Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК_____

Розум
Андрей Владимирович

Исследование и оптимизация способов построения корпоративных сетей связи

АВТОРЕФЕРАТ
на соискание степени магистра технических наук
по специальности 1-45 80 01 «Системы, сети и устройства телекоммуникаций»

_____

Научный руководитель

Хацкевич Олег Александрович
доцент, канд. техн. наук

_____

Минск 2015

Тема диссертации: Исследование и оптимизация способов построения корпоративных сетей связи.

Всё больше объектов хозяйствования как государственной, так и частной формы собственности на территории РБ начинают развивать собственные корпоративные сети. Причин тому несколько: расширение предприятия, связанное с необходимостью обеспечения надежной и качественной связью удалённые офисы и филиалы, а также всевозрастающие требования к пропускной полосе и надежности передачи данных.

В условиях недостаточного финансирования основным вопросом при создании или расширении уже существующей корпоративной сети является вопрос итоговой цены, как на само оборудование, так и на аренду требуемых каналов связи и администрирование сети. В данной работе будут проведены исследования и рассмотрены способы оптимизации построения корпоративных сетей связи. Для исследования будет взята крупная компания, имеющая головной офис в Минске, сеть филиалов в областных городах и сеть районных отделений.

Объектом исследования являются:

Корпоративные сети передачи данных.

Предметом исследования являются:

Способы построения корпоративных сетей связи. Показатели эффективности и качества работы корпоративной сети связи.

Целью исследования является повышение качества и производительности корпоративных сетей связи, сокращение расходов на проектирование, повышение защищённости сети от внешних угроз.

Для решения поставленной цели в работе будут рассмотрены следующие задачи:

1. Выбор технологии для построения сетей передачи данных.
2. Разработка прикладной математической модели сети связи.
3. Расчёт и анализ оценки качественных характеристик корпоративной сети связи.
4. Оптимизация эффективности работы приложений и протоколов ПД корпоративной сети связи, позволяющая повысить её качественные характеристики.
5. Вопросы защиты информации.

Полученные результаты исследования позволяют отойти от наиболее распространённого подхода в проектировании информационных систем – метода экспертных оценок. Данный метод хоть и позволяет минимизировать затраты на этапе проектирования и быстро оценить стоимость реализации решения, однако, носит субъективный характер. Преимуществом имитационных моделей является возможность подмены процесса смены событий в исследуемой системе в реальном масштабе времени на ускоренный процесс смены событий в темпе работы программы.

Для решения поставленных задач и раскрытия темы диссертации необходимо дать само понятие корпоративной сети и определить её роль и особенности в иерархии сетей передачи данных. Исходя из этих особенностей, рассмотренных в первой главе диссертации, будет произведён выбор конкретных технологий и решений, удовлетворяющих требованиям корпоративных сетей. Будет произведён анализ литературных источников, рассмотрены мировые тенденции в области способов и технологий построения современных конвергентных корпоративных сетей связи.

На основе полученных результатов будут предложены наилучшие способы и технологии для построения сети. Так, для организации связи внутри офисов и филиалов выбрана технология Ethernet, позволяющая в кратчайшие сроки осуществить запуск и наладку сети. Технология Ethernet позволяет легко осуществлять масштабирование сети без влияния на работу действующего персонала. Следует отметить, что Ethernet является мировым стандартом для организации LAN сетей.

Для защищённого соединения территориально разнесённых отделений организации целесообразно использовать технологию VPN MPLS. От других технологий построения виртуальных частных сетей, таких как VPN на базе ATM или Frame Relay, технологию VPN MPLS выгодно отличает хорошая масштабируемость, возможность автоматического конфигурирования и естественная интеграция с другими сервисами протокола IP, включая доступ в Интернет, Web и почтовые службы.

Функциональность VPN MPLS можно обобщить следующим образом:

- MPLS позволяет единой конвергентной сети поддерживать как новые, так и существующие услуги, создавая эффективный путь перехода к IP-инфраструктуре.

- MPLS функционирует поверх существующих систем и сетей передачи (ATM, Frame Relay, X.25, IEEE 802.3 и др).

- MPLS позволяет формировать трафик. Маршрутизация пакетов данных осуществляется за счет применения техники обработки меток.

- MPLS поддерживает предоставление услуг с гарантированным качеством обслуживания (QoS). Пакеты, которые должны доставляться с высоким качеством, могут помечаться, позволяя провайдерам обеспечивать определенные малые значения задержки для речевых и видео сигналов в сквозном соединении.

- MPLS обеспечивает соответствующий уровень безопасности, чтобы сделать IP-сеть такой же безопасной, как сеть ретрансляции кадров в WAN, одновременно сокращая потребность на шифрование в IP-сетях общего пользования.

При передаче конфиденциальной информации важно обеспечить высокий уровень надёжности шифрования. Наиболее известным представителем техники шифрования для организации защитного канала в сетях VPN является технология IPSec (Internet Protocol Security – защищенный протокол IP).

Основное назначение сервиса IPSec состоит в обеспечении безопасной ПД по IP-сетям с использованием любой технологии канального уровня (PPP, Ethernet, ATM и т.д.). Применение протокола IPSec гарантирует целостность, аутентичность и конфиденциальность данных; в его состав сейчас входят почти 20 предложений по стандартам и 18 RFC.

В основе IPSec реализованы следующие приемы:

- шифрование исходного IP-пакета, что обеспечивает секретность содержащихся в пакете данных, таких как поля IP-заголовка и поле данных;
- цифровая подпись IP-пакетов, что обеспечивает аутентификацию пакета и источника-отправителя пакета;
- инкапсуляция IP-пакета в новый защищенный IP-пакет с новым заголовком, содержащим IP-адрес устройства защиты, что маскирует топологию внутренней сети.

Таким образом, применение VPN MPLS на основе Ethernet сетей с шифрованием данных по протоколу IPSEC позволяет спроектировать современную корпоративную сеть и создать фундамент для дальнейшего моделирования сети, целью которого является дальнейшая оптимизация.

– Во второй главе рассмотрено применение метода декомпозиции и разбиении задачи синтеза сети на более мелкие компоненты для дальнейшего математического описания. Первый этап декомпозиции исследуемой модели заключается в выяснении всех функциональных связей существующих между узлами сети. Наиболее удобным способом такого описания является графоаналитический. Полученное дерево связности однозначно описывает сеть ПД с точки зрения существующих связей между элементами сети. На этом шаге можно было бы прекратить дальнейшее математическое описание сети и считать необходимую пропускную способность между узлами как сумму максимально необходимых скоростей для каждого пользователя. Однако, проанализировав данные полученного вектора связности, который соответствует математическому описанию дерева связности, а так же в силу асимметрии ПД от узла к узлу выполняется следующее неравенство:

$$b_k \le \sum_{j=1}^{m} b_j \ ,$$

где b_k – пропускная способность уровня с более высоким рангом;

b_j – пропускная способность уровня с более низким рангом;

m – число узлов низкого ранга.

Данное выражение характеризует недостижимость одновременной ПД всех узлов одного уровня с предельно-допустимой пропускной способностью. Поэтому следующим этапом декомпозиции является определение оптимальных потоков ПД для заданных узлов при известных величинах b_n.

Общая методика расчета оптимизации потоков ПД при стохастическом характере поступления данных и их детерминированной обработке в каналах

связи и узлах коммутации предопределяет использование моделей теории массового обслуживания для анализа и проектирования сети ПД.

По результатам оптимизации потоков ПД были выявлены наиболее оптимальные соотношения потоков ПД, позволяющие, при минимизации общих затрат, связанных с арендой каналов передачи данных, обеспечить наиболее эффективную производительность. Кроме того, исследования подобного рода задач может быть использовано администраторами сети и системными программистами для оценки и мониторинга устойчивости архитектуры сети, например, к перегрузкам ПД.

В третьей главе рассматриваются вопросы синтеза безопасной сети передачи данных. Руководствуясь архитектурными концепциями безопасности, приведёнными в стандарте ISO 7498-2:

- определение сервисов безопасности;
- определение механизмов безопасности;
- уровневая модель (OSI) построения сервисов безопасности;
- соотнесение сервисов безопасности и уровневой модели;
- соотнесение механизмов безопасности и сервисов.

а так же используя уравнение множественной линейной регрессии, получим зависимость защищённости от числа и состава систем в КС:

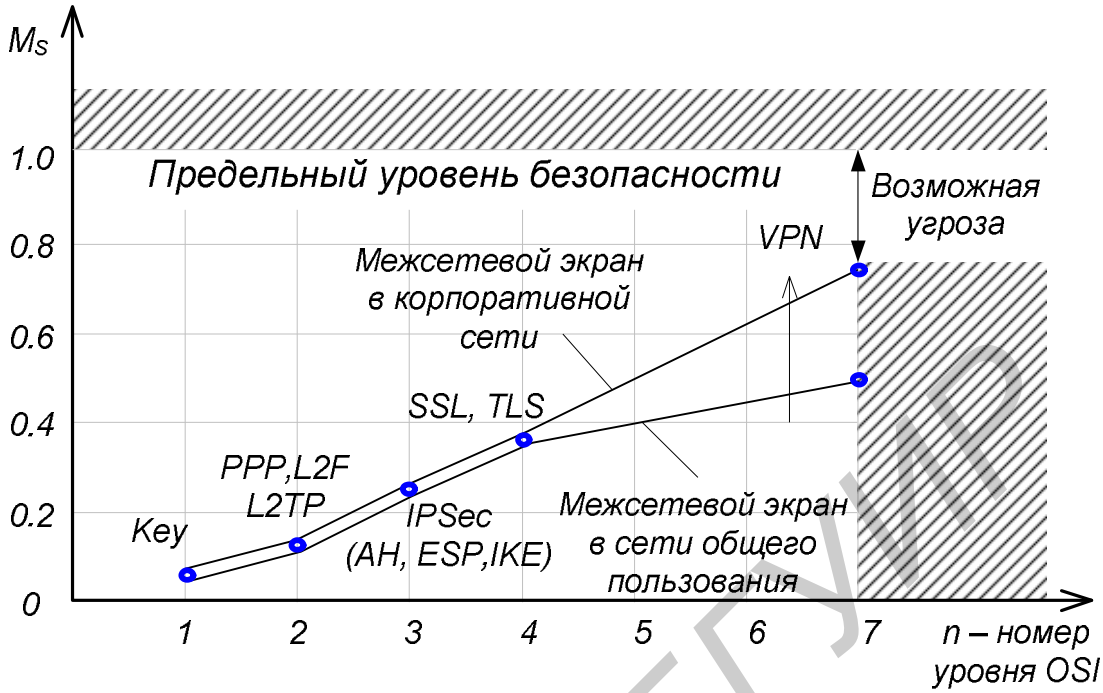
$$M_S = \alpha_0 + \sum_{j=1}^{k} \alpha_j x_j ,$$

где α_0, α_j – коэффициенты множественной линейной регрессии;

x_j – параметры, характеризующие системы безопасности;

M_S – метрика оценки информационной безопасности КС.

В качестве устройств обеспечения информационной безопасности КС применяются межсетевые экраны (FW – FireWall), функционирующие на сетевом, транспортном и прикладном уровне. На основе статистических данных о нарушениях информационной безопасности в компьютерных сетях и уравнении линейной регрессии определим зависимость защищённости системы от использования FW на различных уровнях OSI.



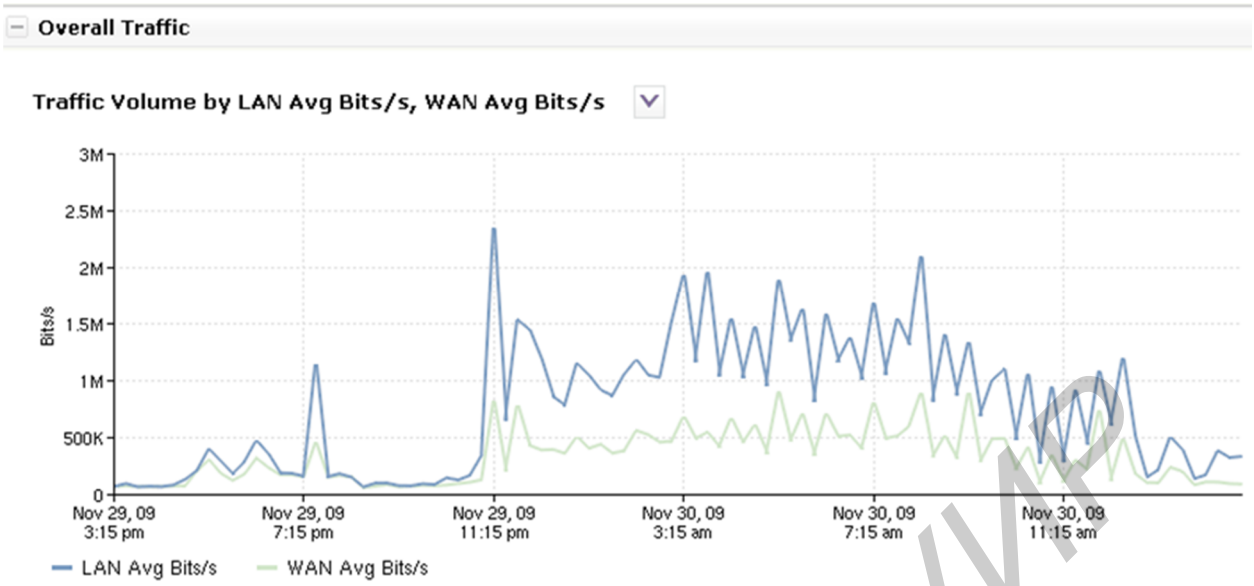
Расчётные данные показали, что наибольшей защищённости $M_S^{(np)}$ =0,726 можно добиться при использовании VPN и FW на прикладном уровне.

Заключающий четвёртый раздел посвящён исследованию качественных показателей работы корпоративной сети.

Одним из важнейших параметров является задержка передачи пакетов τ. Согласно общепринятым нормам по времени задержки передачи пакетов для сетей MPLS (время прохождения пакетов по линии доступа в одну сторону от передающей стороны к приемной), величина τ может составлять не более 20 мс. Расчётные значения для республиканского сегмента сети τ = 15,35 мс удовлетворяют этой норме.

Не менее важной характеристикой качества передачи данных на действующих сетях является пакетный джиттер. Для MPLS-сетей норма джиттера на стыке UNI-UNI может составлять не более 15 мс [30]. Эти нормы выдерживаются национальным поставщиком услуг РУП «Белтелеком».

Актуальным остаётся вопрос эффективности работы сети передачи данных. По статистике КПД стандартной WAN сети составляет около 10%, и связано это с большой долей избыточной (около 60%) или повторяющейся информацией. Программно-аппаратный комплекс, осуществляющий дедупликацию данных и оптимизацию работы определенных протоколов, позволяет разгрузить внешние арендуемые каналы на 60-70%. Эти данные подтверждаются тестами, проведёнными на действующей сети.



Как видно из графика загрузки внешнего канала, пиковую загрузку удалось снизить с 2,4 Мбит/с до 0,8 Мбит/с (тёмный график – загрузка канала без использования оптимизатора).

По результатам данного исследования отчётливо видны шаги проектирования современной корпоративной сети связи. Применяя полученную информацию, можно создавать и оптимизировать работу уже существующих сетей, выводя эффективность и надёжность сети на качественно новый уровень.

Результаты работы докладывались на следующих конференциях:

1. 50-ая научная конференция аспирантов, магистрантов и студентов Белорусского государственного университета информатики и радиоэлектроники. Тема доклада: «Оптимизация трафика на корпоративных сетях связи». БГУИР, Минск 2014.
2. XIX Международная научно-техническая конференция «СОВРЕМЕННЫЕ СРЕДСТВА СВЯЗИ». Тема доклада: «Механизмы дедупликации трафика в корпоративных сетях». ВГКС, Минск 2014.