависимости задержек в сети (количества коллизий и количества потерянных пакетов) от числа хостов в сети. Данный график подтверждает практические наблюдения, что количество задержек в сети возрастает экспоненциально при увеличении числа узлов в сети.

Во второй части работы описана реализация имитационной модели коммутатора. Процесс работы заключается в передаче данных между всеми портами устройства. Входными данными являются число портов и узлов, подключенных к коммутатору, скорость портов коммутатора. Результатом работы приложения являются времена передачи данных для каждого порта коммутатора.

Эксперименты показали, что модель коммутатора и модель сети на основе хабов будут работать одинаково при малых и средних нагрузках, однако при достижении определенного числа хостов (около 40) модель коммутатора сохраняет свою работоспособность, в то время как в модели сети с хабом появляется значительное количество коллизий, значительно снижающих пропускную способность сети.

Использование имитационной модели может показать лишь то, как будут передаваться данные в сети при той или иной топологии и при заданном объеме передаваемого трафика. Но при прогнозировании поведения сетевого оборудования она мало чем поможет. Например, при широковещательном шторме любая имитационная модель покажет прохождение трафика через се-

твое оборудование с той или иной задержкой. Но ни одна подобная модель не покажет, что при длительных штормах могут подвисать модемы из-за перегрева, на маршрутизаторах может произойти полная загрузка процессора и в результате возможна перезагрузка контроллера E1. Это приведет к потере связи с роутером и невозможности функционирования некоторого сегмента сети, что возможны большие проблемы с передачей информации из-за невозможности нормальной синхронизации маршрутизаторов с мультиплексорами и т.д. Также невозможно программно смоделировать ситуацию с повреждением линии связи, когда связь полностью не пропадает, а на сетевых интерфейсах оборудования начинают понемногу накапливаться ошибки. Используя только имитационную модель, практически невозможно предсказать поведение оборудования в критических ситуациях.

Так что поведение оборудования во многих ситуациях предсказать практически невозможно, используя только имитационную модель.

ЗАКЛЮЧЕНИЕ

Основной целью работы явилось изучение методов анализа телекоммуникационного оборудования. В данной работе были выполнены следующие задачи:

- рассмотрены методы анализа стрессоустойчивости телекоммуникационного оборудования;
- изучены методы построения моделей сетей;
- построены имитационные модели сетей;
- был проведен анализ их стрессоустойчивости.

Разработанные в ходе работы модели могут быть использованы для анализа того, как могут передаваться данные в сети при той или иной топологии и при заданном объёме передаваемого трафика.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

- 1 *Кларк, К.* Принципы коммутации в локальных сетях CISCO / К. Кларк. — Москва: Вильямс, 2003.
- 2 *Семишин, Ю. А.* Оценка эффективности atm-коммутаторов методом имитационного моделирования / Ю. А. Семишин, Ю. Г. Майба, О. В. Литвинова // *Технология и конструирование в электронной аппаратуре*. — 2000. — no. 4.
- 3 *Коровин, А.* МОДЕЛИРОВАНИЕ СИСТЕМ / А. Коровин. — Челябинск: Издательский центр ЮУрГУ, 2010.
- 4 Сетевое моделирование [Электронный ресурс]. — URL: <http://citforum.ru/nets/semenov/4/45/modl4517.shtml> (Дата обращения - 28.05.2016). Загл. с экр. Яз. англ.
- 5 *Быков, А. Ю.* Имитационное моделирование с применением библиотеки классов языка java, разработанной для «облачных» сервисов / А. Ю. Быков, Ф. А. Панфилов, О. О. Сумарокова // *Вестник МГТУ им. Н.Э. Баумана: электронное издание*. — 2013.
- 6 *Бабина, О.* Сравнительный анализ имитационных и аналитических моделей / О. Бабина // *ИММОД*. — 2009. — С. 73–77.
- 7 Особенности коммутаторов локальных сетей [Электронный ресурс]. — URL: http://citforum.ru/nets/lsook/glava_7.shtml (Дата обращения - 27.05.2016). Загл. с экр. Яз. англ.
- 8 *Kim, Y.* A performance analysis of integrated social-sensor networking service with usn / Y. Kim, J. Hwang, D. Park // *Innovations and Advanced Techniques in Systems, Computing Sciences and Software Engineering*. — 2008. — Vol. 42. — Pp. 538–549.
- 9 Метод доступа CSMA/CD [Электронный ресурс]. — URL: http://citforum.ru/nets/protocols2/2_04_01.shtml (Дата обращения - 15.05.2016). Загл. с экр. Яз. англ.