Министерство образования Республики Беларусь

Учреждение образования

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

УДК_____

Зинченко
Антон Юрьевич

Анализ трафика в корпоративных IP-сетях

АВТОРЕФЕРАТ
на соискание степени магистра техники и технологий
по специальности 45.81.01 «Инфокоммуникационные системы и сети»

Научный руководитель
Астровский И. И.
кандидат технических наук, доцент

Минск 2016

Нормоконтроль

_____

_____

ВВЕДЕНИЕ

Множество современных разработок в области коммуникаций и ИТ направлены на упрощение коммуникаций между сотрудниками организации и на предоставление новых возможностей для всесторонних улучшений бизнес процессов в компаниях. Развитие зоны покрытия и пропускной способности Интернета, как стационарного, так и мобильного, позволяет сотрудникам быть практически всё время онлайн и работать с корпоративными ресурсами удалённо, при этом пользоваться услугами с высокой скоростью и низкими показателями задержки. Увеличение взаимодействия между сотрудниками открывает большое количество новых возможностей.

Так если еще 5-10 лет назад, общение посредством электронных писем, звонков на стационарные и мобильные телефоны, SMS было основным для людей, то сегодня сервисов для общения и взаимодействия стало в разы больше. Проводя анализ предоставляемых сервисами услуг, можно выделить следующие: передача мгновенных сообщений (как в формате диалога, так и в формате конференции), передача файлов, средства для голосового общения (как в формате диалога, так и в формате конференции), средства для видео общения (как в формате диалога, так и в формате конференции), а также ряд других услуг.

Исторически сложилось, что именно голосовое взаимодействие (разговор) приносило операторам связи существенный доход, в качестве подтверждения можно рассмотреть успех в разные периоды истории и в разных странах таких компаний как: AT&T (в области ТфОП), Vodafone (в области мобильной связи) и другие. Коммерческие структуры всегда вынуждены заботиться о качестве предоставляемых услуг и о будущих доходах, поэтому развитие рынка голосовых звонков и видео звонком развивается благодаря влиятельным коммерческим структурам.

Традиционно голос передают по медной кабельной инфраструктуре как в аналоговом виде (преимущественно последняя миля), так и в цифровом (преимущественно магистральные линии). Передача голоса последние лет 50 была неотделима от сети с коммутацией каналов. Такие сети, где каждый разговор занимает определённую ёмкость оборудования на время длительности всего разговора, и данная ёмкость становилась недоступна другим пользователям.

С развитием технологий стало возможным передавать голосовой трафик через сеть с коммутацией пакетов, в частности через Интернет. Это стало новым этапом развития телефонии. Так, для магистральных операторов связи, как правило предоставляющих доступ и в Интернет, возможность передавать голосовой трафик через Интернет означало как существенную экономию, так и

возможность организации дополнительных услуг и, естественно, их продажу потребителю. В настоящее время и конечному потребителю доступны услуги, основанные на цифровой телефонии, работающей поверх Интернета. Например, компания Белтелеком предлагает услугу «Максифон», которая позволяет потребителю звонить и принимать звонки с смартфона или компьютера точно также, как с обычного стационарного телефона. Услуга отличается качеством и скоростью работы, так как основана на платформе IMS.

Хотя идея отправки аудио и видео через Интернет появилась еще в семидесятых, только в начале XXI века передача мультимедиа в реальном времени (real-time audio и real-time video) стала возможной. Трафик в реальном времени отличается от вебтрафика тем, что передача должна идти с определенной скоростью, чтобы иметь смысл, что налагает ограничения относительно задержки, джиттера и полосы пропускания канала связи.

В настоящее время передачу голоса через интернет, то есть интернет телефонию, называют VoIP (voice over Ip – голосов поверх Ip). Во многих организациях сотрудниками используется программа Skype, или ее аналог для бизнес сегмента Skype for business, для обмена мгновенными сообщениями и файлами. Потребителю доступно огромное количество клиентских программ как платных, так и бесплатных для VoIP.

Skype предоставляет услуги голосовой и видео телефонии, а также обмена сообщениями. Данная программа пользуется огромной популярностью и продолжает увеличивать клиентскую базу. Так происходит благодаря возможности бесплатно общаться людям, как находящимся близко, так и удалённым друг от друга.

Чтобы обеспечить возможность для развития VoIP произошли ряд событий. Во-первых, компьютеры стали гораздо мощнее, они оснащаются микрофонами и камерами, так что появилась возможность легко вводить, обрабатывать и выводить аудио- и видеоданные. Во-вторых, были решены проблемы с пропускной способностью Интернета, а в случае локальной сети, где пропускная способность гораздо выше, тем более. Линки, ведущие к центру Интернета, работают со скоростью сотен гигабит в секунду, а широкополосный стационарный доступ и широкополосная беспроводная связь по стандартам 802.11 и группе стандартов мобильной связи (3GPP Release 8) доходят до пользователей на периферии Интернета.

Также нельзя не отметить активное развитие рынка мобильных устройств. Так, сейчас мобильный телефон представляет собой компьютер миниатюрного размера. Ввиду невысокой цены данных устройств, можно предположить, что использование VoIP программ на смартфонах будет набирать популярность у пользователей весьма стремительно.

Целью данной магистерской диссертации является разработка и реализация метода анализа трафика в корпоративных IP-сетях.

Для достижения поставленной цели требуется решить целый ряд задач, основными из которых являются задачи моделирования состояния сети: при различных нагрузках на оборудование, при различных режимах работы сотрудников. По результатам опытов должна быть получена зависимость параметров передачи трафика от состояния сети. Например, в случае с VoIP, так как голос передаётся по одной и той же сети, что и данные, открываются широкие возможности для эксперимента. Захват и обработку предполагается проводить с помощью анализатора трафика Cisco NAM 2304, сетевого экрана Cisco ASA 5520 и программного сниффера – Wireshark. Для выполнения практической части предполагается использовать как физическое оборудование, так и виртуальное (эмулированное) оборудование.

Также предполагается создание лабораторных работ для студентов, которые помогут им в изучении моделирования и анализа трафика. При этом у студентов должна быть возможность изучать материалы и без физического доступа к оборудованию, для этого будет использоваться программные генераторы трафика, такие как Scapy и packETH.

ХАРАКТЕРИСТИКА

Полученные результаты работы могут быть использованы в организациях среднего и крупного бизнеса при планировании IP-сети, ее мониторинге и аудите безопасности. Так как множество организаций переходит или уже использует технологии voice over IP, то результаты работы помогут прогнозировать качество передачи голосового трафика относительно предполагаемой загрузки сети.

Для достижения поставленной цели также использованы программные продукты: программный анализатор трафика Wireshark, генераторы трафика Scapy и РаскETH. В качестве аппаратных устройств, предоставляющих функции анализа трафика или DPI (deep packet inspection), были использованы Cisco NAM 2304 и Cisco ASA 5520. Так как программные продукты созданы для использования в Linux среде, в качестве операционной системы была выбрана именно эта среда. В частности, дистрибутивы, основанные на Debian.

В разделе ресурсо- и энергосбережения показано, каким образом можно эффективно использовать электроэнергию в организациях, использующих IP-сети поверх Ethernet, при этом не уменьшая производительность устройств телекоммуникаций.

Проведенные в процессе работы над диссертацией исследования позволили сформировать концепции и методики по управлению и обеспечению безопасности передачи информации в корпоративном сегменте сети и разработать метода анализа трафика в корпоративных IP-сетях.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ..... 3

1. Обзор протоколов, используемых для VoIP .....**Ошибка! Закладка не определена.**

1.1. Описание протоколов RTP и RTCP..... **Ошибка! Закладка не определена.**

1.2 Протокол установления соединений SIP.....**Ошибка! Закладка не определена.**

1.3 Протоколы H.323..... **Ошибка! Закладка не определена.**

1.4. SDP – протокол описания сессии передачи данных **Ошибка! Закладка не определена.**

1.5 Обзор протокола NetFlow..... **Ошибка! Закладка не определена.**

2 Обзор используемых технологий и оборудования..... **Ошибка! Закладка не определена.**

2.1 Описание Cisco NAM ..... **Ошибка! Закладка не определена.**

2.2 Сниффер сетевого трафика Wireshark .**Ошибка! Закладка не определена.**

2.3 Описание Cisco ASA..... **Ошибка! Закладка не определена.**

3 Экспериментальная часть ..... **Ошибка! Закладка не определена.**

3.1 Описание экспериментальной сети..... **Ошибка! Закладка не определена.**

3.2 Расчёт показателей экспериментальной сети .....**Ошибка! Закладка не определена.**

3.3 Проводимые эксперименты и результаты.....**Ошибка! Закладка не определена.**

3.4 Концепция защиты от кибер-угроз ..... **Ошибка! Закладка не определена.**

4 Влияние анализа и оптимизации трафика на энерго- и ресурсосбережение..... **Ошибка! Закладка не определена.**

4.1 Техническое обоснование энергоэффективности .....**Ошибка! Закладка не определена.**

4.2 Использование результатов в работе организации УП Велком.....**Ошибка! Закладка не определена.**

ЗАКЛЮЧЕНИЕ 9

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ **Ошибка! Закладка не определена.**

ПРИЛОЖЕНИЕ А (обязательное) Лабораторная работа № 1 «Получение знаний о Wireshark»..... **Ошибка! Закладка не определена.**

1 Изучение расширенных возможностей программы.....**Ошибка! Закладка не определена.**

2 Извлечение информации ..... **Ошибка! Закладка не определена.**

3 Использование Wireshark для захвата и анализа VoIP трафика.....**Ошибка! Закладка не определена.**

4 Задание ..... **Ошибка! Закладка не определена.**

5 Контрольные вопросы ..... **Ошибка! Закладка не определена.**

ПРИЛОЖЕНИЕ Б (обязательное) Лабораторная работа № 2 «Создание пакетов в программе Scapy».....**Ошибка! Закладка не определена.**

1 Описание..... **Ошибка! Закладка не определена.**

2 Установка..... **Ошибка! Закладка не определена.**

3 Знакомство с интерфейсом ..... **Ошибка! Закладка не определена.**

4 Примеры создания простого пакета..... **Ошибка! Закладка не определена.**

5 Углубление навыков работы с программой .....**Ошибка! Закладка не определена.**

6 Адресация ..... **Ошибка! Закладка не определена.**

7 Отправка пакетов в сеть ..... **Ошибка! Закладка не определена.**

8 Работа с ответными пакетами..... **Ошибка! Закладка не определена.**

9 Сниффер и наоборот..... **Ошибка! Закладка не определена.**

10 Автоматизация..... **Ошибка! Закладка не определена.**

11. Создаем трехэтапное TCP-соединение **Ошибка! Закладка не определена.**

12 Продолжение исследования..... **Ошибка! Закладка не определена.**

14 Задание ..... **Ошибка! Закладка не определена.**

15 Контрольные вопросы ..... **Ошибка! Закладка не определена.**

ПРИЛОЖЕНИЕ В (обязательное) Лабораторная работа № 3 «Знакомство с программой packETH»..... **Ошибка! Закладка не определена.**

1 Описание ..... **Ошибка! Закладка не определена.**

2 Установка ..... **Ошибка! Закладка не определена.**

3 Создание пакетов ..... **Ошибка! Закладка не определена.**

4 Задание ..... **Ошибка! Закладка не определена.**

5 Контрольные вопросы ..... **Ошибка! Закладка не определена.**

ЗАКЛЮЧЕНИЕ

В данной магистерской диссертации были рассмотрены несколько задач: создание трафика с различными параметрами, захват и экспорт трафика для анализа и, непосредственно, анализ трафика. Для решения поставленных задач была создана экспериментальная сеть. Рассмотрим решение каждой из поставленных задач.

Для создания трафика были освоены программные генераторы пакетов Scapy и PackETH. Были написаны лабораторные работы по каждой из программ, для внедрения их в учебный процесс. Лабораторная работа по Wireshark представлена в ПРИЛОЖЕНИИ А. Лабораторная работа по Scapy представлена в ПРИЛОЖЕНИИ Б. Лабораторная работа по PackETH представлена в ПРИЛОЖЕНИИ В.

Захват трафика был реализован на уровне коммутатора, для экспорта трафика использовался протокол SPAN. Экспорт информации о свойствах трафика с удаленного сегмента сети осуществлялся посредством протокола NetFlow. В качестве аппаратного сниффера использовалось оборудование Cisco Prime NAM 2304 и Cisco ASA 5520. Также для решения ряда аналитических задач использовался программный сниффер Wireshark. По данной программе также было разработано лабораторное пособие.

Был произведен расчёт основных показателей сети для организации, состоящей из 300 человек. При расчёте показателей было учтено, что структурно организация не однородна и различные подразделения потребляют различное количество трафика.

Расчётная нагрузка на магистраль транспортной сети составила $285{,}6 \cdot 10^6$, бит/с. Данная пропускная способность обеспечивается системами передач не ниже Gigabit Ethernet.

В результате проведенных исследований были получены эмпирические данные зависимости параметров речевого сигнала от загрузки сети. Данные результаты представлены в третьем разделе работы.

Проведенные исследования и их анализ позволили сделать следующие выводы:

1) Средная величина джиттера, увеличивается пропорционально загрузки канала связи. Однако, даже при загруки канала на 80-100 процентов, джиттер не достигает значений, которые могли бы быть восприняты человеческим ухом. Также необходимо заметить, что скорость передачи данных в каналах связи в реальных условиях лишь в редких случаях может достичь 1 Гигабита в секунду, так как она ограничена скоростью чтения/записи устройства

хранения информации компьютера. В большимстве случаев максимально занимается до 30 процентов гигабитного канала.

2) Ощутимая потеря пакетов наблюдается при создании нагрузки на порт PBX. Данный вариант возможен, например, при атаке на организацию. Поэтому на стороне PBX необходимо принимать меры по повышению уровня безопастности.

Следовательно, в современных мультигигабитных сетях пропускной способности канала хватает с запасом как для передачи данных, так и передачи голоса.

Вместе с тем следует уделять особое внимание безопасности. В частности, защита сетевой среды должна состоять из трёх частей: глубокого просмотра в точках анализа (обновление информации о известной угрозе, идентификация/блокировка приложений и файлов, траектория файлов), защита доступа к сети и инфраструктуре (видимость пользователей и устройств, авторизация и сегментация), а также широкий обзор на всех сетевых уровнях (сбор данных по всему трафику, обнаружение подозрительной и аномальной активности).

В 4 главе «Влияние анализа и оптимизации трафика на энерго- и ресурсосбережение» было приведено техническое обоснование возможности энергосбережения на предприятии относительно IP- устройств. Были получены положительные результаты энергосбережения на примере применения технологий 802.3az и Cisco EnergyWise в УП «Велком».

В результате цель магистерской работы была достигнута. Но за рамками данной работы остались смежные важные темы, например, анализ голосового трафика в сетях, основанных на технологиях adsl и gpon.

Интегрируя всё вышесказанное, можно заключить следующее – скорость передачи информации в современных корпоративных сетях значительно выросла, вплоть до гигабита в секунду. В современных корпоративных сетях имеется множество сервисов, которым необходимо определенное гарантированное качество обслуживания. К таким сервисам следует отнести: в первую очередь телефонную связь поверх ip сети, т. е. VoIP, а также видеоконференции. К сервисам менее требовательным к QOS следует отнести видео стриминг и веб серфинг. Для обеспечения необходимого качества обслуживания необходимо иметь средство для анализа трафика и его оптимизации.

Таким образом, в современных корпоративных сетях анализ трафика и его оптимизация выходят на первый план, так как являются необходимыми для организации рабочего и бизнес процесса организации.

СПИСОК СОБСТВЕННЫХ ПУБЛИКАЦИЙ

1. А.Ю. Зинченко, В.Ю. Цветков, Алби Гарби Хушам Абдулхусейен Худайр. Концепция защиты инфокоммуникаций от кибер-угроз. // Технические средства защиты информации: Материалы XIII Белорусско-российской научно технической конференции, 4-5 июня 2015 г., Минск. Минск: БГУИР, 2015. — 100 с.

2. А.Ю. Зинченко. Концепция защиты от современных угроз информационной безопасности. // Современные средства связи: Материалы XX Международная научно-техническая конференция, 14-15 октября 2015 г., Минск. Минск: ВГКС, 2015. — 325 с.