МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ УКРАИНЫ
ЧЕРНИГОВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ
КАФЕДРА ИНФОРМАЦИОННЫХ И КОМПЬЮТЕРНЫХ СИСТЕМ

ГЛОБАЛЬНЫЕ СЕТИ

Методические указания
к выполнению лабораторных работ по дисциплине
„Новейшие архитектуры и средства построения
глобальных и корпоративных сетей”
для студентов специальностей
8.05010201 “Компьютерные системы и сети”
8.05010202 “Системное программирование”
8.05010203 “Специализированные компьютерные системы”

Утверждено
на заседании кафедры
информационных и компьютерных систем

Протокол № 10 от «18» апреля 2013 г.

Чернигов ЧГТУ 2013

Глобальні мережі. Методичні вказівки до виконання лабораторних робіт з дисципліни “Новітні архітектури та засоби побудови глобальних та корпоративних мереж” для студентів спеціальностей 8.05010201 “Комп’ютерні системи та мережі”, 8.05010202 “Системне програмування”, 8.05010203 “Спеціалізовані комп’ютерні системи” / Укл. Є. В. Риндич. – Чернігів: ЧДТУ, 2013. – 16 с., рос. мовою.

Укладачі: Риндич Євген Володимирович, кандидат технічних наук, доцент кафедри інформаційних та комп’ютерних систем

Відповідальний за випуск: Казимир Володимир Вікторович, завідувач кафедри інформаційних та комп’ютерних систем, доктор технічних наук, професор

Рецензент: Нікітенко Євгеній Васильович, кандидат фізико-математичних наук, доцент кафедри інформаційних та комп’ютерних систем Чернігівського державного технологічного університету

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Глобальные сети(WAN) – это сети передачи данных, которые работают за пределами географического охвата локальной сети.

Глобальные сети отличаются от локальных сетей методами соединения элементов такой сети, наличием различных технологий доступа, которые могут использоваться одновременно. Основным отличием глобальных сетей является их географическая расположенность и не возможность использовать технологии доступа и передачи данных для объединения локальных и территориально рассредоточенных компонентов сети.

Зачастую организацией или предоставлением доступа занимаются провайдеры. Глобальные компьютерные сети могут использовать возможности по передаче данных, предоставляемые другими поставщиками услуг, например, компании предоставляющие услуги телефонной или спутниковой связи. В глобальных сетях обычно передаются различные типы трафика, такие как передача голоса, данных и видео.

В глобальных сетях намного более важно не качество связи, а сам факт ее существования. Правда, в настоящий момент уже нельзя провести четкий и однозначный предел между локальными и глобальными сетями. Большинство локальных сетей имеют выход в глобальную сеть, но характер переданной информации, принципы организации обмена, режимы доступа к ресурсам внутри локальной сети, как правило, сильно отличаются от тех, что приняты в глобальной сети. И хотя все компьютеры локальной сети в данном случае включены также и в глобальную сеть, специфику локальной сети это не отменяет. Возможность выхода в глобальную сеть остается всего лишь одним из ресурсов, поделенным пользователями локальной сети.

1 Лабораторная работа №1. Введение в WAN. Конфигурирование и настройка инфраструктуры сети

1.1 Цель работы

Ознакомиться с особенностями реализации глобальных сетей, изучить их характеристики. Ознакомиться и получить практические навыки конфигурирования глобальных сетей.

1.2 Краткие теоретические сведения

Наиболее важным этапом глобальной сети является использование маршрутизаторов – сетевых устройств, принадлежащих к 3 уровню модели OSI, и их конфигурирование.

Маршруты могут задаваться административно (статические маршруты), либо вычисляться с помощью алгоритмов маршрутизации, базируясь на информации о топологии и состоянии сети, полученной с помощью протоколов маршрутизации (динамические маршруты).

Статическими маршрутами могут быть:

— маршруты, не изменяющиеся во времени;

— маршруты, изменяющиеся по расписанию.

Маршрутизация в компьютерных сетях типично выполняется специальными программно-аппаратными средствами — маршрутизаторами; в простых конфигурациях может выполняться и компьютерами общего назначения, соответственно настроенными.

Маршрутизатор — специализированный сетевой компьютер, имеющий минимум два сетевых интерфейса и пересылающий пакеты данных между различными сегментами сети, принимающий решения о пересылке на основании информации о топологии сети и определённых правил, заданных администратором.

Маршрутизаторы делятся на программные и аппаратные. Маршрутизатор работает на более высоком «сетевом» уровне 3 сетевой модели OSI, нежели коммутатор (или сетевой мост) и концентратор (хаб), которые работают на 2 уровне и 1 уровне модели OSI соответственно.

Обычно маршрутизатор использует адрес получателя, указанный в пакетных данных, и определяет по таблице маршрутизации путь, по которому следует передать данные. Если в таблице маршрутизации для адреса нет описанного маршрута, пакет отбрасывается.

Существуют и другие способы определения маршрута пересылки пакетов, когда, например, используется адрес отправителя, используемые протоколы верхних уровней и другая информация, содержащаяся в заголовках пакетов сетевого уровня. Нередко маршрутизаторы могут осуществлять трансляцию адресов отправителя и получателя, фильтрацию транзитного потока данных на основе определённых правил с целью ограничения доступа, шифрование/расшифрование передаваемых данных и т. д.

При построении маршрутов ключевым является отсутствие петель в маршрутах распространения пакетов. Маршрутные петли не возникают в сети передачи данных, в которой маршрутизация поддерживается средствами одного протокола маршрутизации, пока не нарушены ограничения протокола, такие как максимальное количество переходов, в маршруте к сети получателю, а сетевое оборудование и его программное обеспечение работают в нормальном режиме.

В случае если маршрутизация в сети передачи данных поддерживается с помощью более чем одного протокола маршрутизации или комбинации статической и динамической маршрутизации, возникает возможность возникновения маршрутных петель. Эта возможность увеличивается при перераспределении маршрутной информации между протоколами маршрутизации. Поскольку в процессе перераспределения объединяются домены отдельных протоколов маршрутизации, тогда как метрические домены остаются отдельными. Сети получатели, находящиеся в пределах одного домена протокола маршрутизации, становятся доступными из домена другого протокола маршрутизации с одной и той же метрикой.

1.3 Ход работы

1. Подготовить сеть или модель сети с использованием Cisco Packet Tracer, которая показана на рисунке 1.1. Таблица адресации представлена в таблице 1.1.

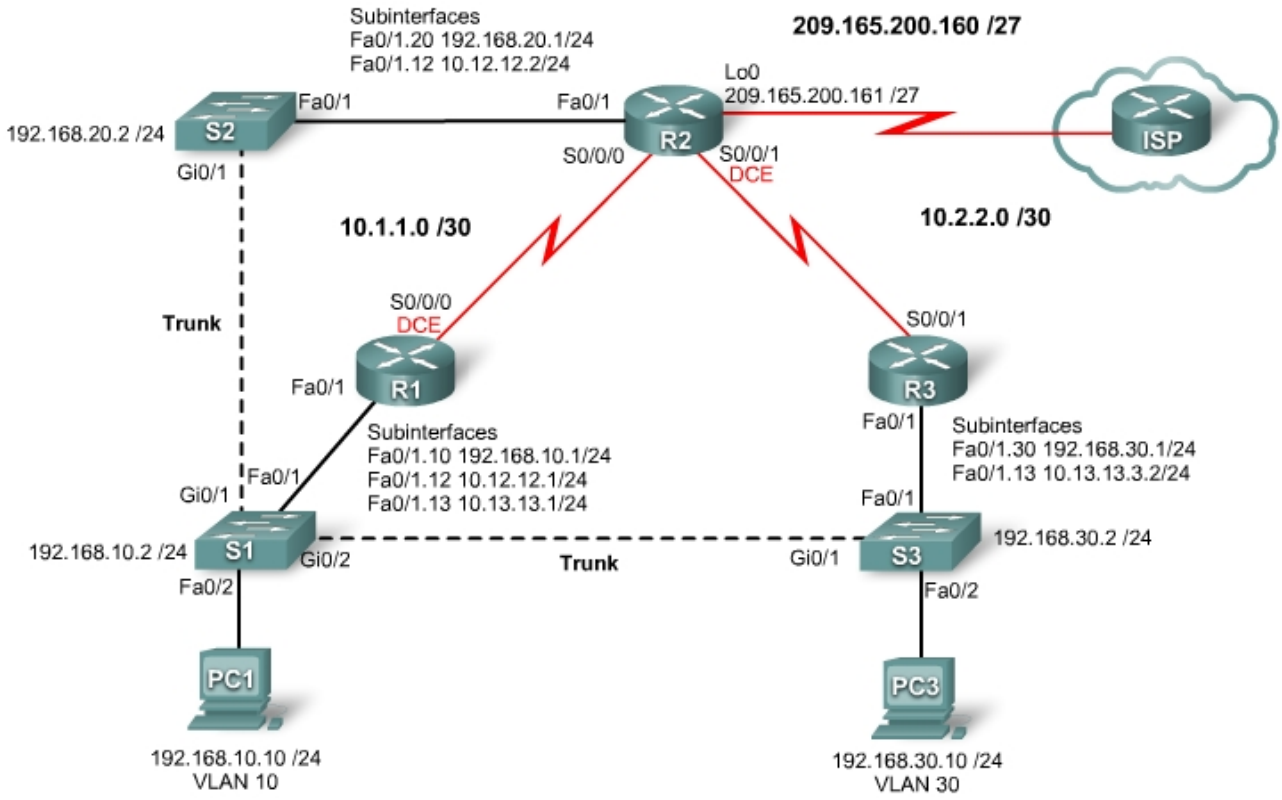

Рисунок 1.1 – Топология сети

Таблица 1.1 – Таблица адресации

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	**Fa0/1**	N/A	N/A	N/A
	Fa0/1.10	192.168.10.1	255.255.255.0	N/A
	Fa0/1.12	10.12.12.1	255.255.255.0	N/A
	Fa0/1.13	10.13.13.1	255.255.255.0	N/A
	S0/0/0	10.1.1.1	255.255.255.252	N/A
R2	**Fa0/1**	N/A	N/A	N/A
	Fa0/1.12	10.12.12.2	255.255.255.0	N/A
	Fa0/1.20	192.168.20.1	255.255.255.0	N/A
	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
R3	**Fa0/1**	N/A	N/A	N/A
	Fa0/1.13	10.13.13.3	255.255.255.0	N/A
	Fa0/1.30	192.168.30.1	255.255.255.0	N/A
	S0/0/1	10.2.2.2	255.255.255.252	N/A
S1	**VLAN10**	192.168.10.2	255.255.255.0	192.168.10.1
S2	**VLAN20**	192.168.20.2	255.255.255.0	192.168.20.1
S3	**VLAN30**	192.168.30.2	255.255.255.0	192.168.30.1
PC1	**NIC**	192.168.10.10	255.255.255.0	192.168.10.1
PC3	**NIC**	192.168.30.10	255.255.255.0	192.168.30.1

2. Настроить R1, R2, R3 и маршрутизаторы S1, S2, S3 в соответствии со следующими принципами:
   - настройка имени хоста;
   - отключить DNS-поиска;
   - настройка EXEC- режима пароля, как "class";
   - настройка следующее ежедневного сообщения-баннера: «Unauthorized access strictly prohibited and prosecuted to the full extent of the law";
   - настройка пароля для консоли соединений;
   - настройка синхронной регистрации;
   - настройка пароля для VTY соединений;
   - сохранение текущей конфигурации в NVRAM.
3. Настроить и активировать последовательный и Ethernet адреса.
4. Настроить STP
5. Настроить VTP
6. Настроить сети VLAN
7. Настроить маршрутизацию RIP
8. Настроить маршрутизацию OSPF
9. Настроить маршрутизацию EIGRP

1.4 Содержание отчета

1. Описание методов решения поставленных задач.
2. Процесс конфигурирования, скриншоты.
3. Анализ полученных графических зависимостей.
4. Графики и расчеты пропускной способности.
5. Схема и анализ структуры сети.

6. Результаты и описание выполненных команд.

1.5 Контрольные вопросы

1. В чем особенности работы протокола RIP?
2. В чем особенности работы протокола OSPF?
3. В чем особенности работы протокола EIGRP?
4. Как работает протокол STP? Какие есть альтернативы данному протоколу?
5. Как создать VLAN, если компьютеры находятся в разных городах?

2 Лабораторная работа №2. Основы конфигурирования безопасности

2.1 Цель работы

Изучить особенности конфигурирования безопасной компьютерной сети.

2.2 Краткие теоретические сведения

Сетевой анализатор Wireshark (Ethereal) построен на той же библиотеке (libpacap), что и утилита tcpdump, но имеет удобный графический пользовательский интерфейс и гораздо больше возможностей по сортировке и фильтрации информации. Программа позволяет пользователю просматривать весь проходящий по сети трафик в режиме реального времени, переводя сетевую карту в неразборчивый режим (promiscuous mode).

Wireshark — это приложение, которое «знает» структуру самых различных сетевых протоколов, и поэтому позволяет разобрать сетевой пакет, отображая значение каждого поля протокола любого уровня. Поскольку для захвата пакетов используется pcap, существует возможность захвата данных только из тех сетей, которые поддерживаются этой библиотекой. Тем не менее, Wireshark умеет работать с множеством форматов входных данных, соответственно, можно открывать файлы данных, захваченных другими программами, что расширяет возможности захвата.

Протокол маршрутной информации(Routing Information Protocol) позволяет маршрутизаторам динамически обновлять маршрутную информацию (направление и дальность в хопах), получая ее от соседних маршрутизаторов.

Протокол RIP предотвращает появление петель в маршрутизации, по которым пакеты могли бы циркулировать неопределенно долго, устанавливая максимально допустимое количество переходов на маршруте от отправителя к получателю. Стандартное максимальное значение количества переходов равно 15.При получении маршрутизатором обновление маршрутов, содержащего новую или измененную запись, он увеличивает значение метрики на единицу.

Если при этом значение метрики превышает 15, то считается бесконечно большим, и сеть-получатель считается недостижимой. Протокол RIP обладает рядом функций, которые являются общими для него и других протоколов маршрутизации. Например, он позволяет использовать механизмы расщепления горизонта и таймеры удержания информации для предотвращения распространения некорректных сведений о маршрутах.

Маршрутизаторы RIP записывают только наилучший маршрут к пункту назначения, однако могут поддерживать и несколько маршрутов, если они имеют одинаковые значения метрики.

После обновления таблицы маршрутизации, вследствие изменения топологи сети маршрутизатор сразу начинает рассылать сообщения об обновлении маршрутов, для того чтобы проинформировать другие маршрутизаторы о произошедших изменениях. Обновления рассылаются независимо от обычных регулярных сообщений RIP-маршрутизаторов.

2.3 Ход работы

1. Настроить сеть согласно схемы, показанной на рисунке 2.1, и таблицы адресации 2.1.

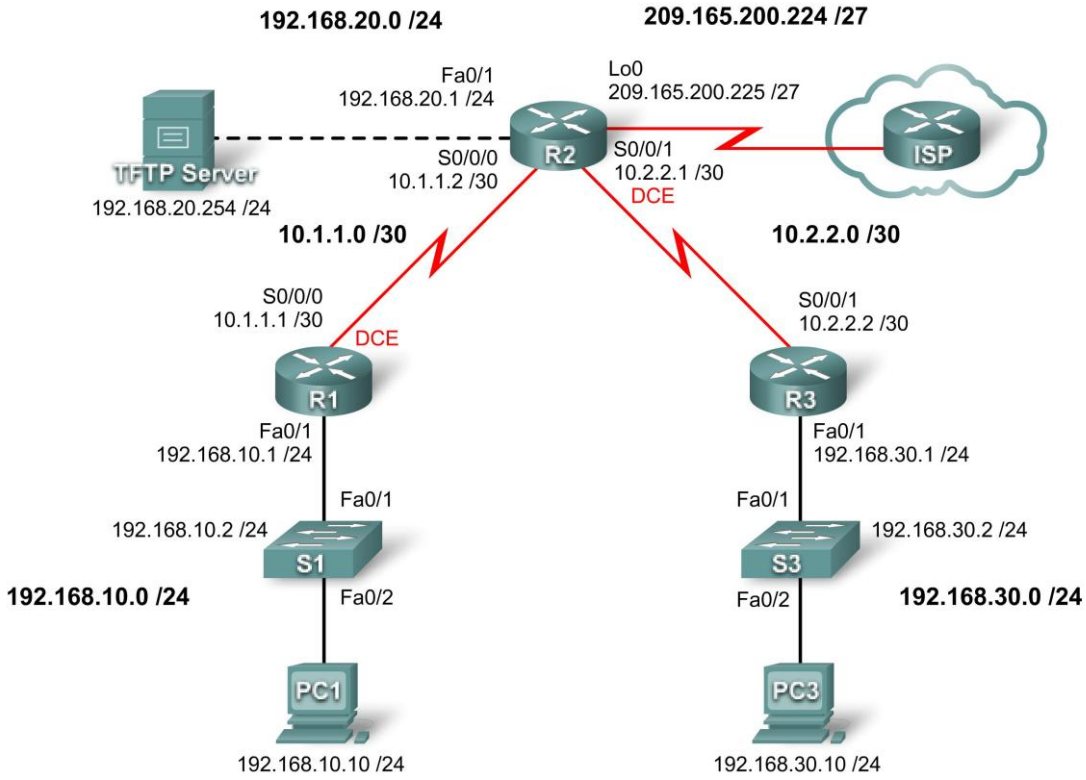

Рисунок 2.1 – Топология сети

Таблица 2.1 – Таблица адресации

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/1	192.168.10.1	255.255.255.0	N/A
	S0/0/0	10.1.1.1	255.255.255.252	N/A
R2	Fa0/1	192.168.20.1	255.255.255.0	N/A
	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
	Lo0	209.165.200.225	255.255.255.224	N/A
R3	Fa0/1	192.168.30.1	255.255.255.0	N/A
	S0/0/1	10.2.2.2	255.255.255.252	N/A
S1	VLAN10	192.168.10.2	255.255.255.0	N/A
S3	VLAN20	192.168.30.2	255.255.255.0	N/A
PC1	NIC	192.168.10.10	255.255.255.0	192.168.10.1
PC3	NIC	192.168.30.10	255.255.255.0	192.168.30.1
TFTP Server	NIC	192.168.20.254	255.255.255.0	192.168.20.1

2. Настроить маршрутизаторы согласно таблице 2.1.
3. Настроить сетевые интерфейсы.
4. Защитить маршрутизатор от несанкционированного доступа:
   – настройте безопасные пароли и аутентификацию AAA;
   – защитите консоль и VTY линии.
5. Организуйте безопасный доступ к сети используя RIP.
6. Настройте ведение журнала с SNMP (Simple Network Management Protocol).
7. Отключите неиспользуемые Cisco Network Services.
8. Настройте Cisco IOS и произведите конфигурирование соответствующих файлов.
9. Настроить использование SDM для обеспечения маршрутизатора.
10. Подробно опишите все произведенные действия с указанием необходимых параметров.

2.4 Содержание отчета

Отчет должен содержать последовательность скриншотов по ходу выполнения работы и соответствующие комментарии.

2.5 Контрольные вопросы

1. Какой добавить маршрут?
2. Какой параметр отвечает за ведение журнала?
3. Перечислите конфигурационные файлы.
4. Опишите основные функции Cisco IOS.
5. Как настроить безопасную маршрутизацию RIP?

3 Лабораторная работа №3. Изучение и настройка сетевых сервисов DHCP и NAT

3.1 Цель работы

Изучить сетевой протокол DHCP и преобразование сетевых адресов NAT в глобальных сетях.

3.2 Краткие теоретические сведения

DHCP (Dynamic Host Configuration Protocol — протокол динамической конфигурации узла) — это сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP. Данный протокол работает по модели «клиент-сервер». Для автоматической конфигурации компьютер-клиент на этапе конфигурации сетевого устройства обращается к так называемому серверу DHCP, и получает от него нужные параметры. Сетевой администратор может задать диапазон адресов, распределяемых сервером среди компьютеров. Это позволяет избежать ручной настройки компьютеров сети и уменьшает количество ошибок. Протокол DHCP используется в большинстве сетей TCP/IP.

Протокол DHCP предоставляет три способа распределения IP-адресов:

1. Ручное распределение. При этом способе сетевой администратор сопоставляет аппаратному адресу (для Ethernet сетей – это MAC-адрес) каждого клиентского компьютера определённый IP-адрес. Фактически, данный способ распределения адресов отличается от ручной настройки каждого компьютера лишь тем, что сведения об адресах хранятся централизованно (на сервере DHCP), и потому их проще изменять при необходимости.
2. Автоматическое распределение. При данном способе каждому компьютеру на постоянное использование выделяется произвольный свободный IP-адрес из определённого администратором диапазона.
3. Динамическое распределение. Этот способ аналогичен автоматическому распределению, за исключением того, что адрес выдаётся компьютеру не на постоянное пользование, а на определённый срок. Это называется арендой адреса. По истечении срока аренды IP-адрес вновь считается свободным, и клиент обязан запросить новый (он, впрочем, может оказаться тем же самым). Кроме того, клиент сам может отказаться от полученного адреса.

NAT (Network Address Translation) — это механизм в сетях TCP/IP, позволяющий преобразовывать IP-адреса транзитных пакетов.

Преобразование адресов методом NAT может производиться почти любым маршрутизирующим устройством — маршрутизатором, сервером доступа, межсетевым экраном. Наиболее популярным является SNAT, суть механизма которого состоит в замене адреса источника (source) при прохождении пакета в одну сторону, и обратной замене адреса назначения

(destination) в ответном пакете. Наряду с адресами источник/назначение могут также заменяться номера портов источника и назначения.

Принимая пакет от локального компьютера, роутер смотрит на IP-адрес назначения. Если это локальный адрес, то пакет пересылается другому локальному компьютеру. Если нет, то пакет надо переслать наружу в интернет. Но ведь обратным адресом в пакете указан локальный адрес компьютера, который из интернета будет недоступен. Поэтому роутер «на лету» производит трансляцию IP-адреса и порта и запоминает эту трансляцию у себя во временной таблице. Через некоторое время после того, как клиент и сервер закончат обмениваться пакетами, роутер сотрет у себя в таблице запись о n-ом порте за сроком давности.

Помимо source NAT (предоставления пользователям локальной сети с внутренними адресами доступа к сети Интернет) часто применяется также destination NAT, когда обращения извне транслируются межсетевым экраном на компьютер пользователя в локальной сети, имеющий внутренний адрес и потому недоступный извне сети непосредственно (без NAT).

Существует 3 базовых концепции трансляции адресов: статическая (Static Network Address Translation), динамическая (Dynamic Address Translation), маскарадная (NAPT, NAT Overload, PAT).

1. Статический NAT — Отображение незарегистрированного IP-адреса на зарегистрированный IP-адрес на основании один к одному. Особенно полезно, когда устройство должно быть доступным снаружи сети.
2. Динамический NAT — Отображает незарегистрированный IP-адрес на зарегистрированный адрес от группы зарегистрированных IP-адресов. Динамический NAT также устанавливает непосредственное отображение между незарегистрированным и зарегистрированным адресом, но отображение может меняться в зависимости от зарегистрированного адреса, доступного в пуле адресов, во время коммуникации.
3. Перегруженный NAT (NAPT, NAT Overload, PAT, маскарадинг) — форма динамического NAT, который отображает несколько незарегистрированных адресов в единственный зарегистрированный IP-адрес, используя различные порты. Известен также как PAT (Port Address Translation). При перегрузке каждый компьютер в частной сети транслируется в тот же самый адрес, но с различным номером порта.

NAT Traversal (прохождение или автонастройка NAT) — это набор возможностей, позволяющих сетевым приложениям определять, что они находятся за устройством, обеспечивающим NAT, узнавать внешний IP-адрес этого устройства и выполнять сопоставление портов для пересылки пакетов из внешнего порта NAT на внутренний порт, используемый приложением; все это выполняется автоматически, пользователю нет необходимости вручную настраивать сопоставления портов или вносить изменения в какие-либо другие параметры. Однако существуют меры предосторожности в доверии к таким приложениям — они получают

обширный контроль над устройством, появляются потенциальные уязвимости.

3.3 Ход работы

1. Настроить сеть согласно схемы, показанной на рисунке 3.1, и таблицы адресации 3.1.

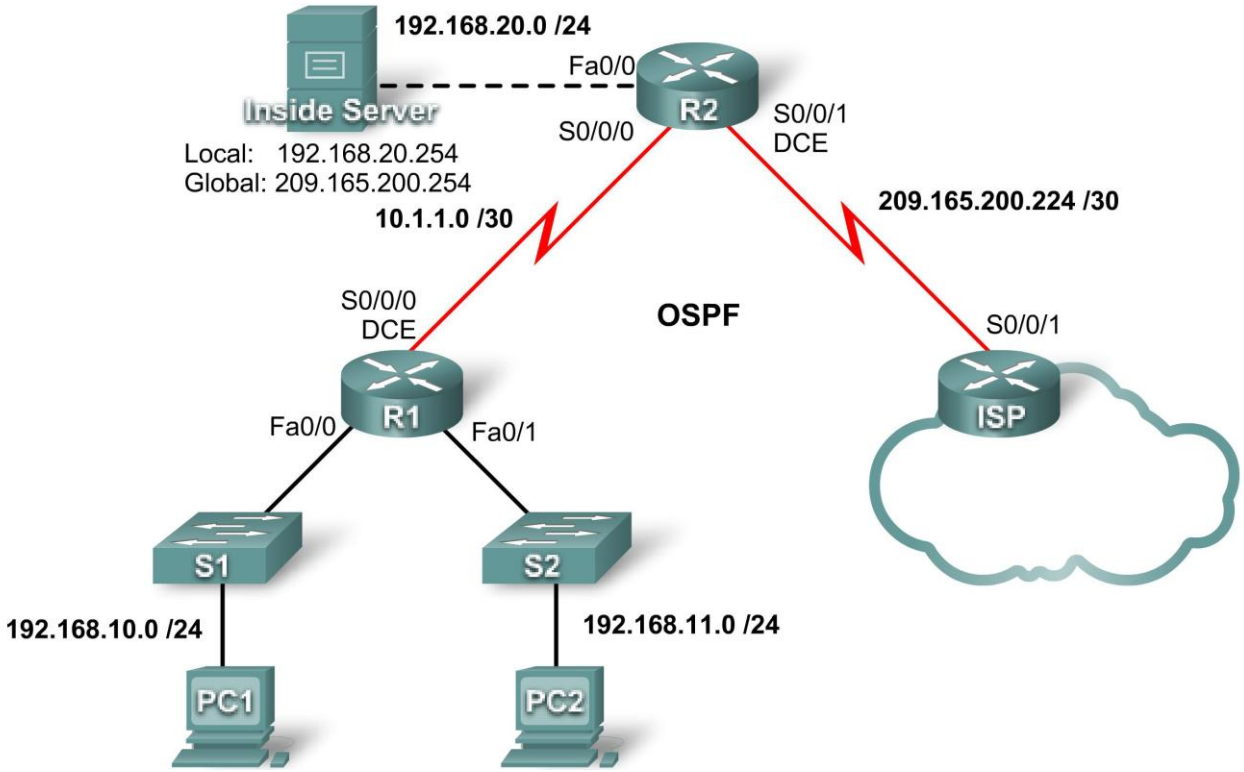

Рисунок 3.1 – Топология сети

Таблица 3.1 – Таблица адресации

Device	Interface	IP Address	Subnet Mask
R1	**S0/0/0**	10.1.1.1	255.255.255.252
	Fa0/0	192.168.10.1	255.255.255.0
	Fa0/1	192.168.11.1	255.255.255.0
R2	**S0/0/0**	10.1.1.2	255.255.255.252
	S0/0/1	209.165.200.225	255.255.255.252
	Fa0/0	192.168.20.1	255.255.255.0
ISP	**S0/0/1**	209.165.200.226	255.255.255.252

2. Настроить PC1 и PC2 для получения сетевого адреса используя протокол DHCP.
3. Настроить Cisco IOS DHCP Server.
4. Произвести тестирование DHCP.
5. Проверить конфигурацию DHCP.
6. Настроить статическую маршрутизацию по умолчанию.
7. Настроить статический NAT. Проверить работоспособность.
8. Настроить динамический NAT. Проверить работоспособность.
9. Задать конфигурацию, при которой происходит перегрузка NAT.

3.4 Содержание отчета

Отчет должен содержать конфигурацию маршрутизаторов и Cisco IOS DHCP Server. Также в отчете должны быть приведены скриншоты или логи, которые подтверждают работоспособность сети. Проанализировать состояние сети при перегрузке NAT.

3.5 Контрольные вопросы

1. Что такое NAT?
2. Какие виды NAT вы знаете?
3. Какие параметры сетевого адаптера отвечают за использование NAT?
4. В чем состоят особенности протокола DHCP?

Рекомендованная литература

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. СПб., Питер, 2001-672с.:ил, ШЫИТ 5-8046-0133-4
2. Таненбаум Э. Компьютерные сети. / Пер. с англ. Под ред. д – К.: BHV, 2002 г.
3. Craig Hunt. TCP/IP network adminisration. O'Relly & Associates, Inc, 1994-1998. 472 pages.
4. http://www.freebsd.org/handbook– Проект документирования FreeBSD
5. http://www.isc.org Сайт проектов bind, dhcpd
6. http://www.kernel.org/LDP – Проект документирования Linux
7. http://www.rfc-editor.org RFC center
8. http://www.samba.org Сайт проекта Samba
9. UNIX. Пособие системного администратора. / Пер. с англ. Под ред. д – К.: BHV, 2002 р.