Представление лояльности при помощи вероятности позволит произвести прогноз о возможных реакциях клиента при совершении со стороны компании-оператора определенного воздействия. Кроме того, данная форма оценки лояльности позволит, используя личностные характеристики клиента, количественно оценить его поведение, приравняв к нему некоторую вероятность ответной реакции клиента на воздействие. Например, как изменится лояльность клиента, если компания-оператор снизит цену на исходящие звонки. В результате анализа клиент может дать некоторую вероятность, например, равную 0,6; которая будет свидетельствовать о том, что с вероятностью 60% клиент будет больше совершать звонков. В дополнении к вероятностному подходу может быть использован фактор доходности, на основании которого можно сделать выводы о возможных будущих платежах клиента, подтверждая это заключение вероятностью. Например, после анализа некоторого клиента было получено, что с вероятностью 0,4 клиент будет платить 50 условных единиц в месяц, что позволит его отнести к определенной категории по внутренней шкале лояльности компании. Подобный анализ, основанный на вероятностных заключениях, также позволит компаниям на основе данных своих абонентов прогнозировать лояльность вновь подключаемых клиентов и определять их в некоторые маркетинговые сегменты.

Литература

1. Мазитов Ю.И, Пуха Ю.В. Инновации в CRM: вызовы времени и выгоды реализации. // Вестник связи. №3, 2005. – С. 32-35.
2. Технология DM и CRM-системы: синергический эффект [Электронный ресурс]. Режим доступа: http://www.snowcactus.ru/crm.htm, свободный. – Загл. с экрана.
3. Особенности маркетинга в телекоммуникациях [Электронный ресурс]. Режим доступа: http://www.nii-ecos.ru/?a=23, свободный. – Загл. с экрана.
4. Системы планирования ресурсов предприятия ERP. [Электронный ресурс]. Режим доступа: http://erpnews.ru/doc1596. html, свободный. – Загл. с экрана.
5. Павлюков Ю.А. Сбор и предобработка CDR в биллинговых системах [Электронный ресурс] // Биллинг. Компьютерная телефония. 2003. № 04. Режим доступа: http://www.cti-online.ru/library_reg.shtml, свободный. – Загл. с экрана.
6. Некрасов В. Мобильный OLAP [Электронный ресурс] // Открытые системы. 2003. № 05. Режим доступа: http://www.osp.ru/os/2003/05/183051/, свободный. – Загл. с экрана.
7. Дюк В., Самойленко А. Data Mining. Учебный курс. СПб.: Питер, 2001. – 368 с.
8. Data Mining в телекоммуникациях [Электронный ресурс]. Режим доступа: http:// www.megaputer.ru, свободный. – Загл. с экрана.

ТЕХНОЛОГИИ КОМПЬЮТЕРНЫХ СИСТЕМ И СЕТЕЙ

УДК 004.421

ПРОГРАММНАЯ СИСТЕМА РАСПОЗНАВАНИЯ ТРАФИКА И ПРОГНОЗИРОВАНИЯ ХАРАКТЕРИСТИК МУЛЬТИСЕРВИСНОЙ СЕТИ

Бахарева Н.Ф., Ушаков Ю.А.

В статье описывается программная система распознавания и анализа трафика, которая позволяет отделять потоки приложений друг от друга, автоматически определять их статистические характеристики. Эти характеристики используются для прогнозирования основных показателей качества сети.

Введение

Современная тенденция развития сетей передачи данных подразумевает собой конвергенцию данных, голоса, видео и учетно-контрольных потоков под единой средой передачи данных IP или ATM. Объединение всех удаленных офисов какой либо фирмы теперь включает в себя единую систему нумерации телефонии, использование каналов передачи данных и общего сетевого оборудования для объединения АТС и унификации предоставления голосовых услуг предприятия. Единое адресное пространство, наличие нескольких физических и логических резервных каналов передачи данных, резервирование центров обработки и конвергенции данных, а также все возрастающие нагрузки на ядро сети и серверные узлы делает как никогда актуальным вопрос адекватного и обоснованного проектирования такой сети. При анализе сложных сетевых структур в большинстве случаев применяют классический подход с использованием пуассоновских потоков заявок и экспоненци-

альное распределение времени обработки заявки. Однако в большинстве случаев сложных высоконагруженных сетей такой подход дает лишь очень приближенный результат. Поэтому для повышения адекватности модели сети, уточнения входных характеристик для моделирования необходимо четко отделять различные классы потоков трафика друг от друга. Кроме того, делать это необходимо с учетом постоянно изменяющегося характера трафика, его периодичности, «часов пик» и т.д.

Постановка задачи и пути ее решения

Все программные компоненты, которые используются в мультисервисных и конвергентных сетях можно условно разделить на две группы:

- компоненты функционального программного обеспечения;
- компоненты технологического программного обеспечения.

Функциональное ПО используется для формирования и приема мультисервисных потоков. Технологическое ПО используется для выполнения разнообразных служебных функций. Это комплекс инструментов, обеспечивающих выполнение вспомогательных задач, возникающих в процессе управления мультисервисными ЛВС. К этим задачам можно отнести:

- сбор и предоставление оперативной информации о состоянии компонентов сети, нагрузке на компоненты и прогноз на загрузку;
- мониторинг и управление информационными потоками мультисервисной ЛВС и КСПД.

Анализ трафика, передаваемого в СПД, предоставляет возможность решения этих задач. Кроме того, учет и анализ трафика позволяет обеспечивать безопасность информационного обмена, определять узкие места и локализовать неисправности, тарифицировать абонентов. Опять же, помогает осуществлять управление качеством предоставления услуг.

Основной целью обеспечения высокого качества обслуживания конвергентной сети является критичность голосового и видеотрафика к любым задержкам и требовательность к выделенной полосе пропускания. После выявления требований к какому-либо сегменту сети (количество одновременных вызовов, сетевые приложения, время отклика) необходимо проанализировать возможности оборудования и существующую ситуацию. В ряде случаев это приходится делать уже на существующем сегменте сети. Чтобы выявить основные тенденции трафика, его пики, пики конкретных приложений, возможности конкретных типов трафика взаимодействовать с различными политиками и типами QoS необходимо произвести следующие действия [2].

1. Разделить логические потоки трафика, хост-хост и приложение-приложение.
2. Определить вероятностные характеристики каждого логического потока для последующего анализа.
3. Определить суточные, часовые и иные циклы периодичности в поведении трафика.

Самым важным является определение вероятностных характеристик. Без них невозможно проводить моделирование сегмента сети для получения стресс-характеристик по каждому приложению и не будет возможности предсказать параметры производительности, время отклика приложения и стабильность этих параметров во времени.

Определение вероятностных характеристик реального трафика сталкивается со многими проблемами. Любая методика тестирования существующей сети существенно зависит от имеющихся в распоряжении системного администратора технических и программных средств. В большинстве случаев для обнаружения дефектов сети и анализа существующего трафика достаточным средством является анализатор сетевых протоколов. Он может быть аппаратным и программным, выделенным и встроенным, универсальным и узконастроенным [2].

Например, у фирмы Network Instruments существует целая серия аппаратно-программных комплексов для анализа трафика.

Рис. 1. Пример подключения зонда «GigaTrunk Probe Appliance» фирмы Network Instruments

Вид результатов работы зонда показан на рис. 2.

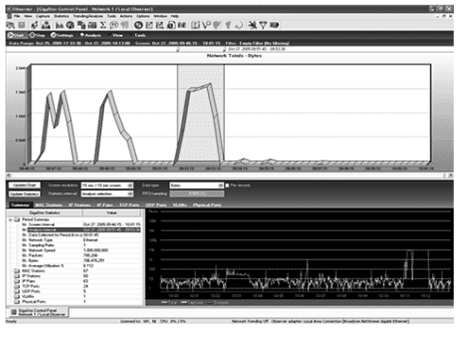

Рис. 2. Результаты работы зонда «GigaTrunk Probe Appliance»

Основной недостаток данного подхода заключается в том, что информация, полученная таким путем, имеет внутреннее хранение в зонде или на внешнем хранилище в закрытом виде. Нет прямого автоматизированного доступа к этому хранилищу. Второй недостаток – это ненадежность. Как только какая-либо часть устройства выйдет из строя, весь сегмент сети окажется отрезанным от общей сети.

Другой способ использования зонда – в порт RMON или порт зеркалирования – иллюстрирует рис. 3. Такой подход более требователен к коммутационному оборудованию, но оказывает меньшее влияние на производительность и надежность сети.

Основным недостатком аппаратных зондов, на сегодняшний день является высокая цена модуля и низкая доступность в России.

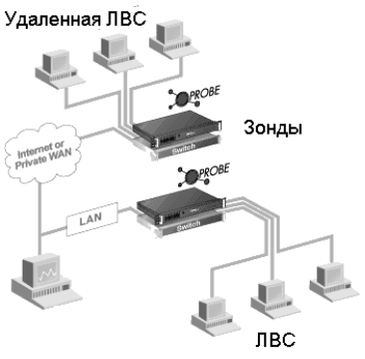

Рис. 3. Пример подключения зонда «10/100/1000 Probe Appliance»

Анализаторы не только трафика, но и содержания трафика выпускаются и в чисто программном исполнении. Недостаточная универсальность компенсируется широчайшим спектром возможностей. Съемом данных может заниматься обычный персональный компьютер, подключенный в роли аппаратного зонда, или сетевое устройство по протоколу NetFlow/SFlow/RMON, а информацию интерпретировать будет специальное программное обеспечение.

Также можно использовать встроенные средства маршрутизаторов и операционных систем клиентов, такие как IpFilter, NetFlow, IPfw и т.д. Все анализаторы делятся на анализаторы реального времени и стековые, а также программные и аппаратно-программные.

Стековые анализаторы используются для детального анализа сохраненного трафика. В файл записывается вся информация, начиная от второго уровня OSI, которая собиралась с определенных точек сети. Преимущество таких анализаторов состоит в возможности одновременного анализа данных со всех контрольных точек сети без использования пропускной способности сети в служебных целях. Информация накапливается в полном объеме и всегда можно посмотреть детали конкретного соединения или пакета.

Анализаторы реального времени работают по особому принципу. Все пакеты с точки сохраняются в кеш памяти, затем производится анализ очереди кеша в реальном времени. То есть после анализа пакета из него сохраняются все скелетные данные, производится анализ уровня 7, и, если требуется, то сохраняется и он. После этого, в зависимости от поставленной задачи и выполняемой функции, данные передаются в модуль математической, статистической, протокольной обработки, где выполняется необходимый анализ.

Аппаратные анализаторы намного лучше справляются с анализом потоков высокоскоростных соединений, имеют функции диагностики 1-2 уровней OSI, могут использоваться автономно в любом месте сети, имеют стандартизированный интерфейс управления и, главное, являются инструментом, который работает независимо от используемых технологий, операционных систем, программ и т.д. Но основным недостатком таких комплексов является очень высокая стоимость.

Активный анализ сети

Для выявления ошибок от канального уровня до уровня приложения измерения необходимо проводить на фоне генерации анализатором протоколов собственного трафика. Генерация трафика позволяет обострить имеющиеся проблемы и создает условия для их проявления. Генерация должна быть управляемой по интенсивности и закону распределения.

Этот метод называется «стресс-тестирование» сети и позволяет довольно быстро на реальном сегменте определить его предельные характеристики и возможности. Данный подход является самым универсальным, потому как используется метод планирования эксперимента на реальном оборудовании. Весь эксперимент будет занимать несколько минут. Будут определены все основные параметры оборудования и каналов связи в требуемых режимах и с требуемыми типами трафика.

Основным недостатком метода стресс-тестирования является его стоимость (аренда анализаторов протоколов, изоляция сегмента на некоторое время, интерпретация результатов) а, также, большая зависимость измерений от корректной настройки оборудования, главным образом служб

QoS. Ведь если QoS не настроен, то голосовой трафик будет передаваться по общему каналу без приоритетов, и при больших загрузках будут возникать большие задержки.

Другой способ определить показатели производительности сети связан с использованием технологии NetFlow компании Cisco Systems. Технология NetFlow – это программная опция доступная в активном оборудовании Cisco, с помощью которой можно собирать и получать статистику по потокам данных, проходящих через оборудование Cisco.

Технология NetFlow была создана изначально для повышения скорости коммутации пакетов и производительности маршрутизаторов. Позже в NetFlow была реализована возможность сбора статистики, которая полезна для анализа сетевого трафика. Маршрутизатор экспортирует NetFlow данные, отправляя UDP пакеты, содержащие статистику по потокам, на один или несколько коллекторов (сборщиков данной информации) как показано на рис. 2, например, ReporterAnalayzer от Fluke Networks или Observer от Network Instruments. Каждый пакет, проходящий через устройство, может быть проанализирован. На основе этого анализа может быть получена точная информация о потоке.

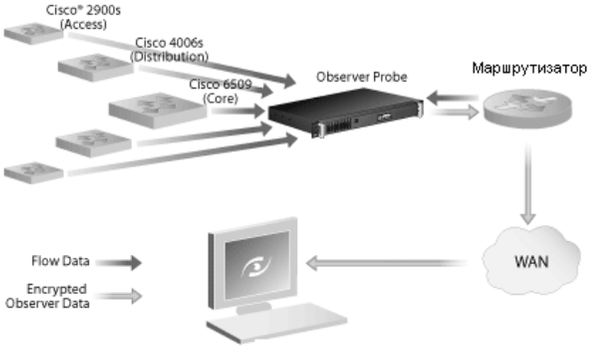

Рис. 4. Подключение потоков Netflow

Конкурирующая технология SFlow имеет схожие возможности. Протокол SFlow был специально разработан для продолжительного, охватывающего всю сеть, мониторинга коммутируемых потоков уровней со 2-го по 7-й OSI высокой степени интенсивности. SFlow функционирует, отслеживая состояние точных интерфейсных счетчиков и статистические выборки решений о пересылке пакетов, производимых коммутатором. Оба типа информации немедленно пересылаются на центральный коллектор-сборщик первичных данных (таких, как InMon Traffic Server или сетевой агент LANBilling SFlow), который производит их анализ. Результатом является детализированная информация о потоках данных уровня приложений. Статистические выборки протокола SFlow – пакетно-ориентированный метод отбора экземпляров. В среднем один пакет из N отбирается из потока и пересылается для последующего анализа. Элемент хаотичности введен в процесс отбора, чтобы предотвратить синхронизацию с любой периодической составляющей трафика. Метод отбора образцов (sampling) не обеспечивает стопроцентной точности результата, но он обеспечивает результат, в котором ошибка может быть точно охарактеризована.

Интеграция этих двух методов с локальным стресс-тестированием каждого направления потоков трафика, при котором на несколько секунд происходит эмуляция реальной активности пользователей, позволяет довольно точно, быстро и без больших затрат выявить основные характеристики оборудования и каналов связи.

Активный мониторинг приложений

Технологии NetFlow и SFlow являются аппаратно-ориентированными технологиями. То есть сетевое устройство, коммутатор или маршрутизатор, должны поддерживать требуемый протокол. Оба протокола поддерживаются только в оборудовании среднего и высшего ценового уровня, что отрицательно сказывается на их распространенности.

Следующий метод анализа и оптимизации сетевой инфраструктуры – это системы мониторинга ИТ-инфраструктуры. Самым распространенным решением в этой области является SuperAgent от Fluke Networks – решение для мониторинга за производительностью и текущим состоянием ИТ – инфраструктуры, поиска и устранения неисправностей в работе сети на ранней стадии. Позволяет выявлять источники задержек и «тормозов» в работе сетевых ресурсов без установки дополнительных агентов или мониторов на рабочие станции пользователей или серверы или устройств диагностики с клиентской стороны. SuperAgent это система управления качеством ИТ-услуг. Данное решение позволяет обеспечить четкую и однозначную взаимосвязь между техническими параметрами ИТ-инфраструктуры и количественными метриками ИТ-услуг. SuperAgent автоматизирует процесс мониторинга за работой приложений и обеспечивает сбор и накопление долговременной статистики по работе сети, используемых приложений и серверов с целью выявления негативных тенденций в их работе, что позволяет ИТ – специалистам быстро выявлять и изолировать возникающие проблемы с произ-

водительностью ИТ – инфраструктуры. Однако цена вопроса – более $ 60000.

Моделирование трафика

После получения, каким-либо образом, суммарных данных о трафике в виде отдельных заголовков пакетов, необходимо выделить отдельные потоки (клиент-сервер, приложение-приложение, АТС-АТС и т.д.). Для планирования активного эксперимента (стресс-тестирования или комбинации его с потоками Netflow/Sflow) необходимо знать вероятностные характеристики каждого из потоков, и, в первую очередь, вид распределения. Если речь идет о внедрении голосовых услуг или перевода коннективности АТС на VoIP поток, то голосового трафика может и не быть в общем потоке. Тогда необходимо задать его вручную.

При построении голосового потока необходимо учесть несколько факторов. Во-первых, размер потока (бит/с) в реальности не совпадает с указанным потоком для выбранного кодека. В таблице 1 показаны реальные потоки для 1 соединения.

Таблица 1. Параметры потока VoIP трафика

Кодек	Размер сегмента	Полоса пропускания	Полоса пропускания со сжатием	Количество одновременных звонков на 512кбит/с (без/с сжатием)
G.711 (64 kbps)	160	83	68	6/7
G.726 (32 kbps)	60	57	36	8/14
G.726 (24 kbps)	40	52	29	9/17
G.728 (16 kbps)	40	35	19	14/26
G.729 (8 kbps)	20	26	11	19/46
G.723 (6.3 kbps)	24	18	8	28/64
G.723 (5.3 kbps)	20	17	7	30/73

Это происходит из-за добавления заголовков (IP, UDP, Ethernet). Во-вторых, при использовании голосовых потоков, активное оборудование (маршрутизаторы, коммутаторы) обязаны поддерживать QoS. Для голосового трафика, как правило, выделяется отдельный VLAN, приоритет для этого трафика ставится наивысший. И, кроме того, часто существует возможность проброса голосовых соединений сквозь обычную телефонную сеть при исчерпании возможностей канала связи (рис. 5).

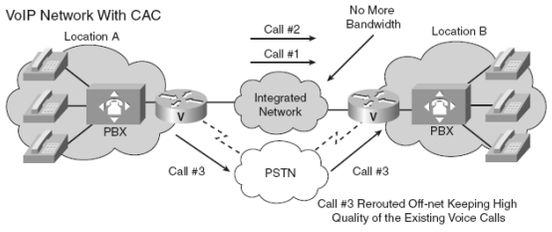

Рис. 5. Дополнительный канал голосовой связи

В-третьих, даже если в маршрутизаторе установлен и настроен QoS, даже если какие-либо приложения уже используют приоритеты в предоставлении канала связи, голосовой трафик всегда идет вперед (рис. 6).

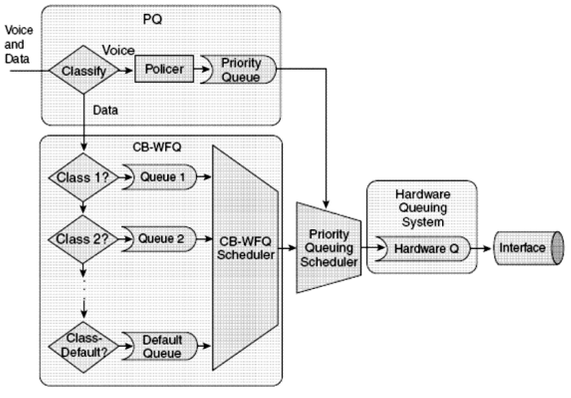

Рис.6. Дополнительная приоритезация голосового трафика

Однако даже если учесть все вышеперечисленное, если в сети используются устройства типа Intrusion Prevention System (устройства предотвращения вторжения, IPS), то весь смысл стресс-тестирования пропадает – IPS заблокирует любую чрезвычайную или нетипичную активность узлов. Зато IPS практически не вносит задержек в распространение пакетов, поэтому его всегда можно просто временно изъять из схемы.

При обмене большими пакетами между маршрутизаторами, чтобы не ожидать окончания передачи большого объема данных, голосовой пакет может быть помещен в середину пакета данных, а на удаленном роутере изъят оттуда и отправлен по назначению.

На оборудовании Cisco Systems существует специальный сервис под названием AutoQoS. Он позволяет автоматически распознать голосовой трафик в общем потоке, выделить под него отдельный VLAN и настроить оптимальный механизм

QoS для существующих каналов и скоростей каналов. Обязательным условием является корректное определение ширины канала или задание его пропускной способности вручную.

Расположение программных сенсоров

Еще одним важным параметром для корректного снятия информации о трафике является расположение сенсоров, чувствительных к трафику.

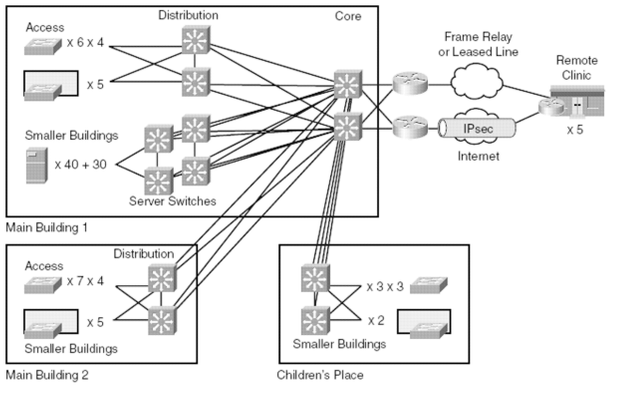

Рис. 7. Типовая сеть среднего предприятия с кампусом и удаленными офисами

На рис. 7 показана типовая сеть с резервным ядром сети, несколькими выносами сети (удаленные корпуса) и удаленными офисами, подключающимися через провайдеров VPN по выделенной линии или через Интернет.

Допустим, стоит задача внедрить в существующий удаленный офис телефонию, включенную в единый план нумерации предприятия, предоставления таких голосовых услуг как голосовые почтовые ящики, автосекретарь, автоперенаправление, конференц-связь. Все услуги предоставляются только в головном офисе на выделенном оборудовании.

Необходимо определить возможности существующей СПД по количеству одновременных голосовых соединений, по возможности одновременной конференц-связи и транзиту услуг из головного офиса в удаленное подразделение.

Для этого, во-первых, необходимо активировать службу AutoQoS на оборудовании, корректно задать реальную ширину каждого WAN канала связи.

Во-вторых, выбрать точку генерации трафика и точку анализа. С генерацией все понятно, точка генерации должна находиться как можно ближе к месту установки и подключения УАТС. С анализом менее понятно.

Для начала точку анализа устанавливают непосредственно на устройстве, агрегирующем все потоки голоса от АТС. Обычно это, так называемый, SoftSwitch (программный коммутатор) или GateKeeper (голосовой шлюз). В случае гетерогенности сети обычно имеет место первый вариант (рис. 8).

Так как в ЛВС чаще всего используется избыточная топология с динамической маршрутизацией и балансировкой трафика, то невозможно предсказать, как именно голосовой поток пройдет к оборудованию. Поэтому рекомендуется включать все оборудование VoIP в одни и те же коммутаторы.

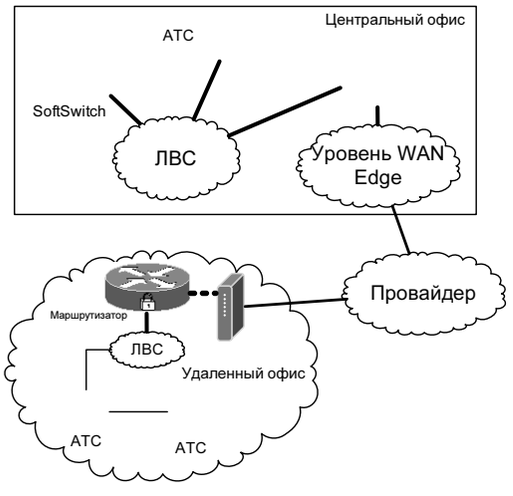

Рис. 8. Голосовое оборудование

Итак, точка конечного анализа установлена около SoftSwitch, точка генерации трафика включена в ЛВС удаленного офиса. При стресс-тестировании выясняется, что задержки слишком большие. Причина может быть в чем угодно и где угодно на пути следования трафика. Надо выяснить причину, или задать другие параметры голосовых потоков. В этом случае без внешних инструментов не обойтись.

Организация программной системы распознавания и анализа трафика

Как только возникает проблема выбора оптимального потока, QoS политики и метода формирования трафика какого-либо приложения, все предположения по оптимизации уходят в сферу интуитивных решений. Потому как протестировать каждый вариант на реальной сети с оборудованием очень затратно, а моделирование не сможет учесть всех аспектов прохождения трафика по всему пути. Кроме того, структура и состав ЛВС обычно скрыты от нас.

Поможет разработанная авторами программная система распознавания и анализа трафика.

Преимущество данной системы заключается в том, что она позволяет на основе анализа одного потока данных от каждого использующегося приложения провести анализ качества прохождения трафика по всему пути.

На первом этапе система отделяет потоки приложений друг от друга. Каждый поток разделяется по направлениям и отдельно анализируется.

Во время анализа происходит автоматическое определение приложения, статистических и вероятностных характеристик, таких как вид распределения, параметры распределения, первые два момента распределений.

Определение вида распределения происходит по алгоритму, показанному на рис. 9 [1].

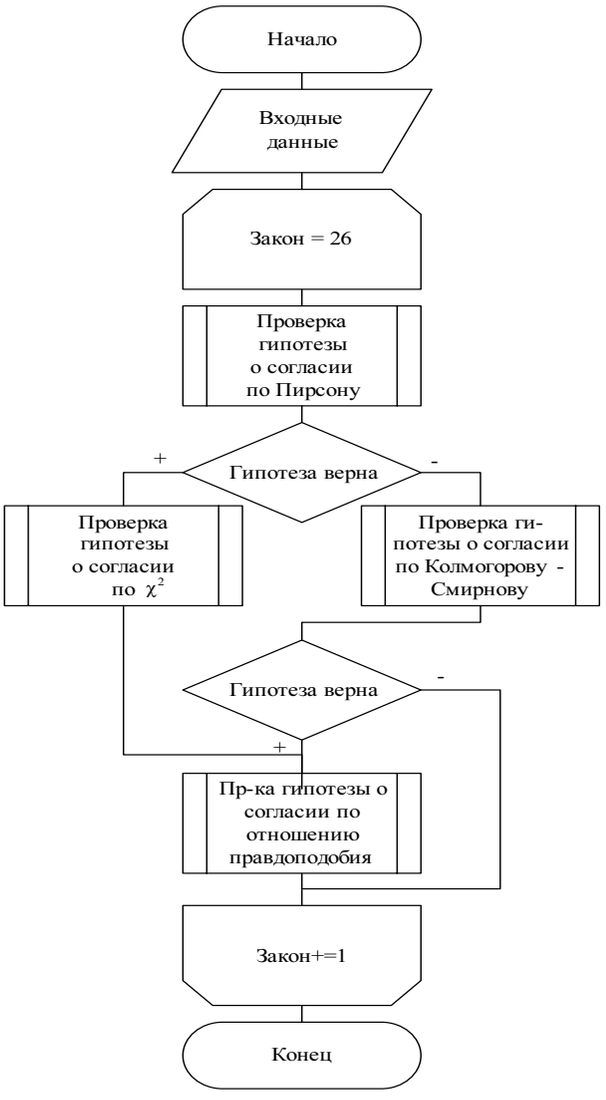

Рис. 9. Определение вида распределения

Библиотека автоматического выбора вида распределения охватывает класс, состоящий из 26 непрерывных законов распределения случайных величин, наиболее часто используемых в приложениях: экспоненциального, полунормального, Рэлея, Максвелла, Парето, Эрланга, Лапласа, нормального, логарифмически нормальных (ln и lg), Коши, Вейбулла, двойного показательного, гамма-распределения, логистического, бета-распределения 1-го рода, распределений Джонсона, экспоненциального семейства распределений.

Затем выбирается наиболее подходящий закон распределения по методу максимального правдоподобия из совокупности всех полученных параметров, как показано в [3].

После этого делается прогноз на возможное количество и качество трафика в соответствии с выбранным приложением и его параметрами.

Например, оптимальные параметры сети для голосового трафика с кодеком G711 показаны на рис. 10.

Как видно из рис. 10, максимальное число голосовых каналов – 4.

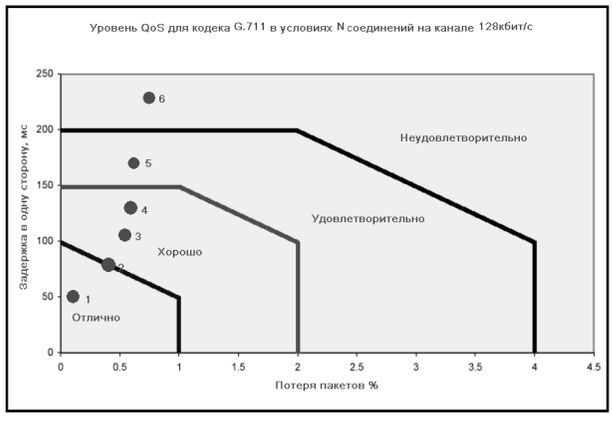

Рис. 10. Параметры качества сети

Аналогичные зависимости, но на основе реальных данных (фоновая загрузка, существующая задержка) демонстрирует рис. 11.

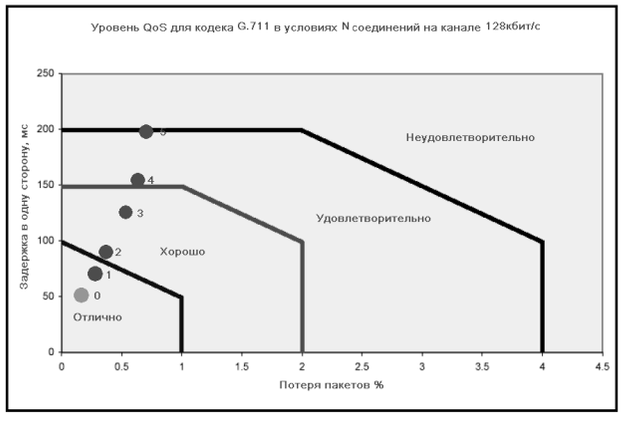

Рис. 11. Реальная ситуация

На уровне 0 – ситуация без голосового трафика (вносимые задержки). Как видим ситуация далека от теоретической даже с использованием QoS. Максимально с существующим трафиком можно пропустить дополнительно около 2-х голосовых соединений и 1 соединение – для услуг (автосекретарь, голосовая почта, автоответчик).

Функциональная схема программы показана на рис. 12. На ней представлены основные функциональные возможности системы и ресурсы, необходимые для их реализации.

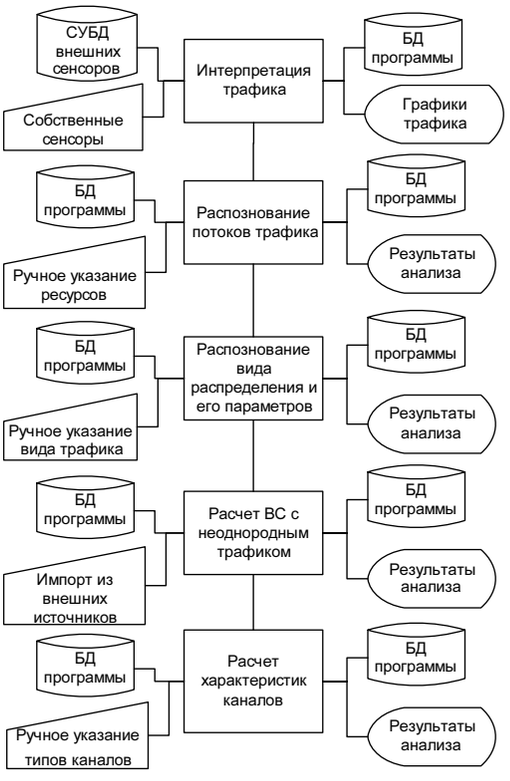

Рис. 12. Функциональная схема программы

1. Интерпретация трафика. Ввод информации возможен с нескольких видов внешних сенсоров и с внутренних сенсоров (SNMP, Sniffing). Анализ размера пакетов, типа трафика, протоколов. Результат заносится в БД и отображается на дисплее.

2. Распознавание потоков трафика и создание матрицы смежности. Ввод из БД по результатам предыдущего шага, ручное уточнение типов. Анализ типа и направления потока, интенсивности и требований к качеству среды. Запись результатов в БД, отображение на дисплее в графическом виде.

3. Распознавание статистического распределения. Ввод данных из БД (1 поток из шага 2 или весь трафик), ручное уточнение видов распределения. Анализ гипотез о распределении, выдача наиболее вероятного распределения и его параметров. Запись в БД и отображение на дисплей.

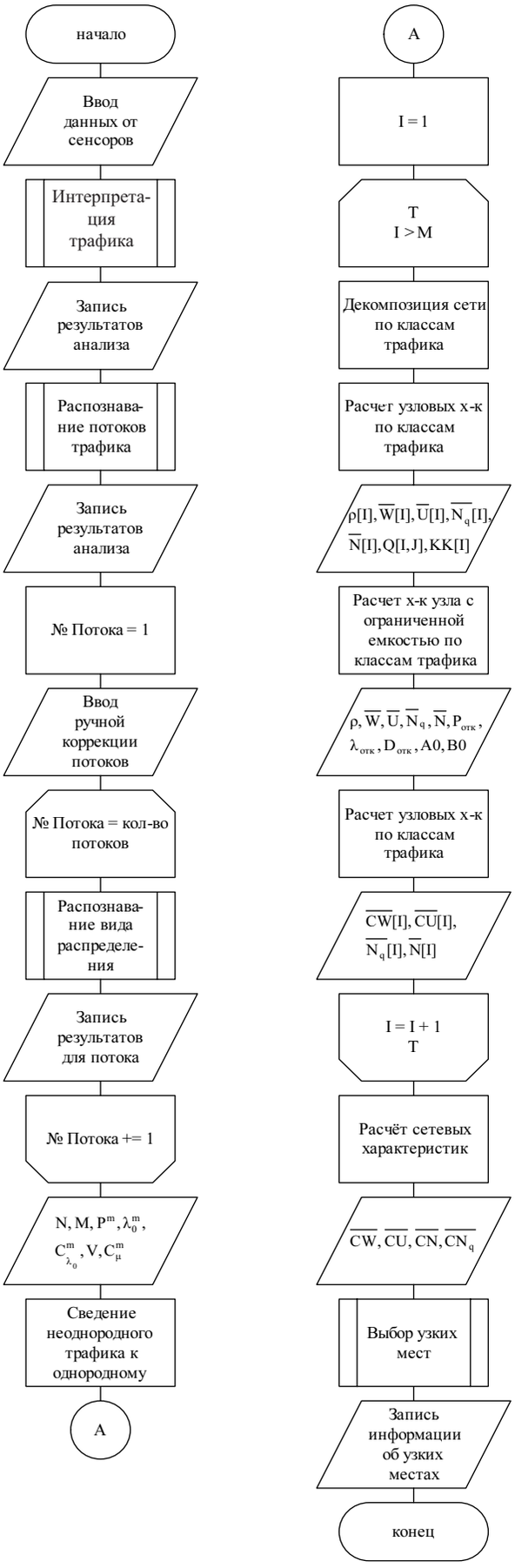

Рис. 13. Укрупненная схема алгоритма программы

4. Расчет ВС с неоднородным трафиком. На основе анализа шагов 1, 2 и 3 расчет характеристик хостов – участников трафика, а также расчет основных характеристик производительности всей сети в целом. Ввод из БД или из сохраненных результатов, запись в БД или отображение на дисплей.

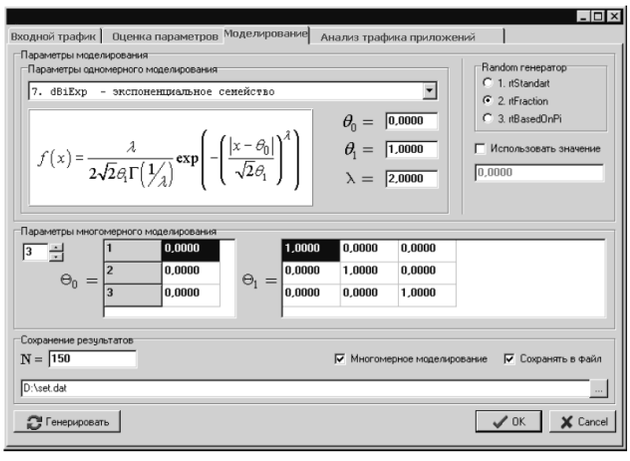

Рис. 14. Интерфейс программной системы распознавания трафика

5. На основе расчета шага 4 распознаются узкие места сети (каналы, узлы) и делается рекомендация по модернизации участка сети.

Укрупненная схема алгоритма программы представлена на рис. 13.

Для определения других параметров трафика, а также для других приложений, для создания модели прогноза поведения качества обслуживания трафика существуют другие модули программы, интерфейс одного из них показан на рис. 14.

Литература

1. Помадин С.С. Исследование распределений статистик многомерного анализа данных при нарушении предположений о нормальности. Дис. к.т.н. 05.13.17. Новосибирск, 2004. – 136 с.
2. Гончаров А. А. Исследование условий обеспечения гарантированного качества обслуживания в сети Интернет :Дис. к.т.н. 05.12.13. Москва, 2007. – 118 с.
3. Вишневский В.М. Теоретические основы проектирования компьютерных сетей. М.: Техносфера, 2003. – 512 с.
4. Филимонов А.Ю. Построение мультисервисных сетей Ethernet. СПб.: БХВ-Петербург, 2007. – 592 с.

УДК 621.39: 681.3

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ДЛЯ РАСЧЕТА ХАРАКТЕРИСТИК СЕТЕЙ НА БАЗЕ КОММУТАТОРОВ ETHERNET ВТОРОГО УРОВНЯ

Гавлиевский С.Л.

В статье разработана математическая модель, описывающая потоки на ветвях сети, построенной на базе коммутаторов Ethernet в виде системы нелинейных алгебраических уравнений. Приводится алгоритм решения системы уравнений при помощи итерационного метода.

Система уравнений для расчета сети при адресной рассылке кадров

В [1] приведены соотношения, позволяющие при фиксированных элементах матриц π и τ для заданной пары узлов k и l, рассчитывать $\psi_j^{[k]\to(l)}$, $\theta_j^{[k]\to(l)}$, а также определять $\lambda_{ij}^{[k]\to(l)}$ – нагрузку на ветви сети, оказываемую процессом передачи кадров между этой парой узлов. На основании соотношений (1)-(8) из [1] для каждой пары узлов k и l можно записать:

$$\begin{aligned}
\overline{\psi}^{[k]\to(l)} &= f_\psi(\overline{\psi}^{[k]\to(l)}, \pi)\\
\overline{\theta}^{[k]\to(l)} &= f_\theta(\overline{\theta}^{[k]\to(l)}, \tau)\\
\lambda^{[k]\to(l)} &= f_\lambda(\overline{\psi}^{[k]\to(l)}, \Lambda)\\
\pi_{ij} &= f_\pi(\lambda_{ij}^{[k]\to(l)})\\
\tau_{ij} &= f_\tau(\lambda_{ij}^{[k]\to(l)})
\end{aligned} .$$

Обобщая последние пять выражений, можно составить систему нелинейных алгебраических уравнений (СНАУ):

$$\begin{cases}
\Psi = f_\Xi(\Psi, \pi)\\
\Theta = f_\theta(\Theta, \tau)\\
\lambda = f_\lambda(\Psi, \Lambda)\\
\pi = f_\pi(\lambda)\\
\tau = f_\tau(\lambda)
\end{cases}, \qquad (1)$$