DOI 10.37882/2223–2966.2020.04.31

РАЗРАБОТКА КОРПОРАТИВНОЙ СЕТИ ПЕРЕДАЧИ ДАННЫХ ПРЕДПРИЯТИЯ

CORPORATE NETWORK DEVELOPMENT ENTERPRISE DATA TRANSFER

R. Nabiev
A. Zaitsev

Summary. The full development cycle of a corporate enterprise data network is presented. A review of the analysis of existing technologies and protocols used in the construction of such systems. Through a multifunctional network-modeling program, the developed network was tested.

Keywords: corporate data network, networking technology.

Набиев Рафит Ренатович
К.х.н., доцент, Казанский национальный исследовательский технологический университет, г. Казань
nabievrafit@mail.ru
Зайцев Александр Валерьевич
Казанский национальный исследовательский технологический университет, г. Казань
realtime555@mail.ru

Аннотация. Приведен полный цикл разработки корпоративной сети передачи данных предприятия. Произведён обзор анализа существующих технологий и протоколов, применяемых при построении подобных систем. Через многофункциональную программу моделирования сетей была проверена работоспособность разработанной сети.

Ключевые слова: корпоративной сети передачи данных, сетевые технологии.

Введение

На сегодняшний день компьютерные сети завоевывают все большую популярность: их применяют как при разработке небольших домашних сетей, так и для создания глобальных вычислительных сетей. Одним из прикладных аспектов применения глобальных сетей является обмен данными между филиалами крупных компаний по всему миру. Основными задачами компьютерных вычислительных сетей на предприятии являются: управление информационными ресурсами; достижение максимально быстрого взаимодействия между подразделениями и филиалами; упрощение документооборота; оптимизация производственных процессов. Подобные компьютерные сети, объединяющие узлы одной компании, называются корпоративными сетями передачи данных.

Основной проблемой крупных компаний является отсутствие корпоративной сети, которая бы отвечала современным требованиям безопасности, быстродействия и т.д.

Для построения корпоративной сети с большим количеством компьютеров используются промежуточные устройства, основными представителями которых являются коммутаторы и маршрутизаторы. Первые обеспечивают связь между узлами сети на основании номеров их сетевых интерфейсных плат, MAC-адресов (от англ. Media Access Control), а вторые определяют наилучший путь от узла источника к узлу назначения используя их адреса третьего уровня модели OSI (от англ. Open Systems Interconnection), IP-адреса.

Исходя из вышесказанного, целью настоящего исследования является проектирование территориально-распределенной корпоративной сети предприятия, отвечающую современным требованиям. Для этого в первую очередь будут проанализированы существующие технологии, протоколы, способы организации отказоустойчивости, балансировки нагрузки, базовые принципы сетевой безопасности и оборудование, применяемые при ее построении. После чего полученные знания будут применены для проектирования и последующей настройки корпоративной сети, состоящей из главного офиса и филиалов, находящихся на значительном расстоянии друг от друга.

Теоретическая часть

Исходя из анализа существующих технологий и протоколов, применяемых при построении корпоративной сети, были выбраны следующие компоненты для разрабатываемой сети.

В качестве протокола организации виртуальных частных сетей был выбран DMVPN (от англ. Dynamic Multipoint VPN) — это сочетание NHRP (от англ. Next Hop Resolution Protocol — протокол разрешения следующего перехода), протокола динамической маршрутизации

и многоточечного GRE туннеля (англ. Generic Routing Encapsulation — общая инкапсуляция маршрутов) [1]. Идея DMVPN заключается в создании центрального динамического «туннеля», настройка которого осуществляется только единожды, а при появлении новых логических связей не нужно добавлять «туннельные» интерфейсы, ни перенастраивать уже существующий, что значительно облегчает работу с сетью.

Сетевая безопасность разрабатываемой сети будет организована с использованием NAT-трансляции (от англ. Network Address Translation) сетевых адресов. NAT бывает трех типов: статический, динамический и перегруженный. В случае статического NAT один внутренний адрес преобразуется в один внешний. И при этом все запросы, приходящие на внешний адрес, будут транслироваться на соответствующей внутренний. В динамическом NAT, в отличии от статического, внешний адрес зафиксирован не чётко и будет выбираться динамически из заданного диапазона. При этом если адреса из данного диапазона закончатся, то и преобразовываться последующие внутренние адреса больше не будут, до тех пор, пока не освободятся внешние IP адреса из выделенного диапазона. Перегруженный NAT позволяет преобразовывать множество внутренних IP адресов в один внешний, но при этом для каждого пакета назначается отдельный порт, что и позволяет обеспечить в глобальном масштабе уникальность сетевого адреса. Для разрабатываемой корпоративной сети был выбран перегруженный NAT.

Для ***обеспечения отказоустойчивости сети*** будут использоваться следующие технологии и протоколы. 1. Агрегирование канала — это технология, которая позволяет объединить несколько физических каналов в один логический. Такое объединение позволяет увеличивать пропускную способность и надежность канала. 2. IP SLA — это функция, включенная в программное обеспечение Cisco IOS, которая позволяет администраторам анализировать уровни обслуживания для IP приложений и сервисов, а также помогать обнаруживать и локализовать неисправности [2]. 3. PBR-маршрутизация (от англ. Policy Based Routing) — представляет собой механизм реализации пересылки (forwarding)/ маршрутизации (routing) пакетов данных, основанный на политике, представляющей собой набор правил, определенной администраторами сети [3]. 4. EEM (от англ. Enhanced Object Tracking) — это функция оборудования Cisco, которая позволяет отслеживать состояние выбранного объекта и влиять на состояние других функций [4].

В качестве протокола, позволяющего автоматически получать IP адреса шлюзов и DNS сервера, использовали DHCP-протокол (англ. Dynamic Host Configuration Protocol) динамической конфигурации узла. Также при разработке сети будет использована технология VLAN (от англ. Virtual Local Area Network) и протокол протокол STP (от англ. Spanning Tree Protocol). VLAN — технология, благодаря которой группа узлов сети может входить в один широковещательный домен, даже будучи подключёнными к разным промежуточным устройствам второго уровня модели OSI. При этом устройства, находящиеся в разных виртуальных локальных сетях, не могут взаимодействовать друг с другом на канальном уровне. STP канальный протокол. Основной задачей STP является устранение петель в топологии произвольной сети Ethernet, в которой есть один или более сетевых мостов, связанных избыточными соединениями. STP решает эту задачу, автоматически блокируя соединения, которые в данный момент для полной связности коммутаторов являются избыточными.

Диаграмма сети будет строиться с помощью Microsoft Visio — это мощный графический инструмент для представления различных диаграмм и схем. С его помощью можно создавать модели процессов и показывать комплексные данные в удобном виде. Простой интерфейс значительно упрощает рисование схем. Так как он входит в состав пакета Microsoft Office, который присутствует практически у 90% компаний то он становится фактически стандартом для создания диаграмм сети.

В результате обзора производителей оборудования для построения корпоративной сети нами был выбран лидер в области сетевых технологий — Cisco Systems.

Практическая часть

Архитектура корпоративной сети — это комплекс, включающий в себя все необходимое для обеспечения сетевой безопасности, а также устойчивости и масштабируемости сети.

Основные требования, предъявляемые к современным компьютерным вычислительным сетям: 1) простота внедрения — развертывание решения в кратчайшие сроки; 2) гибкость и масштабируемость; 3) безопасность и отказоустойчивость — защита пользовательского трафика, отказоустойчивое исполнение гарантирующее стабильную работу сети даже во время атак; 4) простота управления — централизованное управление всей сетевой инфраструктурой; 5) готовность к новым технологиям — построенная архитектура должна позволять внедрять новые технологии и сервисы.

Для простоты внедрения в архитектуре все элементы сети разбивают на так называемы модули. Разбив архитектуру сети на модули, можно сконцентрироваться на функционале каждого из них по отдельности, что существенно упрощает дизайн, внедрение и управление

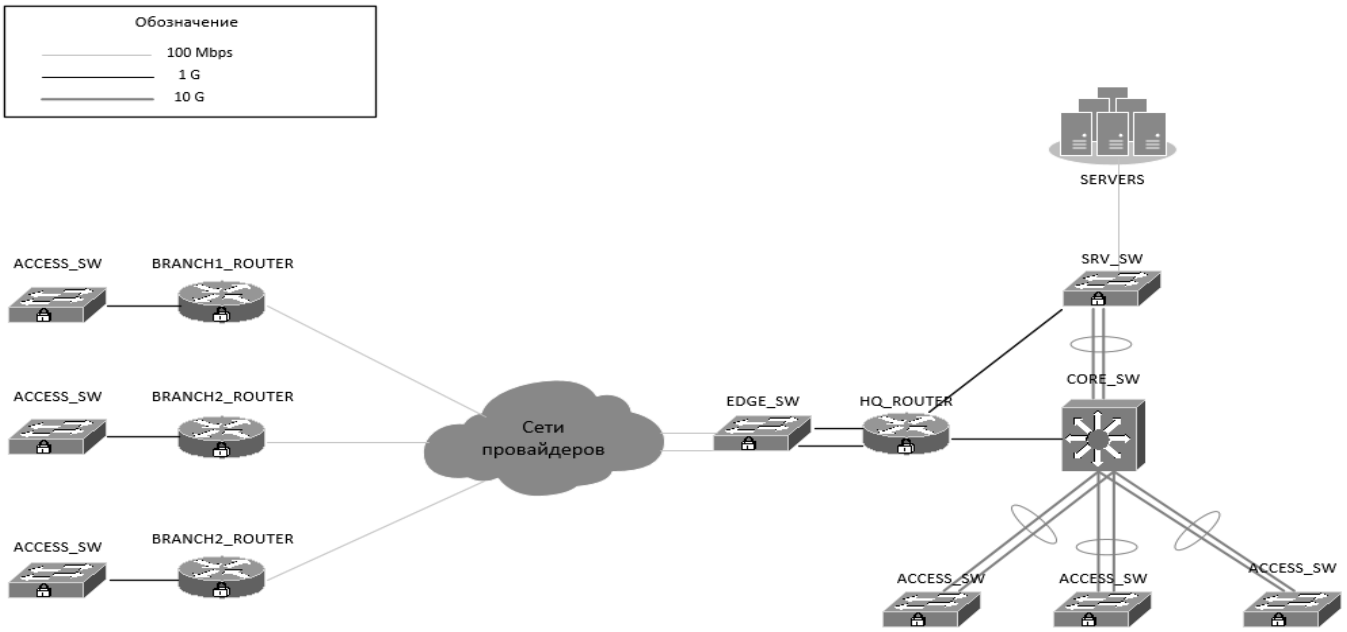

Рис. 1. Структурная схема разрабатываемой вычислительной сети

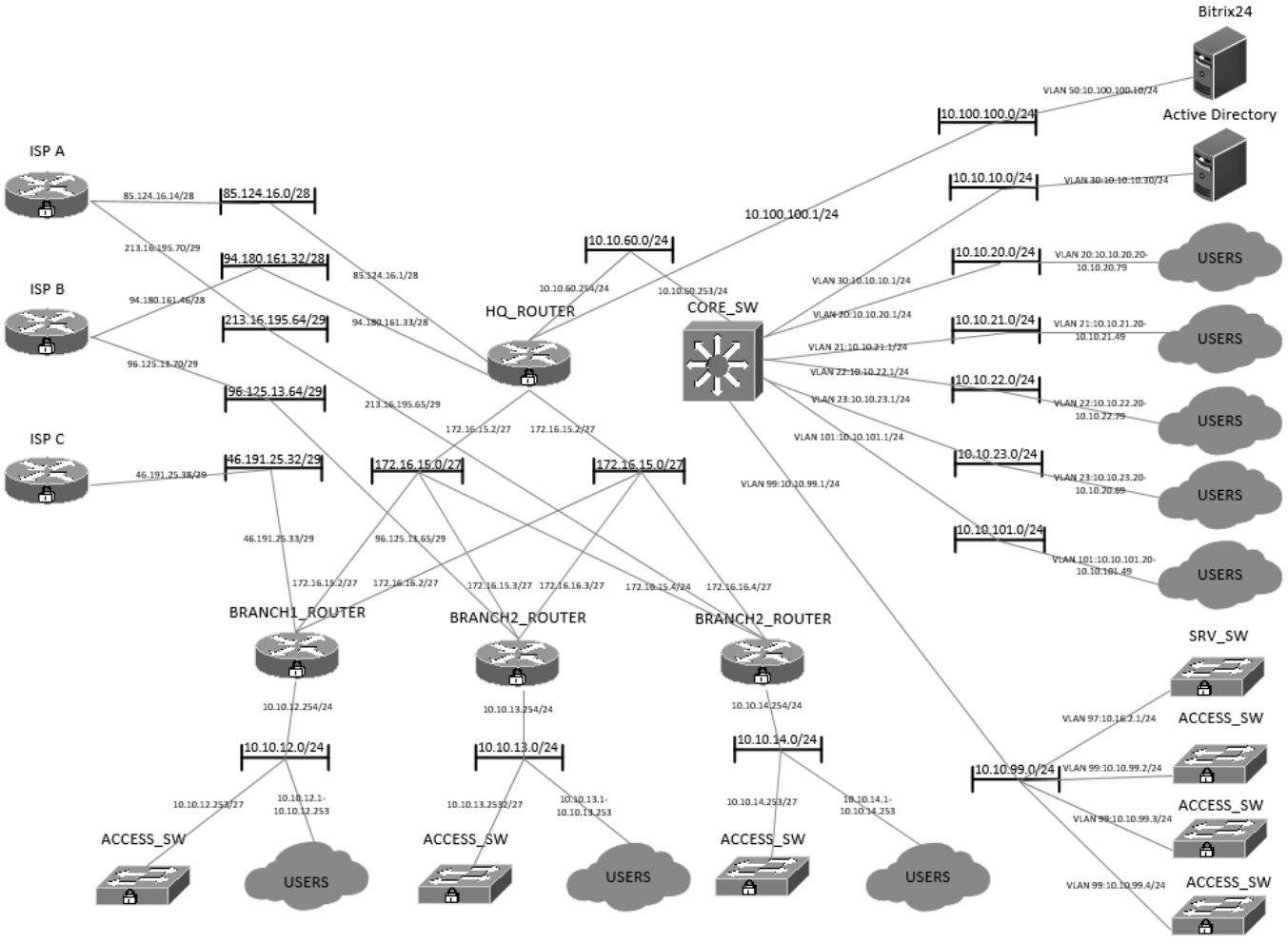

Рис. 2. Логическая схема разрабатываемой вычислительной сети

[5]. Созданные модули, как детали конструктора, из которых можно собрать сеть, соответствующую заданным требованиям. Эти же детали можно применять повторно (репликация), сильно сокращая время проектирования. Принцип репликации (повторения) элемента упрощает масштабируемость сети и ускоряет ее развертывание.

Разбиение большой сети на небольшие, простые для понимания, модули (уровни) способствует устойчивости сети за счет локализации возникающих проблем. Таким образом при возникновении какого-либо сбоя в сети необходимо определить на каком уровне возникла ошибка, затем приступать к ее решению, не затрагивая при этом другие модули сети.

При разработке компьютерной вычислительной сети будет использована иерархическая модель — она представляет собой фундамент для сетевой инфраструктуры: подключение пользователей, принтеров, сканеров, WAN маршрутизаторов, устройств безопасности, серверов и т.д. [6].

Структурная схема разрабатываемой сети показана на рис. 1 и отображает маршрутизаторы, коммутаторы, персональные компьютеры, межсетевые экраны, а также линии связи, соединяющие данные устройства.

На рис. 2 продемонстрирована логическая схема разрабатываемой вычислительной сети, которая описывает взаимодействие устройств между собой по протоколу IP, разбиение сетей на VLAN, организацию VPN туннелей и т.д.

Дальнейшая работа была реализована по следующему алгоритму:

1. составление таблицы адресов;
2. разработка структурной и логической схем корпоративной сети;
2.1. разработка структурной (физической) схемы сети;
2.2. разработка логической схемы сети;
3. выбор сетевого оборудования;
4. настройка корпоративной сети предприятия;
4.1. базовая настройка сетевых устройств Cisco;
4.2. настройка отказоустойчивого соединения провайдера пограничного маршрутизатора центрального офиса;
4.3. настройка DMVPN;
4.4. настройка межсетевых экранов;
4.5. настройка NAT на маршрутизаторах удаленных филиалов;
4.6. настройка локальной вычислительной сети филиала.

Заключение

Таким образом, в настоящей работе приведен алгоритм разработки корпоративной сети передачи данных предприятия. Сеть соответствует всем современным инженерным и архитектурным принципам и позволяет объединить в одно информационное пространство все филиалы компании, а также обеспечивает быстрый, централизованный, защищенный доступ к информации. Организованная корпоративная сеть имеет хорошую масштабируемость, которую была достигнута путем выбора оборудования, которое имеет дополнительные разъемы и высокую модульность, то есть может быть расширено при необходимости. Все оборудование подобрано для возможности роста предприятия в перспективе 5–7 лет.

Приведенные в данной работе настройки были проверены в многофункциональной программе моделирования сетей Graphical Network Simulator-3 (GNS3) — разработанная система показала полное соответствие предъявляемым требованиям.

ЛИТЕРАТУРА

1. Самойленко Н. DMVPN [Электронный ресурс] — Режим доступа: http://xgu.ru/wiki/dmvpn, свободный.
2. Мельников Д. А. Системы и сети передачи данных. Учебник/ Д. А. Мельников.—М.: РадиоСофт, 2015.— 149 с.
3. Леммл Т. CCNP. Маршрутизация. Учебное руководство / Т. Леммл.—М.: Лори, 2015.— 85 с.
4. Максимов Н. В. Компьютерные сети / Н. В. Максимов, И. И. Попов.—М.: Инфра-М, 2013.— 191 с.
5. Ольков Е. А. Архитектура корпоративных сетей [Электронный ресурс] / Режим доступа: http://blog.netskills.ru/p/blog-page.html, свободный.
6. Оптимальные сетевые решения [Электронный ресурс]: офиц. сайт.— ЕКБ., 2015.— Режим доступа: http://www.ons.ru, свободный.

© Набиев Рафит Ренатович (nabievrafit@mail.ru), Зайцев Александр Валерьевич (realtime555@mail.ru).

Журнал «Современная наука: актуальные проблемы теории и практики»