

Министерство образования и науки Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ Н.Г.ЧЕРНЫШЕВСКОГО

Кафедра дискретной
математики и информационных
технологий

Проектирование корпоративной сети.

АВТОРЕФЕРАТ БАКАЛАВРСКОЙ РАБОТЫ

Студента 4 курса 421 группы
направления 09.03.01 – Информатика и вычислительная техника
факультета КНиИТ
Егорова Дениса Владиславовича

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

В.А Поздняков

Заведующий кафедрой
доцент, к.ф.-м.н., доцент

Л.Б. Тяпаев

Саратов 2017

ВВЕДЕНИЕ

Актуальность выбранной темы состоит в том, что корпоративная сеть является средством для организации эффективного функционирования предприятия, которое может выражаться различными факторами: увеличение прибыли предприятия, повышение качества работы сотрудников, эффективное взаимодействие различных отделов предприятия.

Целью бакалаврской работы является создание проекта корпоративной сети. Для достижения этой цели были сформулированы следующие задачи:

1. изучить технологии, необходимые для создания сети;
2. выбрать топологию сети;
3. создать IP-план;
4. выбрать активное оборудование;
5. осуществить настройку активного оборудования и серверов.

Работа состоит из введения, двух глав, заключения и списка использованных источников. В первой главе рассмотрены основные технологии, использующиеся при построении корпоративной сети. Во второй главе описана реализация проекта корпоративной сети. В заключении сделаны выводы о проделанной работе.

Основное содержание работы

1 Основные технологии, использующиеся в корпоративной сети

1.1 Трехуровневая иерархическая модель компании Cisco

Современные крупные сети очень сложны, поскольку определяются множеством протоколов, конфигурациями и технологиями. С помощью иерархии можно упорядочить все компоненты в легко анализируемой модели, распределить объекты по уровням, а так же указать связи между объектами и функции этих объектов.

В модели определены три уровня:

- Базовый уровень или уровень ядра (Core layer)
- Уровень распространения (Distribution layer)
- Уровень доступа (Access layer)

Каждый уровень отвечает за реализацию определенных функций. Однако эти уровни являются логическими и не обязательно согласованы с физическими устройствами.

Базовый уровень формирует ядро сети. На самом верху иерархии этот уровень отвечает за быструю и надежную пересылку больших объемов трафика. Трафик передается на базовом уровне совместно для нескольких пользователей. Однако на уровне распределения обрабатываются пользовательские данные, что может привести к дополнительным запросам в базовый уровень.

Уровень распространения расположен между базовым уровнем и уровнем доступа. Основные функции уровня распространения состоят в маршрутизации, фильтрации и доступе к региональным сетям, а также (если необходимо) в определении правил доступа пакетов к базовому уровню. Уровень распространения обязан устанавливать наиболее быстрый способ обработки запросов к службам.

На уровне доступа реализовано управление пользователями и рабочими группами при обращении к ресурсам объединенной сети.

Наибольшая часть необходимых пользователям сетевых ресурсов должна быть доступна локально. На уровне распределения выполняется перенаправление трафика к удаленным службам.

1.2 Виртуальные локальные сети

Любой широковещательный пакет пересылается всем устройствам, вне зависимости от того, нужно ли устройству принимать эти данные.

Увеличение количества пользователей и устройств приводит к увеличению количества широковещательных рассылок и пакетов, обрабатываемых каждым устройством.

Нельзя отменить широковещательные рассылки в устройстве и ответы пользователей на эти рассылки.

Создание виртуальной локальной сети VLAN помогает решить эту проблему

Все устройства сети VLAN являются членами одного широковещательного домена и получают все широковещательные рассылки. По умолчанию широковещательные рассылки фильтруются на всех портах коммутаторов, которые не являются членами одной сети VLAN.

Для отслеживания кадров, перемещающихся через коммутационную фабрику, используется идентификатор VLAN. Он отмечает принадлежность кадров определенной сети VLAN. Существует несколько методов отслеживания кадров в магистральных связях.

1.3 Протокол покрывающего дерева

Для связи между переключателями полезны избыточные соединения, которые помогают предотвратить отказ сети при выходе из строя отдельной связи. Несмотря на полезность избыточных соединений, они создают гораздо больше проблем, чем решают. Поскольку кадры одновременно передаются в широковещательных рассылках по всем дублирующим соединениям, могут возникать зацикливания.

Протокол STP позволяет найти все связи в сети и выделить среди них избыточные, чтобы отключить избыточные связи и тем самым устранить любые заикливания в сети.

1.4 Протоколы динамической маршрутизации

Динамическая маршрутизация — это процесс использования протокола для поиска и обновления таблиц маршрутизации в устройствах. Динамическая маршрутизация проще статической, но требует существенных ресурсов процессора маршрутизатора и полосы пропускания сетевых линий связи. Протокол маршрутизации определяет набор правил, используемых маршрутизаторами для взаимодействия с соседними маршрутизаторами.

1.5 NAT

NAT (Network Address Translation) – трансляция сетевого адреса. Механизм, применение которого позволяет сократить число глобально уникальных IP-адресов. Организации, не обладающие глобально уникальными адресами, могут подключаться к Интернету, используя NAT для трансляции своих адресов внутрь пространства глобально маршрутизируемых адресов.

1.6 Протокол DHCP

Для нормальной работы сети каждому сетевому интерфейсу компьютера и маршрутизатора должен быть назначен IP-адрес. Протокол динамического конфигурирования хостов (Dynamic Host Configuration Protocol, DHCP) автоматизирует процесс конфигурирования сетевых интерфейсов, обеспечивая отсутствие дублирования адресов за счет централизованного управления их распределением.

Протокол DHCP работает в соответствии с моделью клиент-сервер. Во время старта системы компьютер, являющийся DHCP-клиентом, посылает в сеть широковещательный запрос на получение IP-адреса. DHCP-сервер откликается и посылает сообщение-ответ, содержащее IP-адрес и некоторые другие конфигурационные параметры.

Администратор управляет процессом конфигурирования сети, определяя два основных конфигурационных параметра DHCP-сервера: пул адресов, доступных для распределения, и срок аренды. Срок аренды диктует, как долго компьютер может использовать назначенный IP-адрес, перед тем как снова запросить его от DHCP-сервера.

1.7 Система DNS

В стеке TCP/IP применяется доменная система имен, которая имеет иерархическую древовидную структуру, допускающую наличие в имени произвольного количества составных частей. Иерархия доменных имен аналогична иерархии имен файлов, принятой во многих популярных файловых системах. Дерево имен начинается с корня, обозначаемого здесь точкой (.). Затем следует старшая символьная часть имени, вторая по старшинству символьная часть имени и т. д. Младшая часть имени соответствует конечному узлу сети.

Для каждого домена имен создается свой DNS-сервер. На серверах применяют два подхода к распределению имен. В первом случае сервер может хранить отображения «доменное имя — IP-адрес» для всего домена, включая все его поддомены. Однако такое решение оказывается плохо масштабируемым, так как при добавлении новых поддоменов нагрузка на этот сервер может превысить его возможности. Чаще используется другой подход, когда сервер домена хранит только имена, которые заканчиваются на следующем ниже уровне иерархии по сравнению с именем домена. Именно при такой организации службы DNS нагрузка по разрешению имен распределяется равномерно между всеми DNS-серверами сети.

Каждый DNS-сервер помимо таблицы отображений имен содержит ссылки на DNS-серверы своих поддоменов. Эти ссылки связывают отдельные DNS-серверы в единую службу DNS. Ссылки представляют собой IP-адреса соответствующих серверов.

Для ускорения поиска IP-адресов DNS-серверы широко применяют кэширование проходящих через них ответов. Чтобы служба DNS могла оперативно обрабатывать изменения, происходящие в сети, ответы кэшируются на относительно короткое время — обычно от нескольких часов до нескольких дней.

2 ПРОЕКТ КОРПОРАТИВНОЙ СЕТИ

Проектируемая сеть основывается на трехуровневой иерархической модели. Согласно этой модели сеть подразделяется на:

- Уровень доступа
- Уровень распределения
- Базовый уровень

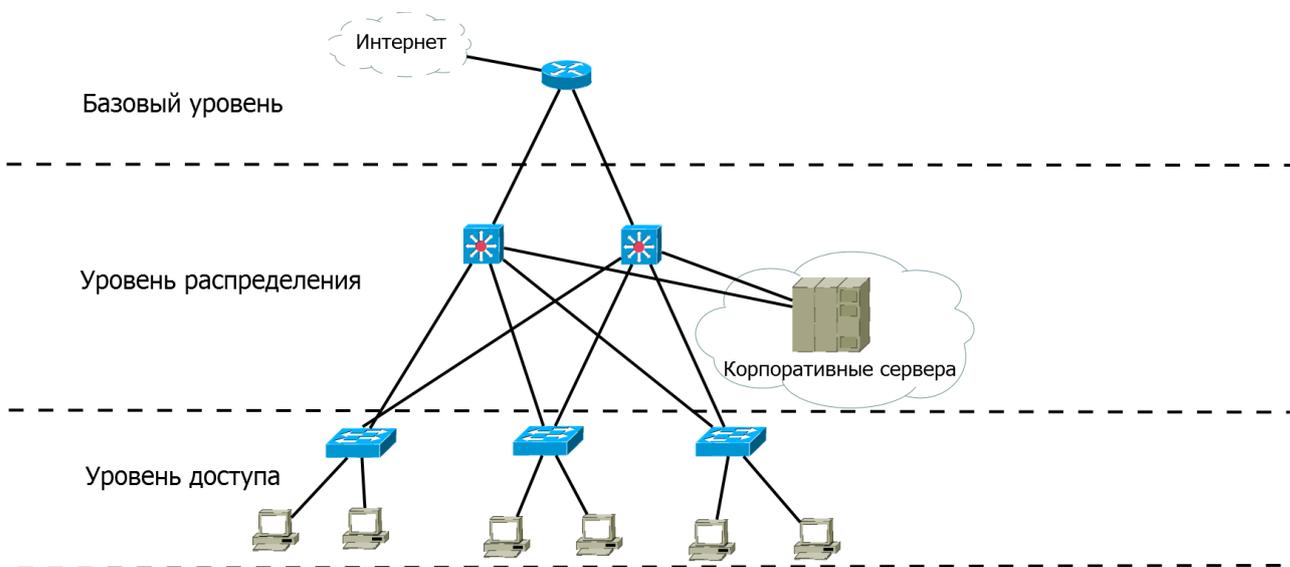


Рисунок 1 – Схема корпоративной сети

Уровень доступа предназначен для подключения конечных устройств. Он представлен коммутаторами второго уровня, к которым подключены пользователи.

Уровень распределения предназначен для агрегации трафика и маршрутизации во VLAN. Этот уровень представлен высокопроизводительными коммутаторами третьего уровня.

Базовый уровень, так же является границей сети. Он представлен маршрутизатором, основной задачей которого является предоставление доступа к сети интернет.

Для раздачи адресов внутри сети выбран частный диапазон 172.16.0.0/12, обладающий 20 битами адресного пространства. План IP-адресации представлен в таблице 1.

Таблица 1 – IP-план.

№ VLAN	IP-адрес	Примечание
VLAN 1		Стандартный VLAN. Не используется
VLAN 2	172.16.2.0/24	1-е подразделение
	172.16.2.1	Шлюз
	172.16.2.2 – 172.16.2.254	Пул устройств
VLAN 3	172.16.3.0/24	2-е подразделение
	172.16.3.1	Шлюз
	172.16.3.2 – 172.16.3.254	Пул устройств
VLAN 4	172.16.4.0/24	3-е подразделение
	172.16.4.1	Шлюз
	172.16.4.2 – 172.16.4.254	Пул устройств
VLAN 5	172.16.5.0/24	4-е подразделение
	172.16.5.1	Шлюз

	172.16.5.2 – 172.16.5.254	Пул устройств
VLAN 6	172.16.6.0/24	5-е подразделение
	172.16.6.1	Шлюз
	172.16.6.2 – 172.16.6.254	Пул устройств
VLAN 7	172.16.7.0/24	Маршрутизатор
	172.16.7.1	Шлюз
	172.16.7.2 – 172.16.7.254	Пул устройств
VLAN 8	172.16.1.0/24	Выделен под сервера
	172.16.1.1	Шлюз
	172.16.1.2 – 172.16.1.254	Пул устройств
VLAN 9	172.16.0.0/24	Управление
	172.16.0.1	Шлюз
	172.16.0.2 – 172.16.0.254	Пул устройств

В дипломной работе требуется выбрать следующее сетевое оборудование:

- коммутатор рабочих групп
- коммутатор уровня распределения
- маршрутизатор доступа в интернет

Будет использоваться оборудование фирмы Cisco Systems. Выбор фирмы обусловлен высокой надежностью оборудования, а так же наличием подробной и разнообразной документации.

Коммутаторы рабочих групп служат для непосредственного подключения компьютеров к сети. От них не требуется высокой производительности и поддержки маршрутизации. В качестве коммутатора рабочих групп выбран коммутатор Cisco Catalyst 2960 Plus на 24 порта Fast Ethernet.

В качестве коммутатора уровня распределения выбран коммутатор Cisco 3650 на 24 порта Gigabit Ethernet. Через уровень распределения проходит большое количество пакетов, а значит, следует обеспечить его отказоустойчивость. Для этой цели необходимо продублировать коммутатор 3-го уровня со всеми подключениями.

Маршрутизатор доступа к сети Интернет должен выполнять фильтрацию пакетов и трансляцию адресов, а также поддерживать безопасность на периметре сети, выполняя функции основного шлюза. Для этого он оснащается встроенным межсетевым экраном (Firewall). Этим требованиям удовлетворяет маршрутизатор Cisco 2921.

Расчет стоимости активного оборудования при проектировании сети приведен в таблице 2.

Таблица 2 – Расчет стоимости активного оборудования

Наименование	Цена, руб.	Количество, шт.	Стоимость, руб.
Коммутаторы			
Cisco Catalyst WS-C2960+24LC-L	55450	4	221800
Cisco WS-C3650-24TS-S	139236	2	278472
Маршрутизаторы			
Cisco 2921-SEC/K9	164569	1	164569

Итого:	664841
---------------	--------

Для работы сети были настроены следующие технологии и сервера:

Виртуальные локальные сети. С помощью технологии VLAN уменьшается количество широковещательных запросов, которые снижают пропускную способность сети. Для настройки VLAN необходимо установить режим работы портов (access или trunk), и присвоить им номера VLAN.

Access port — порт доступа — к нему подключаются, как правило, конечные узлы. За каждым access-портом закреплён один определённый VLAN.

Trunk port. Порты через которые передаётся трафик нескольких VLAN.

На коммутаторе уровня распределения создаются виртуальные порты, и устанавливаются как шлюз по умолчанию для каждого из VLAN.

Для обеспечения отказоустойчивости на уровне распределения были продублированы коммутаторы, что привело к созданию петель. Для решения этой проблемы используется Протокол покрывающего дерева или Spanning Tree Protocol. Коммутаторы, работающие по этому протоколу, отключают запасные пути. В случае если одна из линий связи перестанет работать, коммутаторы перестраивают топологию сети таким образом, чтобы она имела вид покрывающего дерева - охватывала бы все узлы, но при этом не имела петель. Покрывающее дерево строится отдельно для каждой виртуальной локальной сети.

Для маршрутизации трафика между коммутаторами уровня распределения и маршрутизатором был настроен протокол динамической маршрутизации EIGRP. Для настройки протокола EIGRP необходимо указать номер автономной системы и подключенные к устройству сети, для которых необходима маршрутизация.

Технология NAT необходима для доступа к сети Интернет. NAT используется для отображения частных ip-адреса в публичные. Для ее настройки необходимо указать какие порты маршрутизатора будут внутренними, а какие внешними. После настройки интерфейсов нужно создать список доступа, в котором будет определено для каких подсетей используется NAT и включить NAT для этого списка доступа.

Для автоматической раздачи ip-адресов внутри сети, настраивается DHCP сервер. В конфигурационный файл вносится информация о сети, а именно подсети для которых настраивается служба DHCP, диапазон выдаваемых адресов, шлюз по умолчанию, срок аренды адреса и так далее.

Далее создается DNS сервер. В конфигурационных файлах указываются адреса которые будет обслуживать dns сервер, адреса вышестоящих dns серверов, dns зона и информация о домене.

ЗАКЛЮЧЕНИЕ

За время работы над бакалаврским проектом, была изучена специальная литература, разобраны основные понятия, необходимые для создания проекта корпоративной сети. Были выполнены следующие задачи: выбрана топология сети, создан IP-план сети, подобрано активное оборудование, подсчитана его общая стоимость, а так же выполнена настройка оборудования и серверов. Таким образом, был создан проект корпоративной сети, что и являлось целью бакалаврской работы.