

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО РЫБОЛОВСТВУ

*Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
Астраханский Государственный Технический Университет
Институт Информационных Технологий и Коммуникаций*

Кафедра «Информационная Безопасность»

**Лабораторный практикум по основам организации защищенных
сетей на основе оборудования cisco с использованием программного
эмулятора Cisco Packet Tracer**

Методическое пособие по дисциплине «Программно-аппаратные средства обеспечения информационной безопасности»

для студентов специальности 090303 «Информационная безопасность автоматизированных систем»

Астрахань 2011

Составители: Савельев А.Н., к.т.н., доцент кафедры «Информационная безопасность»

Белов С.В., к.т.н., доцент кафедры «Информационная безопасность»

Выборнова О.Н., студентка группы ДИБ-51

Донской А.А., студент группы ДИБ-51

Соловьев Ю.Ю., к.э.н., старший преподаватель кафедры «Экономика и управление предприятием»

Рецензент: Попов Г.А., д.т.н., профессор, заведующий кафедрой «Информационная безопасность»

Методическое пособие представляет собой сборник лабораторных работ по дисциплине «Программно-аппаратные средства обеспечения информационной безопасности автоматизированных систем». В лабораторных работах содержатся основные теоретические сведения, касающиеся организации защищенных IP-сетей на основе оборудования Cisco. Практические примеры реализованы с использованием программного обеспечения Cisco Packet Tracer.

Рекомендуется для студентов специальности «Информационная безопасность автоматизированных систем».

Методическое пособие утверждено на заседании методического совета кафедры «___» _____ 201_ г., протокол №_____

© Астраханский государственный технический университет

СОДЕРЖАНИЕ

Лабораторная работа №1. Обзор возможностей программного эмулятора Cisco Packet Tracer.....	4
Лабораторная работа №2. Обзор аппаратных устройств Cisco, реализованных в программном эмуляторе Cisco Packet Tracer	12
Лабораторная работа №3. Маршрутизация в TCP/IP сетях. Статическая и динамическая маршрутизации	24
Лабораторная работа №4. Фильтрация IP пакетов. Стандартные и расширенные списки доступа	33
Лабораторная работа №5. Создание защищенной распределенной сети передачи данных	37
Лабораторная работа №6. Виртуальные частные сети передачи данных	46
Лабораторная работа №7. Агрегирование каналов передачи данных.....	50

ЛАБОРАТОРНАЯ РАБОТА №1

Обзор возможностей программного эмулятора Cisco Packet Tracer

Цель работы: получить основные понятия и знания о функционировании программного эмулятора Cisco Packet Tracer как о программном средстве эмуляции линейки программно-аппаратного оборудования компании Cisco Systems.

Теоретическое описание

Cisco Packet Tracer – это мощный программный продукт моделирования сетей передачи данных, на основе сетевого оборудования компании Cisco Systems. Программный эмулятор Cisco Packet Tracer позволяет создавать модели сетей передачи данных, администрировать виртуальное активное сетевое оборудование, использовать различные виды каналов передачи данных. Данное программное обеспечение позволяет создавать сложные макеты сетей передачи данных, проверять работоспособность их топологии. Программный эмулятор Packet Tracer дополняет учебную программу Сетевых академий Cisco, позволяя облегчить изучение сложных технических концепции и дизайна сетевых систем.

На рисунке 1.1 представлен внешний вид интерфейсного окна.

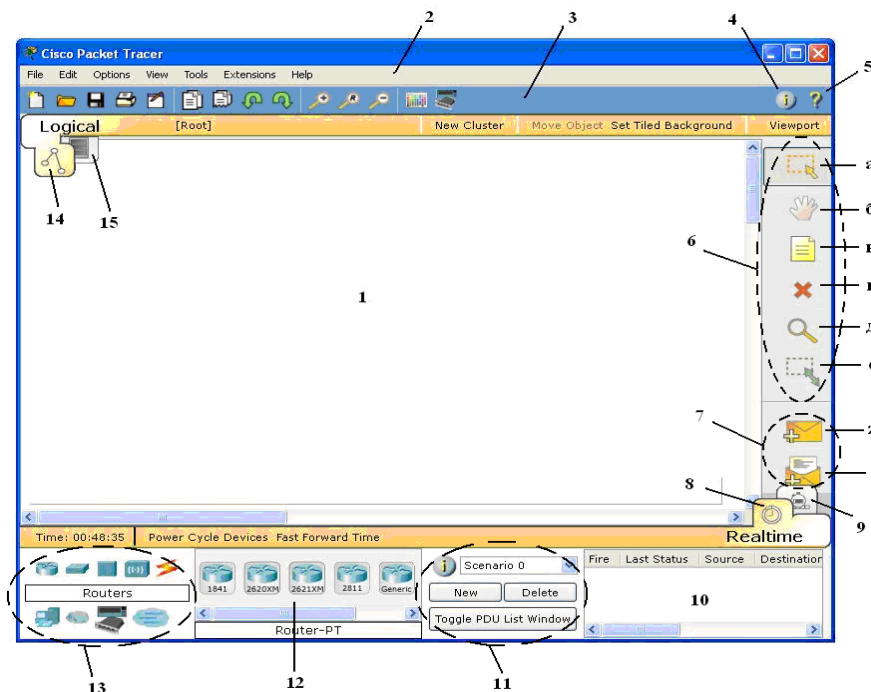


Рис. 1.1. Интерфейс эмулятора Cisco Packet Tracer

Интерфейс эмулятора Cisco Packet Tracer содержит следующие элементы:

1. Рабочая область. Область для построения и конфигурирования сетей;
2. Главное меню;
3. Главная панель инструментов;
4. Кнопка «Network Information» позволяет ввести описание текущей сети;
5. Кнопка «Contents (F1)» вызывает файл справки;
6. Общая панель инструментов. Содержит инструменты, которые часто используются в рабочей области программы:
 - а) «Select». Используется для выделения, перемещения и выбора объектов, устройств и неподсоединенных кабелей;
 - б) «Move Layout». Используется для перемещения рабочей области внутри поля логической диаграммы сети;
 - в) «The Place Note». Используется, чтобы добавить в рабочую область примечания;
 - г) «Delete». Используется для удаления объектов, устройств, примечаний и связей (кабелей);
 - д) «The Inspect». Позволяет посмотреть относящиеся к выбранному устройству таблицы (ARP таблицу, таблицу маршрутизации и др.);
 - е) «The Resize». Позволяет изменять размеры иконок устройств и объектов в рабочей области.
7. Кнопки визуального моделирования потоков данных:
 - ж) «The Add Simple PDU». Выполняет простой ping-запрос между двумя устройствами;
 - з) «The Add Complex PDU». Позволяет сформировать сложные пакеты данных.
8. Вкладка «Realtime». По умолчанию Packet Tracer работает в реальном времени. На счетчике в левой части этой панели время идет так же, как и на обычных часах;
9. Вкладка «Simulation». Служит для перехода в режим моделирования. Этот режим используется для наблюдения за сетевым трафиком. При этом время контролируется пользователем. Время может останавливаться или замедляться, чтобы просматривать сетевой трафик с интенсивностью 1 пакет в единицу времени;
10. Окно наблюдения за пакетами визуального моделирования по заданному сценарию;
11. Блок сценариев. Позволяет пользователям создавать и удалять сценарии работы устройств;
12. Блок выбора модели сетевых компонент или соединений, относящихся к определенному классу (на рисунке 1.1 показаны устройства, относящиеся к классу Routers);
13. Блок выбора класса устройства или соединения;
14. Вкладка «Logic», панель инструментов «Logic». Кнопки, располо-

женные на данной панели, функционируют только в рабочей области вкладки «Logic»;

15. Вкладка «Physical». Предназначена для перехода к физической рабочей области. Также имеет собственную панель инструментов. Физическая рабочая область обеспечивает физическое представление логической топологии сети, дает ощущение пространства и расположения устройств и сетей.

Построение модели сети передачи данных осуществляется перетаскиванием необходимых устройств в рабочую область. В программном эмуляторе Cisco Packet Tracer реализованы следующие типы соединений перечисленных на рисунке 1.2, а именно:

1. Автоматический;
2. Консольное соединение;
3. Прямой патч-корд (конечное сетевое устройство (персональный компьютер, сервер, сетевой принтер), маршрутизатор, точка доступа и т.д.);
4. Кроссовый (обратный) патч-корд (персональный компьютер, сервер – персональный компьютер, сервер, принтер; активное сетевое устройство – активное сетевое устройство);
5. Оптоволоконный канал передачи данных;
6. Телефонный канал передачи данных;
7. Коаксиальный канал передачи данных;
8. Последовательный (серийный) канал передачи данных.

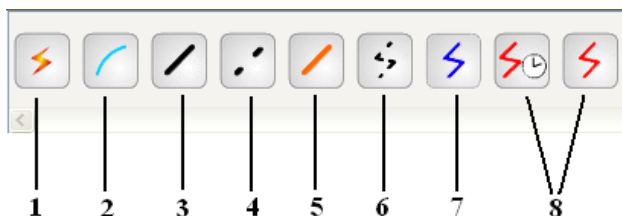


Рис. 1.2. Типы соединителей

Программный эмулятор Cisco Packet Tracer позволяет сохранять информацию о топологии сети и настройках сетевых устройств в файл формата *.pkt.

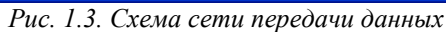
В качестве примера соберем простую схему сети, состоящую из двух персональных компьютеров и одного маршрутизатора. Для этого выберем и перетащим на рабочую область следующие устройства:

- в классе Routers – роутер модели 2811,
- в классе End Devices (оконечные устройства) – Generic (PC-TP).

По умолчанию персональным компьютерам присваиваются названия «PC1» и «PC2», а маршрутизатору – «Router1». Имя устройства можно изменить, щелкнув по нему левой кнопкой мышки и введя новое имя устройства.

Далее соединяем персональные компьютеры «PC1» и «PC2» с портами «FastEthernet0» маршрутизатора «Router1». Для этого выбираем тип соединения

В конечном итоге должна получиться схема, изображенная на рисунке 1.3. Изначально интерфейсы на устройствах отключены. Отключенные интерфейсы обозначаются красным цветом, включенные интерфейсы отображаются зеленым цветом.



Присвоим персональному компьютеру «PC1» – ір адрес 192.168.1.2, ір адрес маршрутизатора по умолчанию (шлюз по умолчанию) 192.168.1.1, маска подсети 255.255.255.0. Персональному компьютеру «PC2» – ір адрес 192.168.2.2, шлюз 192.168.2.1, маска подсети 255.255.255.0.

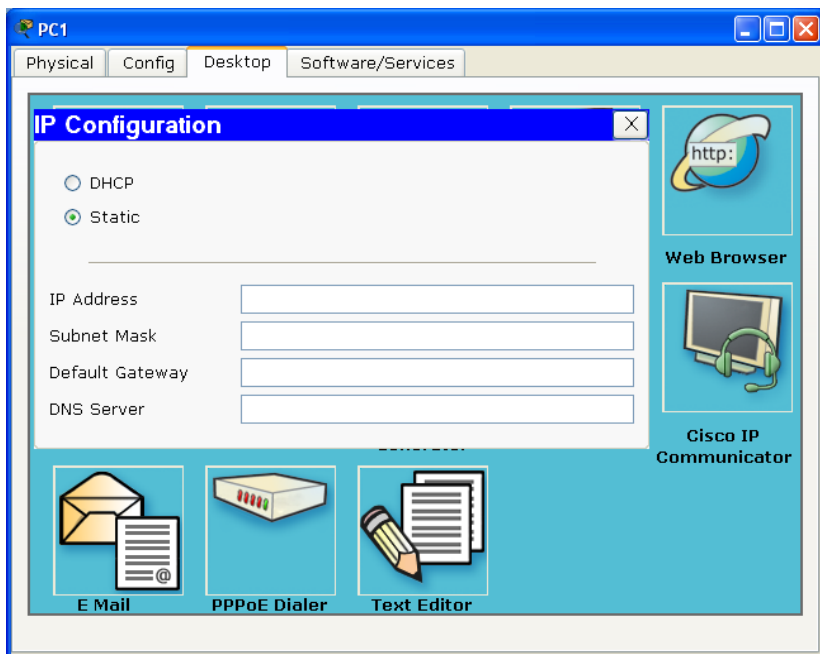


Рис. 1.4. Конфигурирование персонального компьютера

В программном эмуляторе Cisco Packet Tracer конфигурирование активных сетевых устройств (маршрутизаторов, коммутаторов, концентраторов, и.т.д.) можно производить путем ввода необходимых параметров в соответствующие поля вкладки «Config». Этот метод рекомендуется не использовать, поскольку в реальных условиях конфигурирования сетевых устройств подобной возможности нет. При выполнении заданий, указанных в методическом пособии, конфигурирование следует производить во вкладке «CLI», используя управляющие команды операционной системы Cisco IOS в консольном режиме.

Первоначально необходимо перевести маршрутизатор в привилегированный режим командой **enable** (сокращенно – **en**) – при этом консольное приглашение изменяется на символ «#». Затем переходим в режим конфигурирования с терминальной строки командой **configure terminal** (**conf t**). В режиме конфигурирования маршрутизатора консольное приглашение оканчивается на «config-terminal». В режиме конфигурирования маршрутизатора производится администрирование его основных параметров.

Для администрирования сетевых интерфейсов маршрутизатора необходимо перейти в режим конфигурирования сетевых интерфейсов. Для перехода в режим конфигурирования сетевого интерфейса необходимо в режиме конфигурирования устройства выполнить команду:

interface *название_интерфейса*.

В этом режиме выполняется настройка выбранного интерфейса. Командой **ip address** *адрес* *маска* назначается IP адрес сетевого интерфейса.

Включение интерфейса осуществляется командой ***no shutdown (no shut)***, выключение – командой ***shutdown (shut)***. Для информативности с помощью интерфейсной подкоманды ***description*** можно добавлять текстовый комментарий.

Состояние интерфейсов можно посмотреть, выйдя из режима конфигурирования (командой ***exit*** или нажав <Ctrl+Z>) и выполнив команду ***show interface (sh int)***. Краткую сводную информацию о статусе всех имеющихся на устройстве интерфейсов можно получить при помощи команды ***show ip interface brief***.

Результатом конфигурирования устройства Cisco является скрипт команд конфигурирования, интерпретируемый устройством. Текущую, или используемую, конфигурацию устройства – скрипт конфигурирования устройства – можно посмотреть при помощи команды ***show running-config (sh run)***.

Рассмотрим пример конфигурирования маршрутизатора. Присвоим порту FastEthernet0/0 – IP адрес 192.168.1.1, маска 255.255.255.0; порту FastEthernet0/1 – IP адрес 192.168.2.1, маска 255.255.255.0 (Рис. 1.5).

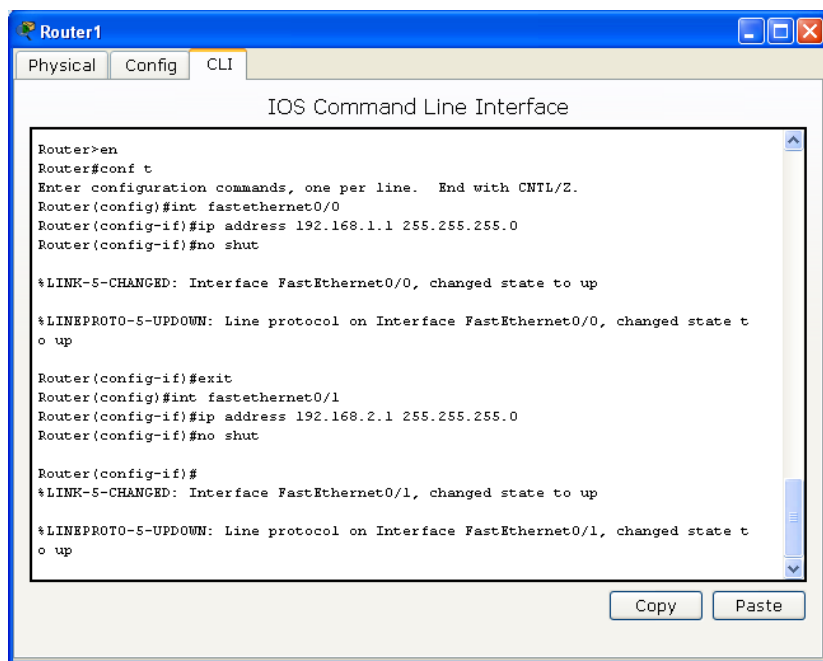


Рис. 1.5. Конфигурирование маршрутизатора

В итоге интерфейсы устройств окрашиваются в зеленый цвет. Это является признаком того, что они включены и нормально функционируют.

Проверить функционирование сети можно, отправив ICMP-запрос (выполнив команду ***ping***) с персонального компьютера PC1 на персональный компьютер PC2. Команду ***ping*** можно выполнять и на активных сетевых устройствах, например, на маршрутизаторе. В программном эмуляторе Cisco Packet Tracer отправить ICMP-запрос можно двумя способами:

1. Используя консольное приложение («Command Prompt» во вкладке «Desktop» одного из компьютеров или вкладку «CLI» маршрутизатора);
2. Используя инструмент моделирования потоков данных «The Add Simple PDU»: выбрать инструмент «The Add Simple PDU», щелкнуть по устройству-источнику запроса, щелкнуть по устройству-приемнику запроса. При успешном выполнении запроса в окне наблюдения за пакетами визуального моделирования устанавливается статус «Successful» (рис. 1.6).



Рис. 1.6. Моделирование потоков данных

В операционной системе Cisco IOS, управляющую устройствами Cisco, встроена система помощи, к которой можно обратиться из режима исполнения команд. Система помощи является контекстной, что означает, что оказываемая помощь зависит от того, что пользователь пытается сделать в ОС Cisco IOS в данный момент времени. Для получения списка имеющихся опций достаточно в любое время ввести команду в виде знака вопроса (?). Эта команда осуществит поиск доступных команд (подкоманд) и выведет их список на экран. Система помощи построена таким образом, что в левой части выводимого текста содержатся сами команды, а в правой – короткие пояснения к каждой из них.

Следует помнить, что в программном эмуляторе Cisco Packet Tracer система помощи показывает только список команд, которые могут быть смоделированы данной программой. Этот список может несколько отличаться от списка команд, доступных на реальном устройстве.

Кроме того, встроенная система помощи позволяет вводить команды не полностью, а автоматически дополняя команду до конца при нажатии клавиши **Tab**. Если ввести часть команды, которая не имеет нескольких значений, и нажать клавишу **Tab**, то ОС IOS сама дополнит команду. При вводе неоднозначной команды ОС Cisco IOS не сможет ее дополнить.

Задание к лабораторной работе:

1. В программном эмуляторе Cisco Packet Tracer собрать макет сети по схеме, рассмотренной выше.
2. Настроить устройства согласно вариантам;
3. Проверить доступность активных элементов сети, используя команду **ping**.
4. Проверить доступность активных элементов сети, используя инструмент моделирования потоков данных «The Add Simple PDU».

Варианты заданий:

Вариант	Подсети
1	172.16.1.x/24; 172.16.2.x/24
2	192.168.1.x/30; 192.168.2.x/30
3	172.12.1.x/24; 172.12.2.x/24
4	192.168.1.x/24; 172.12.1.x/24
5	192.168.1.x/28; 192.168.5.x/24
6	192.168.1.x/24; 192.168.21.x/28

Контрольные вопросы:

1. Семиуровневая модель OSI.
2. Функционирование физического и канального уровней модели OSI.
3. Функционирование сетевого и транспортного уровней модели.
4. Функционирование сеансового уровня, уровней представлений и приложений.
5. Основные сведения по стандарту Ethernet 802.3u.
6. Понятие IP адреса, маски подсети.
7. Классы IP адресов.
8. Разбиение сетей на подсети, сегментирование сетей.

ЛАБОРАТОРНАЯ РАБОТА №2

Обзор аппаратных устройств Cisco, реализованных в программном эмуляторе Cisco Packet Tracer

Цель работы: ознакомиться с активными сетевыми устройствами, реализованными в программном эмуляторе Cisco Packet Tracer. Научиться настраивать и управлять маршрутизатором через консольный порт. Ознакомиться и настроить сетевые сервисы виртуального сервера.

Теоретические сведения

Сетевой коммутатор (*свитч* от англ. switch — переключатель) — это сетевое устройство активного типа, соединяющее хосты сети передачи данных в пределах одного сетевого сегмента. Коммутатор (switch) передаёт полученные пакеты не на все порты, как это делает концентратор, а непосредственно получателю, тем самым устанавливает виртуальный канал передачи данных. Сетевой коммутатор Ethernet по сравнению с концентратором (хабом) обладает увеличенной эффективностью и производительностью. За счет использования изолированных каналов передачи данных уровень сетевой безопасности повышается.

Маршрутизатор или *роутер* (от англ. router) — специализированное сетевое устройство, передающее пакеты сетевого уровня (уровень 3 модели OSI) между разными частями сетевой инфраструктуры на основе данных о топологии сети и определённых алгоритмов и правил.

Каждое устройство Cisco имеет консольный порт, который используется для обращения к нему с помощью непосредственно подключаемого терминала. Консольный порт часто представляет собой порт интерфейса типа RS-232C или разъем типа RJ-45 и обозначается надписью «Console» («Консоль»).

Установив физическое соединение между терминалом или персональным компьютером и устройством, необходимо произвести конфигурирование терминала для его соответствующего взаимодействия с устройством. Для этого следует настроить параметры терминала (или программы эмуляции терминала на персональном компьютере) таким образом, чтобы поддерживались следующие установки:

- Тип эмулируемого терминала – VT100;
- Скорость передачи данных – 9600 бод;
- Запрет контроля четности;
- 8 бит данных;
- 1 стоп-бит.

После проверки правильности установок следует подать на устройство питание. На экране терминала появится информация об устройстве, что свидетельствует об успешном подключении. Если сообщения на экране терминала или устройства, эмулирующего его, нет, нужно проверить соединение и удостовериться в правильности установок терминала.

Соберём схему, состоящую из 3-х персональных компьютеров, сервера, маршрутизатора и коммутатора. Для этого выберем и перетащим на рабочую

область следующие составляющие сети:

- в разделе Routers – маршрутизатор модели 2811,
- в разделе Switches – коммутатор модели 2960-24,
- в разделе End Devices – персональные компьютеры Generic (PC-TP), сервер Generic (Server-PT).

Соединим устройства между собой, как показано на рисунке 2.1, и приступим к конфигурированию сети.

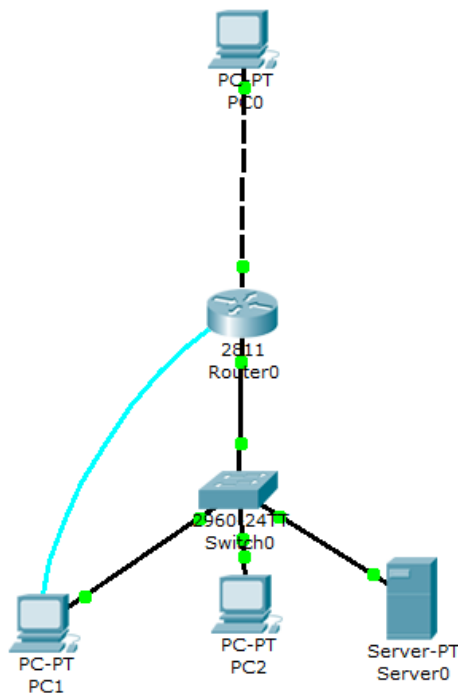


Рис. 2.1. Схема модели сети

В данной схеме сети используем следующие подсети:

1. Персональные компьютеры PC1, PC2 и сервер Server0, подключенные к маршрутизатору через коммутатор Switch0, и порт FastEthernet0/0 маршрутизатора Router0 представляют собой подсеть NetA;
2. Персональные компьютеры PC0 и маршрутизатор Router0 (порт FastEthernet0/1) представляют собой подсеть NetB.

В лабораторной работе настройку маршрутизатора необходимо производить через терминальное подключение с персонального компьютера PC1. Для этого соединяем PC1 и Router0 консольным соединением (на PC1 выбираем порт RS 232, на Router0 – консольный порт Console). Затем на PC1 заходим во вкладку «Desktop», выбираем «Terminal» и нажимаем «Ок». Если все проделано

правильно, то в итоге подключаемся к маршрутизатору через терминальное подключение (Рис. 2.2).

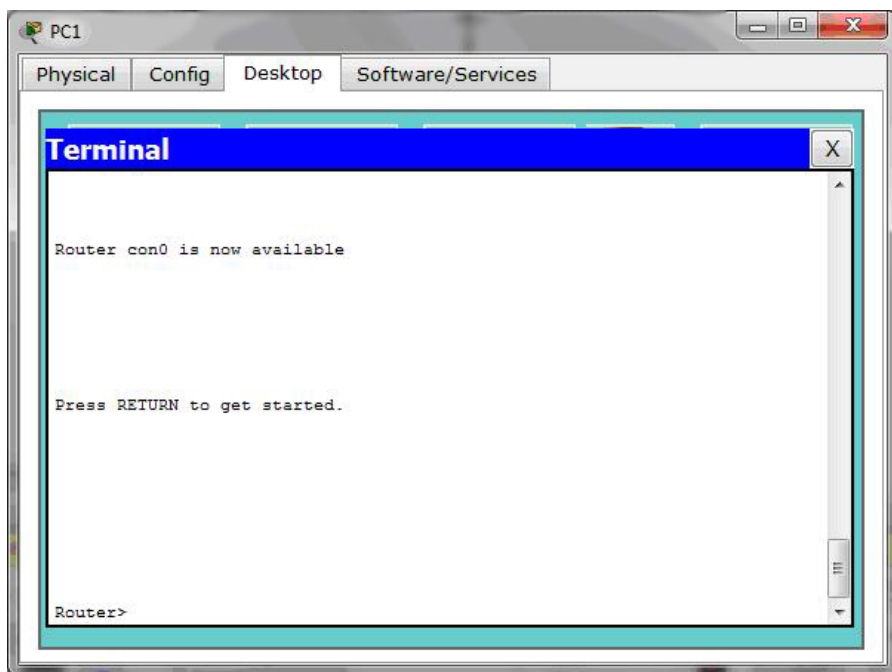


Рис. 2.2. Интерфейс терминального подключения

В качестве примера подсети NetA присвоим параметры 192.168.1.0/28, а подсети NetB – параметры 192.168.2.0/28.

Назначим IP адреса сетевым интерфейсам, аналогично предыдущей лабораторной работе.

Выполнять администрирование сетевых активных устройств возможно не только через консольное подключение, но и удаленно, используя протокол telnet. Для этого необходимо сначала настроить на устройстве (маршрутизаторе) доступ для удаленных (виртуальных) пользователей. В привилегированном режиме выполним следующие команды:

```
line vty 0 4  
login  
password пароль.
```

После этого с любого компьютера можно зайти в командную строку и ввести команду **telnet IP_адрес_роутера**. Если соединение удалось, то запрашивается пароль, который установлен на доступ к роутеру для удаленных пользователей. При правильном вводе пароля подключаемся к маршрутизатору (Рис. 2.3).

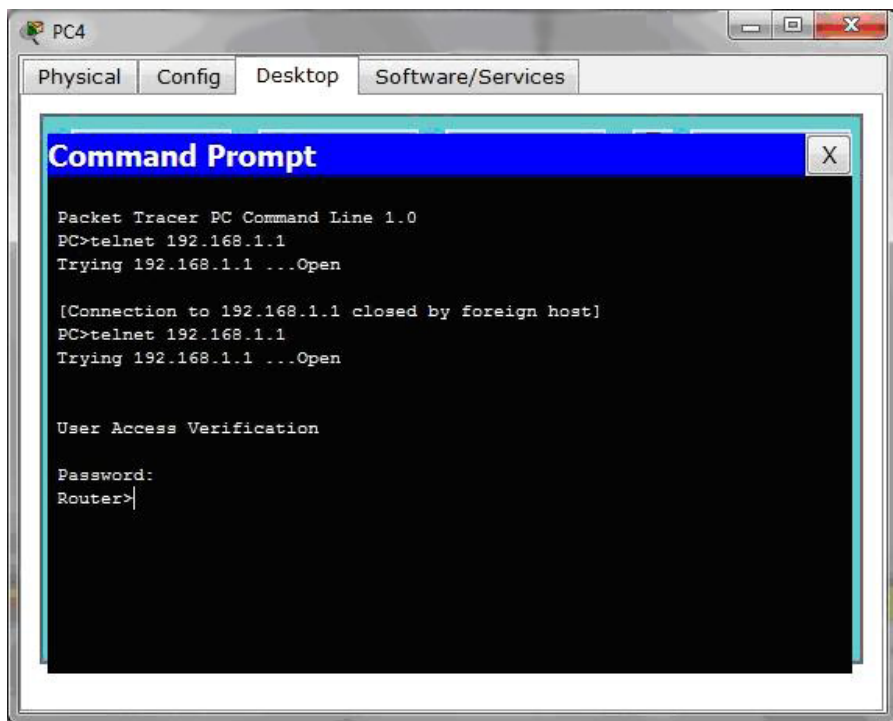


Рис. 2.3. Подключение к маршрутизатору по протоколу telnet

Коммутатору Switch0 также можно присвоить IP адрес. Чтобы присвоить IP адрес устройству в целом, необходимо присвоить IP интерфейсу Vlan1. Теперь коммутатору присвоен ip-адрес, и доступность его можно проверить командой **ping**. Коммутаторы могут работать как на 2-ом уровне сетевой модели OSI, так и на 3-ем уровне данной модели. В коммутаторах третьего уровня имеется возможность присваивать IP адреса отдельным портам. Коммутаторы 3-го уровня позволяют сегментировать сеть передачи данных на отдельные изолированные подсети.

В программном эмуляторе Cisco Packet Tracer реализованы следующие сетевые сервисы виртуальных серверов.

Сервис DNS (англ. Domain Name System – система доменных имён) – это система (база данных), способная по запросу, содержащему доменное имя хоста (компьютера или другого сетевого устройства), сообщить его IP адрес. Каждый компьютер в TCP/IP сетях передачи данных имеет свой уникальный адрес – это ряд цифр формата XXX.XXX.XXX.XXX (где XXX – число от 0 до 255). Запомнить ip-адрес хоста достаточно сложно, гораздо проще запомнить символьное наименование того или иного элемента сети, ассоциированное с его IP адресом, например, www.mail.ru, www.rambler.ru и т.д.

Сервис HTTP (сокр. от англ. HyperText Transfer Protocol — «протокол передачи гипертекста») — протокол прикладного уровня передачи данных (зна-

начально — в виде гипертекстовых документов). Основой HTTP является технология «клиент-сервер», то есть предполагается существование потребителей (клиентов), которые иницируют соединение и посылают запрос, и поставщиков (серверов), которые ожидают соединения для получения запроса, производят необходимые действия и возвращают обратно сообщение с результатом.

Основным объектом манипуляции в HTTP является ресурс, на который указывает **URI** (англ. Uniform Resource Identifier) в запросе клиента. Обычно такими ресурсами являются хранящиеся на сервере файлы, но ими могут быть логические или абстрактные объекты. Особенностью протокола HTTP является возможность указать в запросе и ответе способ представления одного и того же ресурса по различным параметрам: формату, кодировке, языку и т.д. Именно благодаря возможности указания способа кодирования сообщения клиент и сервер могут обмениваться двоичными данными, хотя данный протокол является текстовым. Протокол HTTP по умолчанию реализован по TCP-порту 80, в случае необходимости номер порта можно изменить.

Сервис HTTPS (HyperText Transfer Protocol Secure) — расширение протокола HTTP, поддерживающее шифрование. Данные, передаваемые по протоколу HTTPS, «упаковываются» в криптографический протокол SSL или TLS, тем самым обеспечивается защита данных. В отличие от HTTP, для HTTPS по умолчанию используется TCP-порт 443.

Электронная почта (англ. email, e-mail, от англ. electronic mail) — технология и предоставляемые ею услуги по пересылке и получению электронных сообщений по распределённой (в том числе глобальной) компьютерной сети. Для отправки почты от пользователей к серверам и между серверами для дальнейшей пересылки получателю используется протокол SMTP (TCP-порт 25). Для приема почты почтовый клиент использует протокол POP3 (TCP-порт 110) или IMAP (TCP-порт 143).

Сервис FTP (англ. File Transfer Protocol — протокол передачи файлов) — протокол, предназначенный для передачи файлов в сетях передачи данных. Протокол FTP позволяет подключаться к серверам FTP, просматривать содержимое каталогов и загружать файлы с сервера или на сервер; кроме того, возможен режим передачи файлов между серверами.

Рассмотрим особенности настройки указанных сетевых сервисов в программном эмуляторе Cisco Packet Tracer.

На сервере Server0 сконфигурируем DNS-сервер. Для этого необходимо зайти во вкладку «Config», на левой панели выбрать вкладку «Services» → «DNS». Далее выбираем тип записи «A Record», в поле «Name» вписываем имя (символьный адрес) хоста, в поле «Address» — IP-адрес хоста и нажимаем кнопку «Add». Запись добавится в таблицу (Рис. 2.4).

При необходимости записи таблицы можно редактировать и удалять. Для этого нужно выбрать соответствующую запись таблицы, внести необходимые изменения и нажать кнопку «Save» для сохранения изменений или кнопку «Remove» для удаления строки из таблицы.

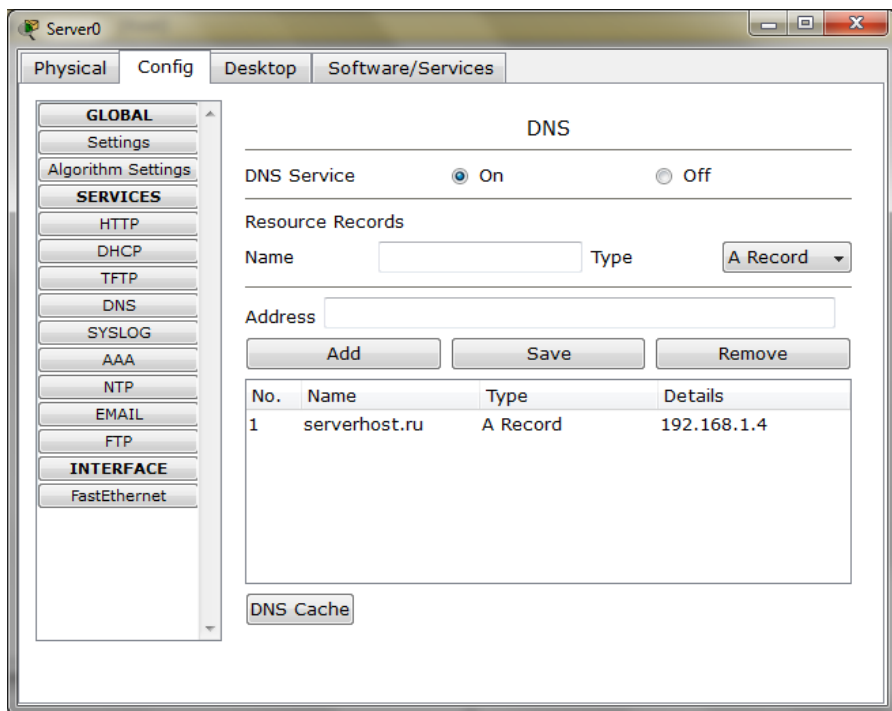


Рис. 2.4. Интерфейс настройки DNS-сервера

После настройки DNS-сервера в конфигурации компьютеров в поле «DNS Server» необходимо внести IP-адрес, присвоенный Server0.

Аналогично настроим сервис HTTP. На сервере Server0 необходимо зайти во вкладку «Config», на левой панели выбрать вкладку «Services» → «HTTP», включить «HTTP».

В текстовом поле показан HTML-код страницы, которая будет отображаться в браузере. Код страницы можно изменить, используя HTTP теги. На рисунке 2.5 показан измененный HTML-код страницы index.html. Здесь изменен цвет текста «Cisco Packet Tracer» и текст заголовка.

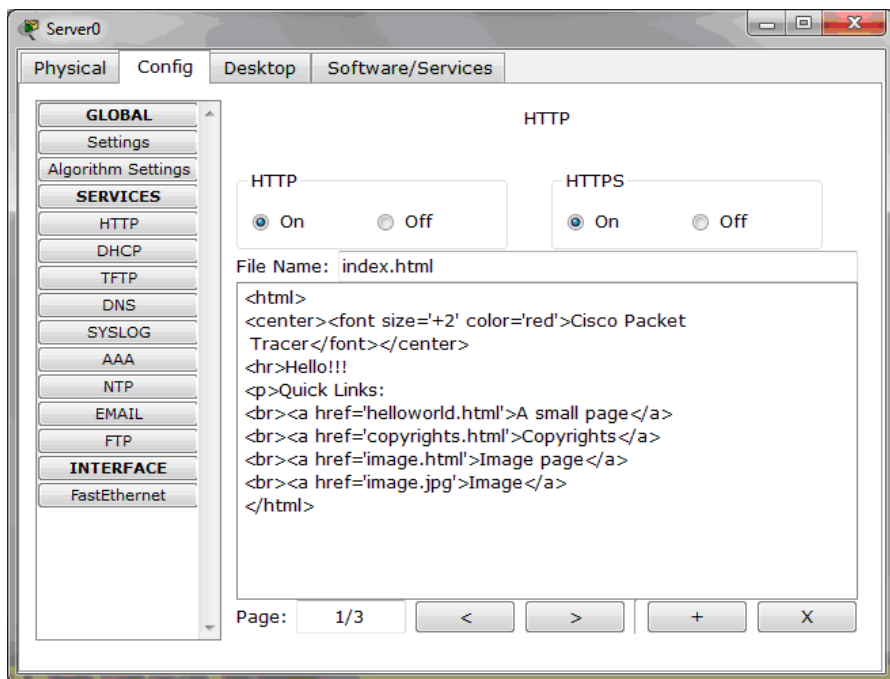


Рис. 2.5. Настройка HTTP сервера

Чтобы проверить работоспособность DNS-сервера и сервера HTTP, необходимо во вкладке «Desktop» компьютера запустить «Web Browser» и в адресную строку ввести имя хоста. В случае правильной настройки откроется HTML-страница (рис. 2.6).

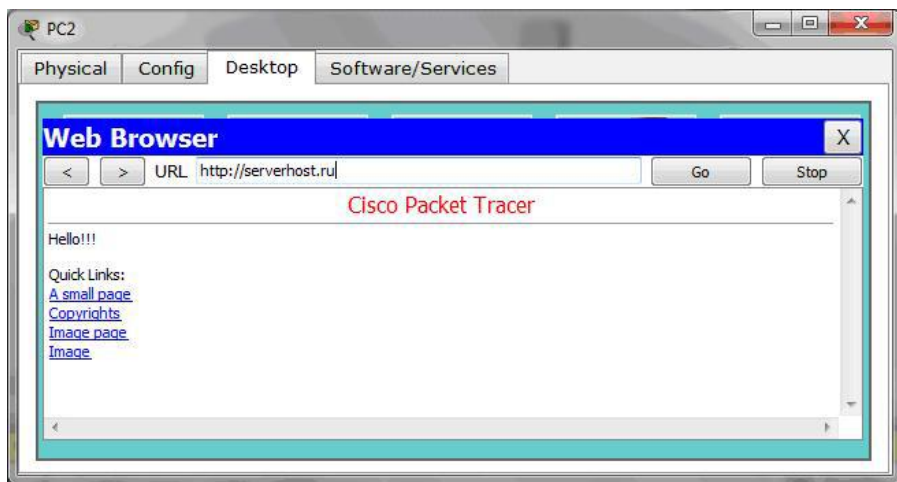


Рис. 2.6. Окно эмуляции Web браузера

Настроим на Server0 почтовый сервер. Для этого необходимо зайти во вкладку «Config», на левой панели выбрать вкладку «Services» → «EMAIL». Включить «SMTP Service» и «POP3 Service». Прописать доменное имя и нажать кнопку «Set». Добавить пользователей (Рис. 2.7).

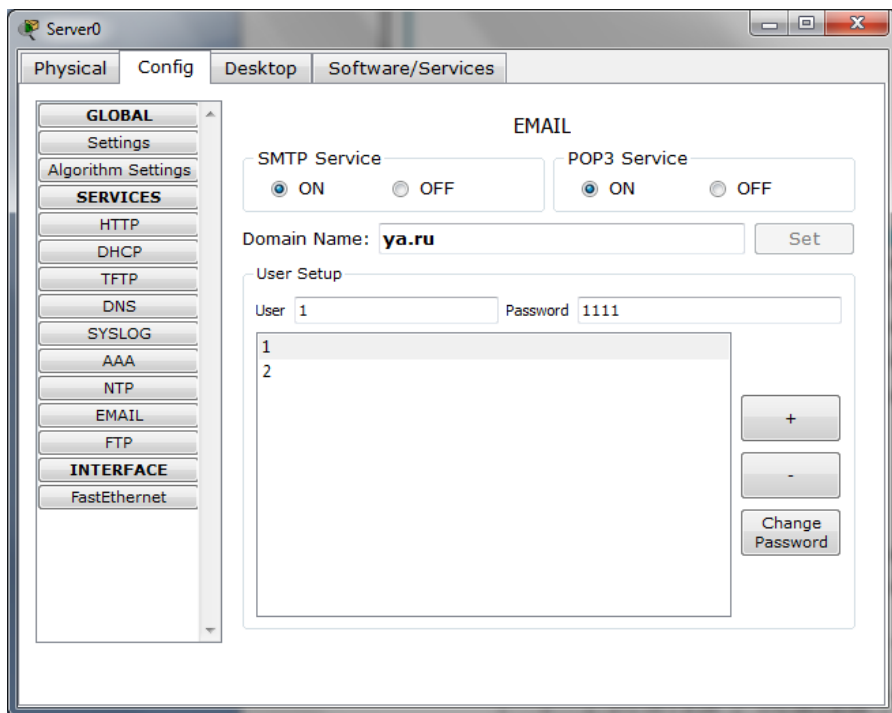


Рис. 2.7. Настройка почтового сервера

После настройки сервера необходимо настроить почтовый клиент на ПК. Во вкладке «Desktop» выбираем «E Mail». Откроется окно конфигурации почтового клиента. В последующем его можно будет вызвать нажатием кнопки «Configure Mail» в окне клиента.

В окне конфигурирования почтового клиента в блоке «User Information» вводится имя автора писем и почтовый адрес вида *имя_пользователя@имя_домена*, в блоке «Server Information» указывается символическое имя или IP адрес почтового сервера, в блоке «Logon Information» указываются имя пользователя и пароль пользователя, зарегистрированного на почтовом сервере (Рис. 2.8). После этого следует нажать кнопку «Save», в результате чего откроется «Mail Browser» – главное окно почтового клиента.

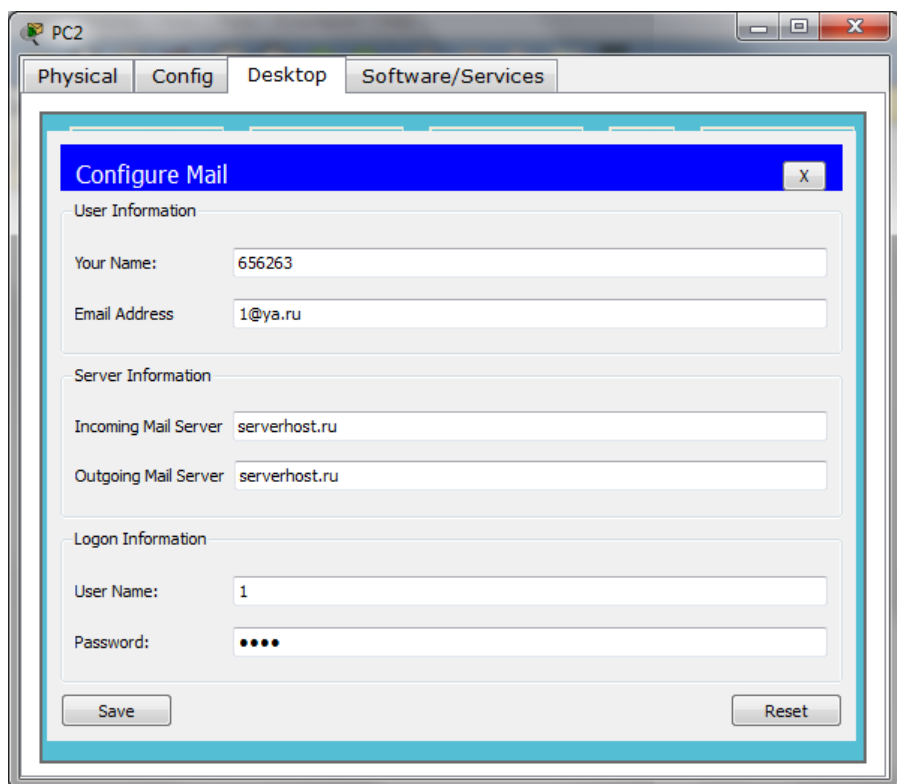


Рис. 2.8. Настройка почтового клиента

Чтобы написать письмо, нажимаем кнопку «Compose», заполняем текстовые поля и отправляем письмо (Рис. 2.9).

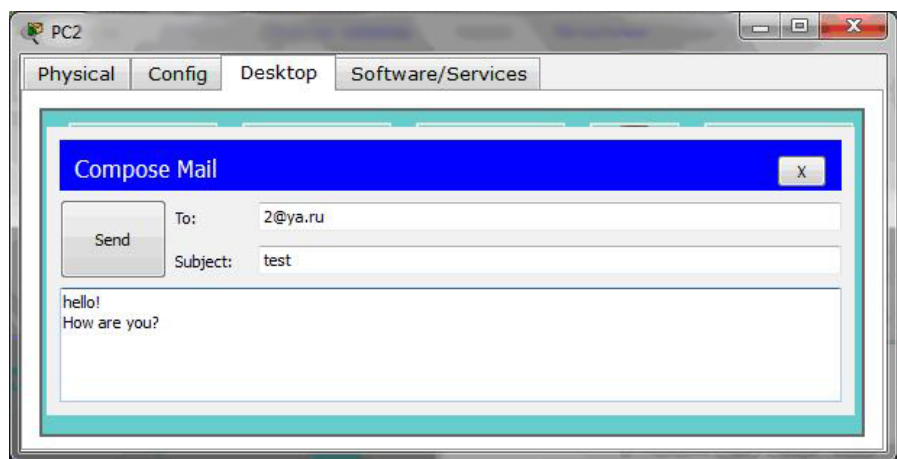


Рис. 2.9. Отправка электронного письма

Чтобы проверить, пришло ли письмо адресату, нужно зайти в почтовый клиент на ПК адресата и нажать кнопку «Receive». Мы увидим, есть ли письма для данного адресата. В текстовом поле под списком входящих писем отображается содержание выделенного письма (Рис. 2.10).

Чтобы ответить на какое-то из входящих писем, необходимо выделить его и нажать кнопку «Reply».

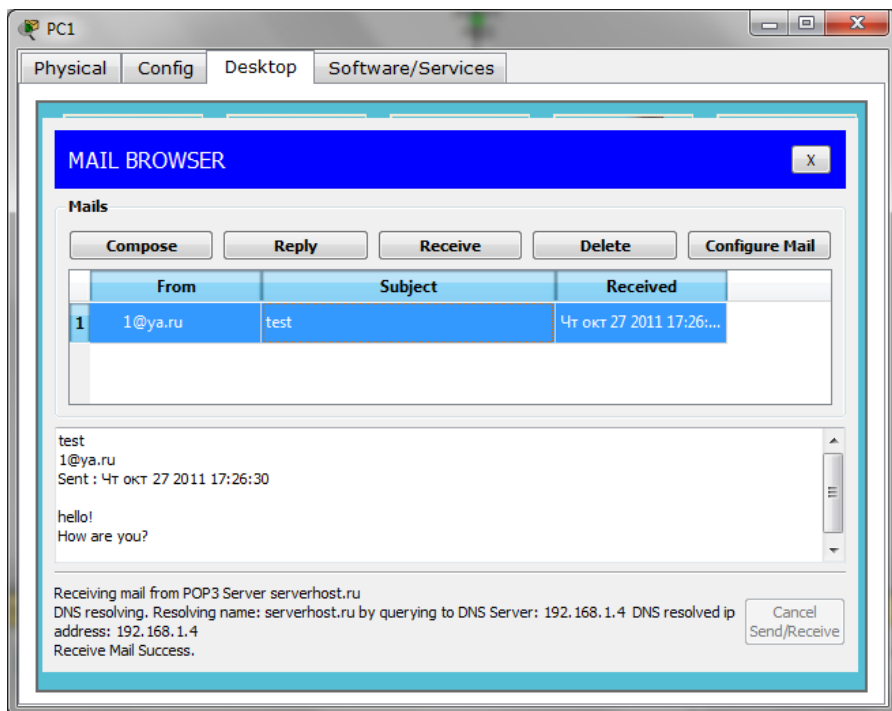


Рис. 2.10. Полученное электронное письмо

Настроим на Server0 FTP сервис. Для этого необходимо зайти во вкладку «Config», на левой панели выбрать вкладку «Services» → «FTP». Включить «FTP Service». Добавить пользователя для доступа к FTP-ресурсу. Для этого необходимо в полях «UserName» и «Password» прописать имя пользователя и пароль, назначить права доступа (Write, Read, Delete, Rename, List) и нажать кнопку «+» для добавления (Рис. 2.11). В таблице «File» содержится список файлов, доступных пользователям.

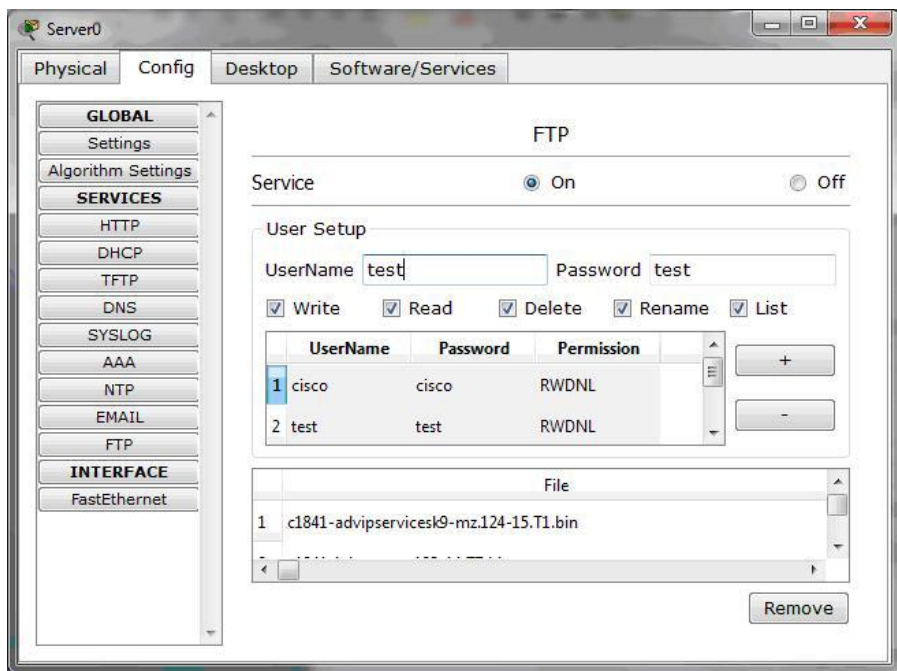


Рис. 2.11. Настройка FTP-сервера

Чтобы зайти на сервер FTP, необходимо в командной строке одного из ПК ввести команду **ftp имя_хоста** (символьное имя или IP адрес). Перед нами появится запрос имени пользователя. Если введено имя пользователя, зарегистрированного на FTP-сервере, то появится запрос пароля. Если пароль введён верно, то мы подключились (Рис. 2.12).

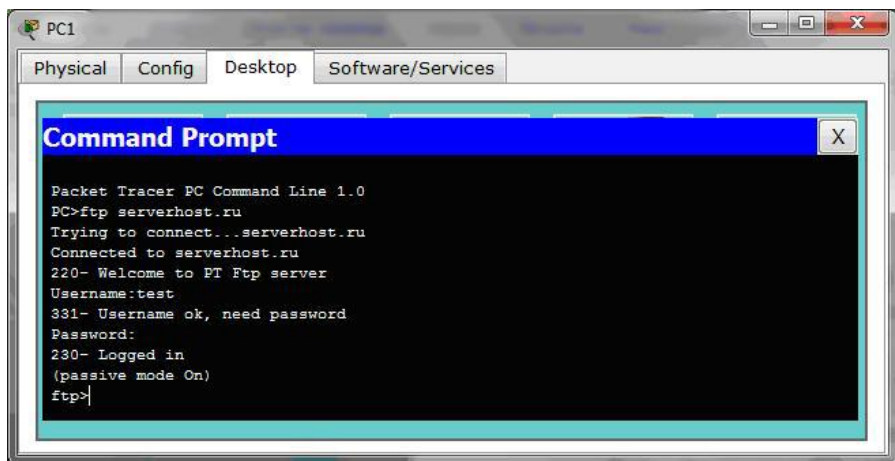


Рис. 2.12. Подключение к FTP-серверу

При помощи команды ***dir*** можно просмотреть список файлов, которые хранятся на сервере. Также можно скачать файл с сервера при помощи команды ***get имя_файла***. Команда ***put имя_файла*** позволяет загрузить файл на FTP сервер.

Задание к лабораторной работе:

1. В программном эмуляторе Cisco Packet Tracer собрать модель сети по схеме, изображенной на рис. 2.1;
2. Настроить устройства через терминальное подключение с PC1 согласно вариантам;
3. Подключиться к маршрутизатору по протоколу telnet.
4. Настроить сетевые сервисы DNS, HTTP, EMAIL, FTP.
5. Проверить доступность сетевых узлов с использованием утилиты ***ping***.
6. Проверить работу установленных сервисов сервера.

Варианты заданий:

Вариант	Подсети		Имя хоста
	NetA	NetB	
1	172.16.1.x/24	172.16.2.x/24	myHost.ru
2	192.168.1.x/28	192.168.2.x/30	Cisco.lab
3	172.12.1.x/24	172.12.2.x/24	MySecondLab
4	192.168.1.x/24	172.12.1.x/24	Lab2.ib
5	192.168.1.x/28	192.168.5.x/24	Ib4.astu
6	192.168.1.x/24	192.168.21.x/28	Host.name

Контрольные вопросы:

1. Общие сведения о линейке продуктов Cisco.
2. Понятие коммутатора. На каком уровне модели OSI работает коммутатор?
3. Понятие маршрутизатора. На каком уровне модели OSI работает маршрутизатор?
4. Понятие шлюза, брандмауэра.
5. Сервис DNS, типы DNS-записей.
6. Сервис HTTP, общие понятия.
7. Понятие электронной почты, протоколы SMTP, POP3 и IMAP.
8. Протокол обмена файлами FTP, основные понятия и команды FTP.
9. Протокол Telnet, основные понятия.

ЛАБОРАТОРНАЯ РАБОТА №3

Маршрутизация в TCP/IP сетях. Статическая и динамическая маршрутизации

Цель работы: смоделировать сеть передачи данных с использованием маршрутизатора Cisco. Рассмотреть особенности настройки последовательного канала передачи данных. Настроить DHCP сервер. Настроить статическую и динамическую маршрутизацию пакетов в локальной сети.

Теоретические сведения

Маршрутизаторы Cisco обладают возможностью соединения не только по стандарту 802.3u (Fast Ethernet), но и по серийному соединению с использованием последовательных портов. Такое соединение необходимо, например, при построении телефонного пула голосовых модемов на маршрутизаторе.

Для рассмотрения такого способа построения сети создадим локальную сеть, изображенную на рисунке 3.1.

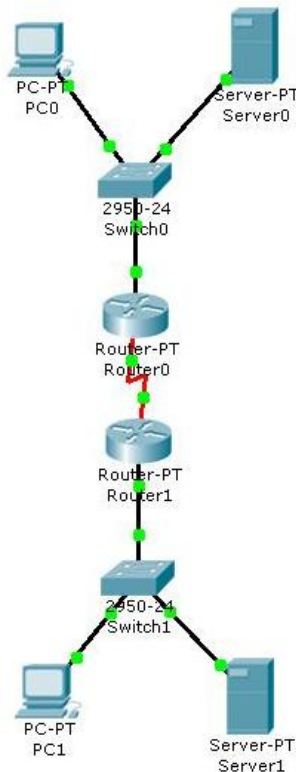


Рис. 3.1. Схема модели сети

В модели сети используются маршрутизаторы Generic (Router-PT). Обозначим их Router0 и Router1. Сетевые имена роутеров назначаются в режиме конфигурирования командой **hostname имя**. Между собой они соединяются кабелем Serial DCE.

Также в сети имеются 2 сервера (в классе конечных устройств выбирается Generic – Server-PT), 2 коммутатора Cisco 2950-24 и 2 персональных компьютера.

Примем следующее обозначение подсетей:

1. NetA: ПК PC0, сервер Server0, подключенные к маршрутизатору через коммутатор Switch0, и порт FastEthernet0/0 маршрутизатора Router0;
2. NetB: ПК PC1, сервер Server1, подключенные к маршрутизатору через коммутатор Switch1, и порт FastEthernet0/0 маршрутизатора Router1;
3. NetC: последовательное соединение – порты Serial маршрутизаторов Router0 и Router1.

Для примера рассмотрим подсети NetA 192.168.1.0/24, NetB 192.168.2.0/24, NetC 192.168.3.0/30.

Включение интерфейсов FastEthernet0 выполняется аналогично действиям, описанным в лабораторной работе №1. Включение портов Serial производится следующим образом:

1. Маршрутизатор переводится в режим конфигурирования – **conf t**;
2. Маршрутизатор переводится в режим конфигурирования интерфейса Serial2/0 – **int s2/0**;
3. Порту Serial2/0 назначается IP адрес;
4. Порту Serial2/0 назначается режим инкапсуляции ppp (командой **encapsulation ppp**), чтобы проходящие Ethernet пакеты передавались в режиме туннелирования протоколом «точка-точка» (опционально);
5. Порту Serial2/0 назначается скорость взаимодействия 64000 бит/с – **clock rate 64000** (для порта, который при создании схемы сети был выбран в качестве DCE (ведущий), т.е. для порта, который при соединении выбирался первым);
6. Включить порт Serial2/0 командой **no shut**.

После выполнения данных команд порты и протокол PPP активируются автоматически.

Ранее были приведены примеры назначения устройствам статического IP адреса. Существует динамический способ назначения IP адресов с использованием специализированного протокола и сервиса.

Сервис DHCP (англ. Dynamic Host Configuration Protocol — протокол динамической конфигурации узла) — это сетевой протокол, позволяющий узлам (хостам) автоматически получать IP-адрес и ряд других параметров, необходимых для работы в TCP/IP сетях. Данный протокол работает по модели «клиент-сервер». Для автоматической конфигурации сетевой узел–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 возникающих при настройке сетевых интерфейсов.

Помимо IP-адреса, DHCP сервер также может сообщать клиенту дополнительные параметры, необходимые для работы в сети. Эти параметры называются опциями DHCP. Некоторыми из наиболее часто используемых опций являются:

- IP-адрес шлюза по умолчанию;
- Маска подсети;
- Адреса серверов DNS;
- Имя домена DNS.

Для сети NetA DHCP-сервером будет Server0, а для сети NetB – Router1.

Рассмотрим конфигурирование DHCP сервера на Server0. Для этого необходимо зайти во вкладку «Config», на левой панели выбрать вкладку «Services» → «DHCP». Включить «DHCP Service». Далее указываются следующие значения:

- В поле «Pool name» – имя пула адресов (диапазона адресов);
- В поле «Default Gateway» – IP адрес шлюза;
- В поле «Start IP Address» – IP, с которого начнется раздача адресов;
- В поле «Subnet Mask» – маска подсети (при этом в поле «Maximum number of Users» автоматически отображается объем пула адресов).

После нажатия кнопки «Add» запись добавляется в таблицу. Запись можно редактировать, не забывая при этом нажимать кнопку «Save». Удалить запись можно нажатием на кнопку «Remove».

После того, как настроен сервер DHCP, на ПК в «IP configuration» вместо «Static» необходимо выбрать «DHCP». На сервере IP адрес присваивается вручную.

На рисунке 3.2 показан пример настройки DHCP сервера на Server0.

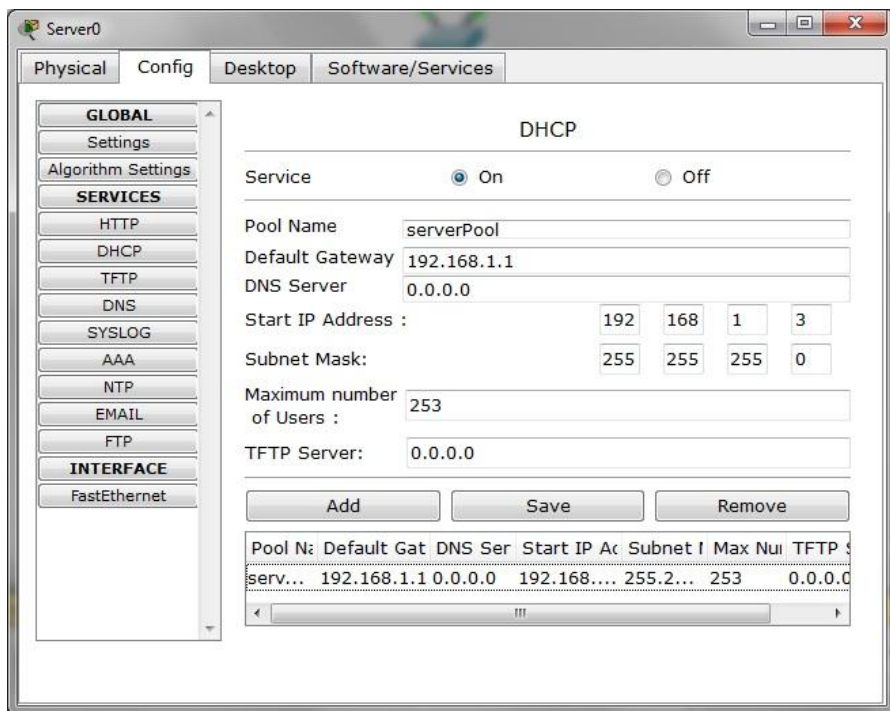


Рис. 3.2. Конфигурирование сервера DHCP на сервере Server0

Рассмотрим конфигурирование DHCP сервера на маршрутизаторе Router1.

По-умолчанию на маршрутизаторах Cisco включена функциональная возможность DHCP-сервера.

Объявление пула адресов производится командой:

ip dhcp pool имя_пула.

Роутер переходит в режим конфигурирования пула (консольное приглашение будет оканчиваться на (config-pool)). В этом режиме указывается подсеть: **network x.x.x.x маска**, затем – адрес шлюза: **default-router IP_адрес**.

Из пула адресов необходимо исключать адреса шлюза, DNS сервера. Исключение IP адреса из пула DHCP производится в режиме конфигурирования маршрутизатора командой **ip dhcp excluded-address IP_адрес**.

На рисунке 3.3 показано содержание файла конфигурации маршрутизатора Router1 после настройки на нем DHCP сервера.

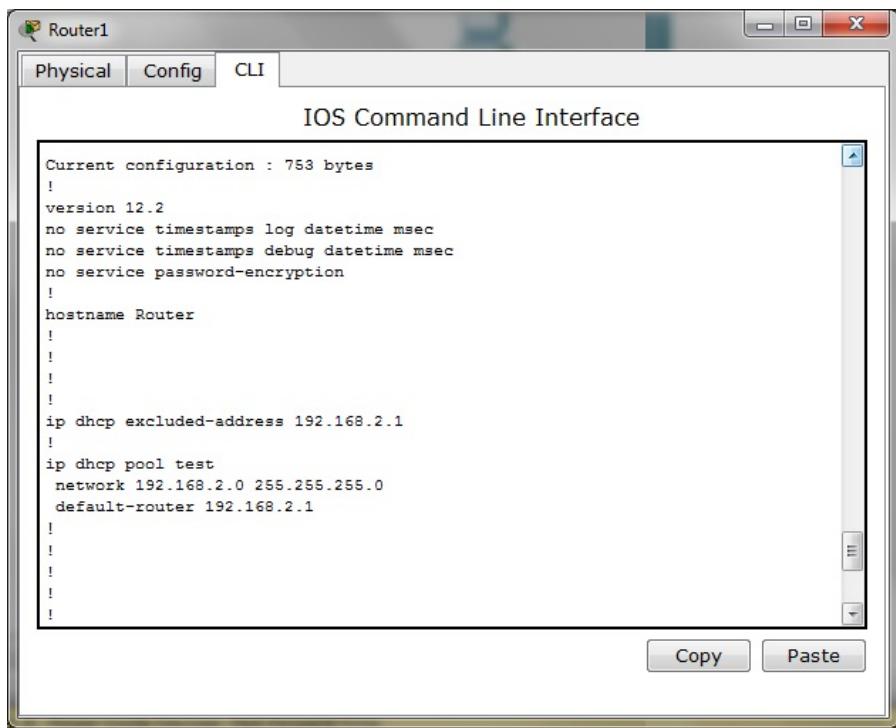


Рис. 3.3. Конфигурирование сервера DHCP на маршрутизаторе

Как и при настройке сервера DHCP на Server0, после настройки сервера DHCP на маршрутизаторе, на ПК в «IP configuration» вместо «Static» необходимо выбрать «DHCP».

Посмотреть информацию об адресах, выданных DHCP сервером, можно командой **show ip dhcp binding**.

Настроим маршрутизацию IP пакетов.

Стек протоколов TCP/IP позволяет создавать маршрутизируемые сети. Маршрутизация позволяет избежать широковещательного трафика. Существуют как динамические, так и статические способы маршрутизации. Для начала рассмотрим статическую маршрутизацию. Смысл ее состоит в указании маршрутизатору достижимости какой-либо подсети через последний доступный напрямую маршрутизатор. Указание маршрута осуществляется командой:

ip route подсеть маска IP_адрес шлюза метрика,

где подсеть и маска задаются для сети, которую мы хотим достигнуть, а **IP_адрес_шлюза**, соответственно, IP адрес последнего достижимого напрямую маршрутизатора или шлюза. Метрики — это значения, привязанные к определенным маршрутам, и классифицирующие их от наиболее предпочтительных до наименее предпочтительных. Параметры, используемые для расчета метрик, зависят от протокола маршрутизации. Путь с самой низкой метрикой выбирает-

ся в качестве оптимального пути и устанавливается в таблицу маршрутизации. Если к одной точке назначения существует несколько путей с одинаковыми метриками, нагрузка распределяется по этим путям.

Таким образом, в нашем случае, чтобы из подсети NetA можно было получить доступ в подсеть NetB, необходимо войти в режим конфигурации маршрутизатора (Router0) и прописать маршрут:

```
ip route 192.168.2.0 255.255.255.0 192.169.3.2
```

Аналогично настраивается маршрутизация на Router1.

Отменить маршрут можно добавив **no** к команде. Например:

```
no ip route 192.168.2.0 255.255.255.0 192.169.3.2
```

Статическая маршрутизация имеет ряд недостатков:

- Очень плохое масштабирование: добавление (N+1)-ой сети потребует сделать $2*(N+1)$ записей о маршрутах, причём на большинстве маршрутизаторов таблица маршрутов будет различной, при $N>3-4$ процесс конфигурирования становится весьма трудоёмким;
- Низкая устойчивость к повреждениям линий связи (особенно, в ситуациях, когда обрыв происходит между устройствами);
- Отсутствие динамического балансирования нагрузки;
- Необходимость в сопровождении отдельной документации к маршрутам, проблема синхронизации документации и реальных маршрутов.

Для устранения недостатков статической маршрутизации разработаны протоколы динамической маршрутизации. В отличие от статической маршрутизации динамическая маршрутизация имеет следующие преимущества:

- Периодический обмен информацией о маршрутах между маршрутизаторами;
- Повышенная отказоустойчивость.

Рассмотрим основные динамические способы маршрутизации.

Протокол **RIP** (англ. Routing Information Protocol) — один из наиболее распространенных протоколов маршрутизации в небольших компьютерных сетях, который позволяет маршрутизаторам динамически обновлять маршрутную информацию (направление и дальность в хопах), получая ее от соседних маршрутизаторов.

RIP — дистанционно-векторный протокол, который оперирует хопами (ретрансляционными «скачками», переходами) в качестве метрики маршрутизации. Максимальное количество хопов, разрешенное в RIP — 15 (метрика 16 означает «бесконечно большую метрику»). Каждый RIP-маршрутизатор по умолчанию вещает в сеть свою полную таблицу маршрутизации раз в 30 секунд, генерируя достаточно большой объем служебного трафика. Протокол RIP работает на сетевом уровне стека TCP/IP, используя UDP порт 520.

В современных сетевых средах RIP — не самое лучшее решение для выбора в качестве протокола маршрутизации, так как его возможности уступают более современным протоколам, таким как EIGRP, OSPF. Ограничение на 15 хопов не дает применять его в больших сетях. Единственный плюс этого протокола — простота конфигурирования.

Для того чтобы включить данный режим маршрутизации, необходимо:

1. Войти в режим конфигурирования маршрутизатора – **conf t**;
2. Войти в режим маршрутизации RIP – **router rip**;
3. Перечислить подсети, которые будут маршрутизироваться, и о которых будет передаваться информация вовне, то есть для каждого маршрутизатора должны быть описаны подсети, в общем случае, напрямую подключенные к маршрутизатору. Описание ведется с помощью команды **network x.x.x.x**.

В соответствии с определением протокола, данным выше, необходимо подождать синхронизации в течение 30 секунд или перезагрузить маршрутизатор командой **reload**, предварительно сохранив конфигурацию командой **write memory (write mem)** или заменив стартовую конфигурацию текущей при помощи команды **copy running-config startup-config**. Последняя команда производит запись содержимого первой указанной памяти во вторую, т.е. в нашем случае содержимое энергонезависимой памяти копируется в энергонезависимую память.

OSPF (англ. Open Shortest Path First) – протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала и использующий для нахождения кратчайшего пути алгоритм Дейкстры.

Протокол OSPF представляет собой протокол внутреннего шлюза. Протокол OSPF распространяет информацию о доступных маршрутах между маршрутизаторами одной автономной системы. Автономную систему можно рассматривать как набор сетей или сред с общим элементов маршрутизации. К автономным системам можно обращаться как к самостоятельным объектам, адресуя данные целой сети.

Чтобы включить режим маршрутизации OSPF, в режиме конфигурирования маршрутизатора необходимо ввести команду **router ospf 1111**, где 1111 – произвольный идентификатор процесса OSPF. Затем указываются подсети, которые будут участвовать в процессе OSPF:

network x.x.x.x wildcard_mask area id,

где команда **area** указывает зону действия OSPF, **wildcard_mask** – шаблонная маска (обратная маска):

wildcard_mask = 255.255.255.255 – маска_cети.

Для настройки протокола OSPF в нашей сети примем подсеть NetA за area 1, подсеть NetB – за area 2, подсеть NetC – за area 0. Таким образом, на Router0 необходимо прописать:

```
router ospf 1111  
network 192.168.1.0 0.0.0.255 area 1  
network 192.168.3.0 0.0.0.255 area 0
```

А на Router1:

```
router ospf 1111  
network 192.168.2.0 0.0.0.255 area 2  
network 192.168.3.0 0.0.0.3 area 0
```

После настройки маршрутизатора Router1 должно появиться сообщение о том, что процесс OSPF загрузил таблицу маршрутизации. Пример:

%OSPF-5-ADJCHG: Process 1111, Nbr 192.168.3.1 on Serial2/0 from LOADING to FULL, Loading Done

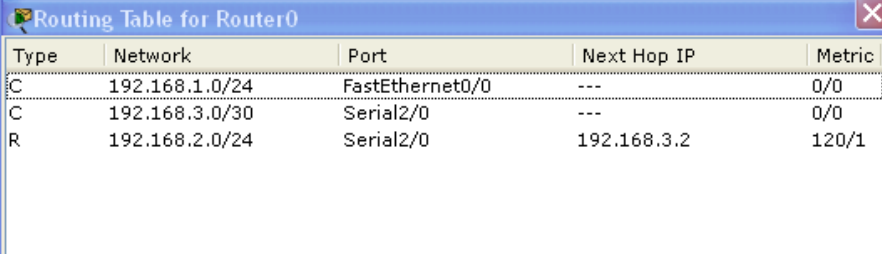
EIGRP (англ. Enhanced Interior Gateway Routing Protocol) – протокол динамической маршрутизации, разработанный фирмой Cisco. EIGRP для выбора наиболее короткого маршрута использует механизм DUAL.

Протокол EIGRP — переработанный и улучшенный вариант протокола IGRP, свободный от основного недостатка дистанционно-векторных протоколов — особых ситуаций с заикливанием маршрутов — благодаря специальному алгоритму распространения информации об изменениях в топологии сети. EIGRP более прост в реализации и менее требователен к вычислительным ресурсам маршрутизатора, чем OSPF.

Для того чтобы войти в режим конфигурирования протокола EIGRP, необходимо набрать команду **router eigrp номер_автономной_системы**.

Далее с помощью команды **network x.x.x.x wildcard_mask** задается сеть, которая непосредственно подключена к маршрутизатору и о существовании которой наш маршрутизатор будет сообщать своим соседям. Так же с помощью команды **passive-interface** можно указать порт, в который маршрутизатор не должен отправлять обновленную таблицу маршрутизации.

Текущие обслуживаемые маршрутизатором подсети (таблицу маршрутизации) можно посмотреть с помощью команды **sh ip route** или с помощью инструмента программного эмулятора – «The Inspector»: выбрать интересующий маршрутизатор и в раскрывающемся меню – пункт «Routing Table» (Рис. 3.4).



Type	Network	Port	Next Hop IP	Metric
C	192.168.1.0/24	FastEthernet0/0	---	0/0
C	192.168.3.0/30	Serial2/0	---	0/0
R	192.168.2.0/24	Serial2/0	192.168.3.2	120/1

Рис. 3.4. Таблица маршрутизации

Как видно из рисунка, слева от каждой записи, содержащейся в таблице, имеется буквенный код:

- Код *C* означает, что обслуживаемые подсети непосредственно подсоединены к маршрутизатору. Запись с кодом *C* появляется в таблице сразу после включения интерфейса маршрутизатора и назначения ему IP адреса;
- Код *S* является обозначением статического маршрута;
- Маршруты, полученные от протоколов динамической маршрутизации:
 - Код *R* – RIP;
 - Код *D* – EIGRP;
 - Код *O* – OSPF;

- Код * – маршрут по умолчанию.

Задание к лабораторной работе:

1. В утилите Cisco Packet Tracer собрать модель сети по схеме, изображенной на рисунке 3.1;
2. Присвоить Server0 – IP 192.168.1.3, шлюз 192.168.1.1, маска 255.255.255.0;
Присвоить int s2/0 на Router0 – 192.168.3.1/30;
Присвоить int s2/0 на Router1 – 192.168.3.2/30;
(см. варианты ниже).
3. Настроить DHCP: для подсети NetA DHCP-сервером будет Server0, а для подсети NetB – Router1.
4. Настроить маршрутизацию статическим и динамическими способами.
5. Посмотреть полученные таблицы маршрутизации.
6. Проверить работу сети, используя команды *ping* и *tracert*.

Варианты заданий:

Вариант	NetA	NetB	NetC
1	192.169.1.0/24	192.169.2.0/24	192.169.3.0/30
2	172.16.1.0/24	172.16.2.0/28	172.16.3.0/30
3	10.10.1.0/24	10.10.2.0/24	10.10.3.0/30
4	172.168.1.0/24	172.168.2.0/24	172.168.3.0/30
5	192.16.1.0/28	192.16.2.0/24	192.16.3.0/30
6	172.12.1.0/24	172.12.2.0/24	172.12.3.0/30

Контрольные вопросы:

1. Понятие инкапсуляции.
2. Основные понятия протокола PPP (точка-точка).
3. Понятие маршрутизации в сетях TCP/IP. Маршруты и таблица маршрутизации.
4. Статическая маршрутизация, настройка и недостатки.
5. Динамическая маршрутизация, основные понятия, протоколы и алгоритмы реализации.
6. Основные принципы маршрутизации по протоколу RIP.
7. Основные принципы маршрутизации по протоколу OSPF.
8. Основные принципы маршрутизации по протоколу EIGRP.
9. Назначение протокола DHCP. Опции DHCP.
10. Сегментирование TCP/IP сетей.

ЛАБОРАТОРНАЯ РАБОТА №4

Фильтрация IP пакетов. Стандартные и расширенные списки доступа

Цель работы: ознакомиться с понятием фильтрации трафика, типами листов доступа. Научиться настраивать листы доступа на оборудовании компании Cisco.

Теоретические сведения

В данной работе используется схема сети из лабораторной работы №3. Маршрутизацию пакетов в данной локальной сети необходимо назначить с использованием протокола динамической маршрутизации RIP.

Access Control List или **ACL** — список контроля доступа, который определяет, кто или что может получать доступ к конкретному объекту, и какие именно операции разрешено или запрещено этому субъекту проводить над объектом. В оборудовании Cisco ACL представляют список правил, определяющих порты служб или имена доменов, доступных на узле или другом устройстве третьего уровня OSI, каждый со списком узлов и/или сетей, которым разрешен доступ к сервису. Сетевые листы ACL могут быть настроены как на обычном сервере, так и на маршрутизаторе и могут управлять как входящим, так и исходящим трафиком, в качестве межсетевого экрана.

Для внедрения фильтрации трафика необходимо назначить списки доступа, которые создаются по принципу «запрещено все, что не разрешено». Списки доступа создаются для каждого необходимого интерфейса маршрутизатора, однако прописываются они в общем режиме конфигурирования устройства.

Списки доступа подразделяются на две категории: стандартные и расширенные. Стандартный список доступа выполняет сравнение только с IP-адресом источника пакета, тогда как расширенный список доступа может осуществлять сравнение с IP-адресами источника и пункта назначения, типом IP-протокола, портами источника и пункта назначения транспортного уровня.

Список доступа выглядит следующим образом:

ip access-list 1 permit 175.10.1.0 0.0.0.255,

где *1* – идентификатор листа доступа, ***permit*** – префикс разрешения (***deny*** – префикс запрещения), после чего идет подсеть и обратная маска подсети. Такой лист доступа разрешает любые действия по отношению к указанной подсети. Возможен лист доступа следующего вида:

ip access-list 100 permit tcp host 175.10.1.2 any eq telnet,

где после ***permit*** идет обозначение протокола, далее идет адрес, к которому разрешено данное соединение (***host 175.10.1.2***), после чего – обозначение группы адресов, которым оно разрешено (***any*** – всем); после префикса ***eq*** идет номер порта, по которому разрешено соединение (используется стандартное наименование порта или его номер: ***http*** или ***80***, ***ftp*** или ***21*** и т.п.).

Данные ***access-list's*** являются простыми, так как позволяют разместить внутри себя только одно правило. В случае, когда правил должно быть несколько, используется расширенный ***access-list***, который строится следующим обра-

ip access-list extended test***remark-----this is an example-----******permit tcp host 192.168.1.3 host 192.168.3.2 eq 80******permit tcp host 192.168.1.2 host 192.168.3.2 eq 21***

где ***extended*** обозначает тип листа доступа (расширенный), ***remark*** – комментарий к листу доступа, далее идут стандартные правила для листа доступа.

Все списки доступа неявно имеют в конце оператор ***deny***. Это означает, что любой пакет, который не удовлетворяет критериям фильтрации одной из строк списка доступа, запрещается.

Затем необходимо включить данный интерфейс в группу листа доступа (находясь в режиме конфигурирования интерфейса) командой:

ip access-group test in,

где ***test*** – имя листа доступа (при создании листа доступа он автоматически распространяется на все интерфейсы), ***in*** – направление трафика – входящий (может быть установлено значение ***out*** – исходящий). Следует отметить, что одному интерфейсу может быть назначен только один список доступа в одном направлении.

Отменить действие листа доступа можно командой:

no ip access-group test in.

К примеру, если на Router0 поставить лист доступа, представленный ниже, то с ПК PC1 будет возможен ping на ПК PC0, однако невозможен ping на Server0.

ip access-list extended test***permit icmp host 192.168.2.2 host 192.168.1.3******permit udp host 192.168.3.2 host 192.168.1.2***

Также с Router0 в соответствии с данным листом доступа станет возможна выгрузка конфигурации на Server0. Пример выгрузки конфигурации показан ниже:

Router#***copy running-config tftp***Address or name of remote host []? ***192.168.1.2***Destination filename [Router-config]? ***555***

Writind running-config...!!

[OK – 956 bytes]

956 bytes copied in 0.021 secs (45000 bytes/sec)

Router#

Однако если принудительно исключить все интерфейсы из-под действия командой ***no ip access-group 1 in***, ограничения будут сняты.

В Cisco Packet Tracer имеется возможность экспорта конфигурации маршрутизаторов и коммутаторов в текстовый файл. Для этого необходимо зайти на устройстве в раздел «Config», на левой панели выбрать пункт «Settings» и

произвести экспорт «Running Config». Данные будут экспортированы в текстовый файл, открыв который через текстовый редактор, можно изменить конфигурацию устройства. Поскольку листы доступа прописываются в файле конфигурации, их так же можно редактировать при помощи экспорта конфигурации. После того как мы отредактировали этот файл, необходимо произвести загрузку данной конфигурации в маршрутизатор. Для этого в разделе «Config» выбираем пункт «Settings», нажимаем на кнопку «Merge» и выбираем изменённый нами файл. Чтобы изменения вступили в силу, маршрутизатор необходимо перезагрузить командой **reload**.

Так же можно экспортировать конфигурацию на сервер и скачать на компьютер через FTP сервер. Для этого необходимо зайти на маршрутизатор, установить имя пользователя и пароль для подключения к FTP, командами: **ip ftp username имя_пользователя** и **ip ftp password пароль**. Чтобы скопировать конфигурацию на FTP сервер, необходимо ввести команду **copy running-config ftp**. В результате проделанных действий, файл конфигурации появится на FTP сервере. Далее скачиваем файл с FTP сервера на компьютер (рассматривалось в лабораторной работе №2).

Задание к лабораторной работе:

1. Загрузить схему из лабораторной работы №3;
2. Настроить сервисы, описанные в лабораторной работе №2.
3. В соответствии с вариантами настроить списки доступа.
4. Продемонстрировать работу списков доступа.

Варианты листов доступа:

1. С PC0 возможен ping на Server1, но не возможен на PC1;
С Server0 возможен ping и на Server1, и на PC1;
Router0 может выгружать конфигурацию на Server1;
PC1 не может подключаться к FTP на Server0;
2. С PC0 не возможен ping на Server1, но возможен ping на PC1;
С Server0 не возможен ping ни на Server1, ни на PC1;
Router1 может выгружать конфигурацию на Server1;
PC0 может подключаться по HTTP к Server1;
3. С PC1 возможен ping на Server0, но не возможен ping на PC0;
С PC0 возможен ping и на Server1, и на PC1;
Router0 не может выгружать конфигурацию на Server1;
PC0 может подключаться к FTP на Server1;
4. С PC0 не возможен ping ни на Server1, ни на PC1;
С Server0 возможен ping и на Server1, и на PC1;
Router1 может выгружать конфигурацию на Server0 и Server1;
PC1 может подключаться к FTP и HTTP к Server0;
5. С Server1 возможен ping на Server0, но не возможен ping на PC0;
С Server0 возможен ping на Server1, но не возможен ping на PC1;
Router0 не может выгружать конфигурацию на Server0, но может – на

Server1;

PC0 может подключаться к HTTP на Server1;

Контрольные вопросы:

1. Понятие списка доступа.
2. Простые и расширенные списки доступа.
3. На каком уровне модели OSI работает протокол UDP?
4. Различия между протоколами UDP и TCP.
5. Назначение протокола ICMP.
6. Перечислите и опишите основные протоколы прикладного уровня модели OSI.

ЛАБОРАТОРНАЯ РАБОТА №5

Создание защищенной распределенной сети передачи данных

Цель работы: ознакомиться с различными линиями связи и активными сетевыми устройствами; смоделировать и настроить защищенную распределенную сеть передачи данных; настроить маршрутизацию, списки доступа; изучить сервис Syslog.

Теоретические сведения

Рассмотрим сеть передачи данных, изображенную на рисунке 5.1. На примере этой сети рассмотрим различные типы устройств и различные типы соединений.

В качестве центрального устройства в схеме используется **коммутатор третьего уровня**. Коммутаторы третьего уровня в дополнение к обычным функциям способны маршрутизировать трафик между портами на IP-уровне (3-м уровне модели OSI). Примерами таких устройств могут служить коммутаторы Catalyst 3550, 3560, 3750, Catalyst 4500/4000 с модулем Sup II+ и выше или Catalyst 6500/6000, работающие на основе системного ПО Cisco IOS. В данной лабораторной работе выбираем модель 3560-24PC в разделе Switches.

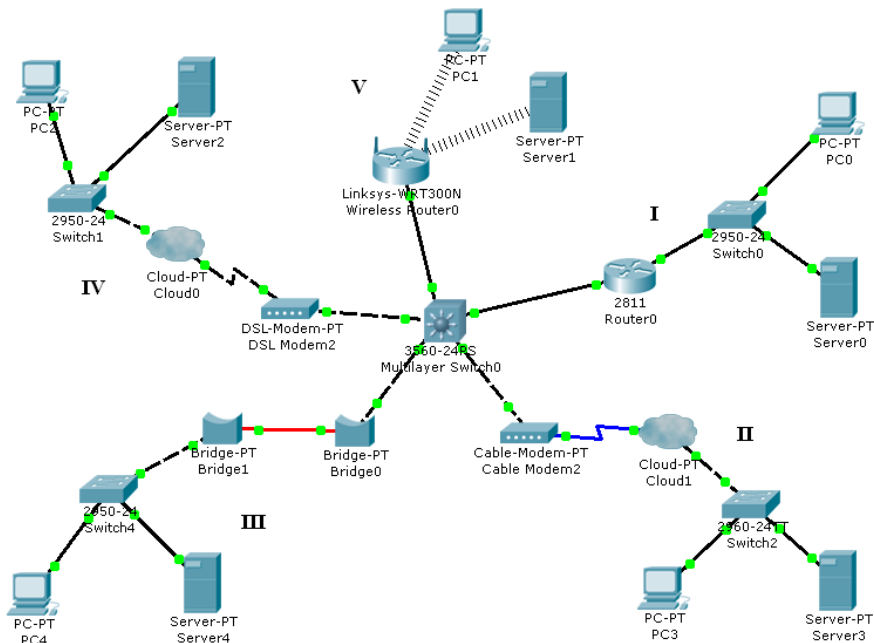


Рис. 5.1. Схема сети

Ветвь I является примером сети, построенной с использованием витой

пары по технологии FastEthernet; в ветви II используется коаксиальное соединение; в ветви III – оптическая линия передачи данных; в ветви IV – соединение по технологии DSL, в ветви V – беспроводное WiFi соединение.

Сеть передачи данных состоит из следующих подсетей:

1. NetA: интерфейс FastEthernet 0/1 центрального свитча (в качестве шлюза) и интерфейс FastEthernet 0/0 маршрутизатора Router0 – подсеть 192.168.2.0/30;
2. NetB: интерфейс FastEthernet 0/2 центрального свитча (в качестве шлюза) и подсоединенная к нему ветвь II – подсеть 192.168.3.0/24;
3. NetC: интерфейс FastEthernet 0/3 центрального свитча (в качестве шлюза) и подсоединенная к нему ветвь III – подсеть 192.168.4.0/24;
4. NetD: интерфейс FastEthernet 0/4 центрального свитча (в качестве шлюза) и подсоединенная к нему ветвь IV – подсеть 192.168.5.0/24;
5. NetE: интерфейс FastEthernet 0/5 центрального свитча (в качестве шлюза) и интерфейс Internet роутера Wireless Router0 – подсеть 192.168.6.0/24;
6. NetF: интерфейс FastEthernet 0/1 маршрутизатора Router0 подсоединенные к нему через Switch0 ПК PC0 и сервер Server0 – подсеть 192.168.7.0/24.
7. NetG: сеть WiFi, образованная роутером Wireless Router0, ПК PC1 и сервером Server1 – подсеть 192.168.8.0/24.

Подробно рассмотрим каждую ветвь сети.

Ветвь I состоит из следующих сетевых устройств: маршрутизатор Cisco 2811, коммутатор 2950-24, персональный компьютер и сервер.

Рассмотрим ветвь II. В нее входят устройства: кабельный модем Cable-Modem-PT и облако Generic Cloud-PT из класса устройств WAN Emulation, коммутатор 2960-24TT, персональный компьютер и сервер.

Кабельным модемом называется абонентское устройство, обеспечивающее высокоскоростной доступ к Интернету по сетям кабельного телевидения, они используют асимметричную технологию, которая наиболее оптимально подходит для пользовательского доступа к Интернету. При этом максимально возможная скорость приема данных таким модемом, может достигать порядка 40 Мбит/с и скорость передачи данных порядка 10 Мбит/с. Как и модем, предназначенный для соединения по коммутируемым телефонным линиям, это устройство представляет собой двунаправленный аналогово-цифровой преобразователь данных, использующий в процессе передачи информации принцип наложения на несущую частоту модулированного аналогового сигнала. Существенным отличием данного аппаратного средства от обыкновенного модема является то, что кабельный модем не требует установки каких-либо драйверов, поскольку он подключается к компьютеру посредством сетевой карты и является абсолютным прозрачным для системы.

Модем подсоединяется к центральному свитчу обратным патч-кордом, а к облаку – коаксиальным соединением; далее от облака к свитчу подключен обратный патч-корд и т.д. Как настраивать ПК и сервер, вам уже известно. Ка-

бельный модем не имеет никаких настроек. Для настройки облака необходимо зайти во вкладку «Config», на левой панели выбрать пункт «Interface» → «Ethernet6» и указать для этого интерфейса тип соединения «Cable». Затем на левой панели следует выбрать «Connections» → «Cable», указать порты, соединенные кабелем, и нажать кнопку «Add» (Рис. 5.2).

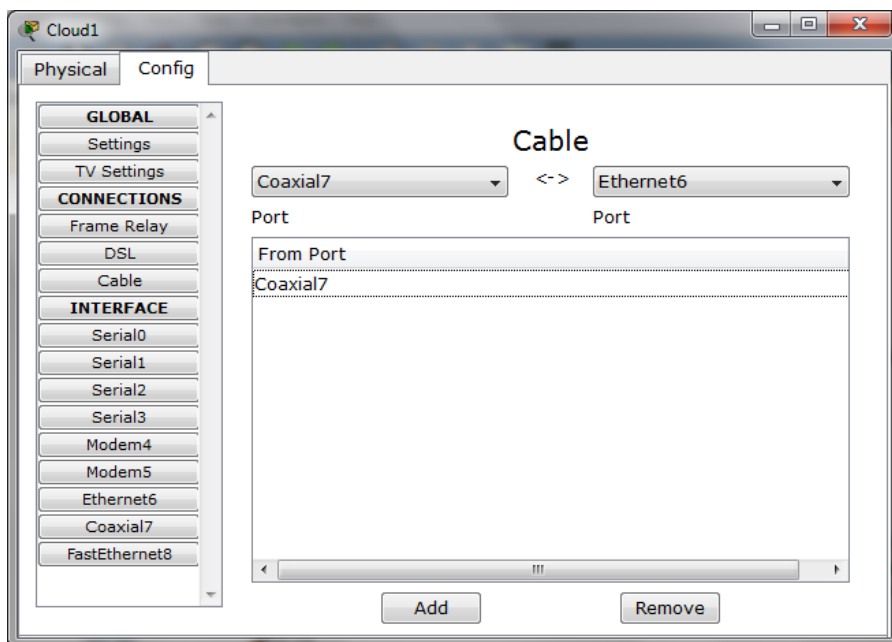


Рис. 5.2. Настройка облака (ветвь II)

Рассмотрим ветвь III. В нее входят 2 моста Generic Bridge-PT (из класса устройств Switches), коммутатор 2950-24, ПК и сервер.

Мост — это сетевое устройство, которое функционирует на канальном уровне сетевой модели. Мост на уровне канала передачи данных соединяет несколько сетевых сегментов в один логический сетевой сегмент. Существует несколько различных типов мостов:

- Прозрачные или обучающиеся (способны обрабатывать соединение только с одинаковыми протоколами канального уровня).
- Инкапсулирующие (вкладывают кадр канального уровня одного типа в кадр канального уровня другого типа, что делает возможным прозрачное мостовое соединение между одинаковыми канальными уровнями передачи данных, когда они физически разделены вторым отличающимся канальным уровнем).
- Транслирующие (выполняют функции прозрачного моста между двумя различными типами протоколов канального уровня).
- С маршрутизацией от источника.

- Транслирующие с маршрутизацией от источника.

Применение мостов позволяет разделить физический и логический виды трафика и этим снизить нагрузку на сегмент сети.

В программном эмуляторе Cisco Packet Tracer мосты Generic Bridge-PT по умолчанию содержат 2 порта Ethernet. Один из них необходимо заменить на GigabitEthernet (для обеспечения оптического соединения). Для этого необходимо зайти во вкладку «Physical» устройства, на левой панели выбрать необходимый модуль: PT-Switch-NM-1FGE (изображение модуля появится в нижней части окна) (Рис. 5.3).

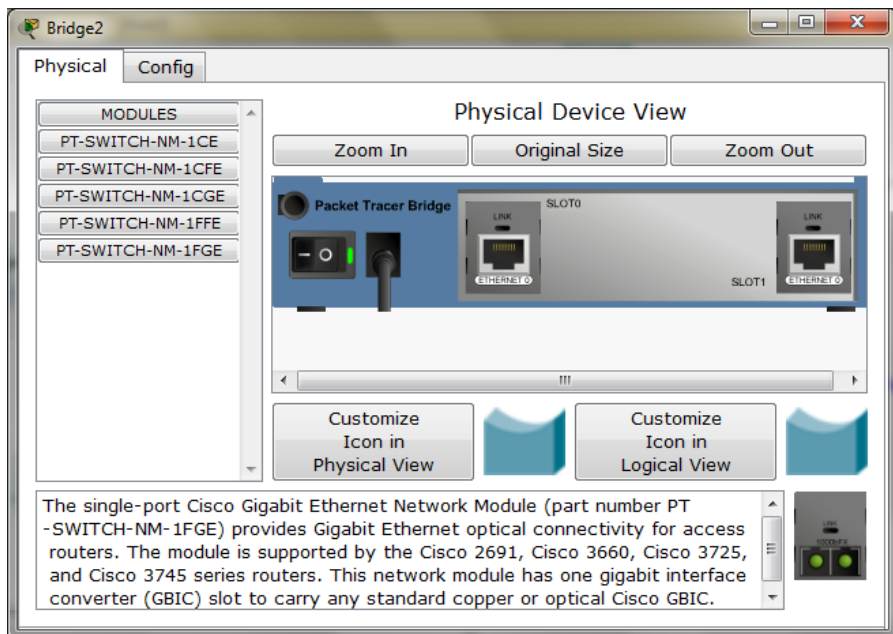


Рис. 5.3. Замена интерфейса в мосте

Чтобы заменить порт, устройство необходимо выключить: на изображении устройства щелкнуть по кнопке питания. Затем один из слотов устройства освобождается (его содержимое перетаскивается на левую панель), и на освободившееся место перетаскивается изображение выбранного ранее модуля. После замены порта устройство необходимо включить.

Подобным образом можно заменять (добавлять) порты в других устройствах.

Рассмотрим ветвь IV. В нее входят устройства: DSL модем DSL-Modem-PT и облако Generic Cloud-PT из класса устройств WAN Emulation, коммутатор 2950-24, ПК и сервер.

Технология цифровых абонентских линий **Digital Subscriber Line** (DSL) — это набор различных технологий, позволяющих организовать цифровую абонентскую линию. DSL работает в сетях с топологией «звезда», в которых от

центра к листовым узлам проложены выделенные линии связи на основе медных кабелей типа «витая пара» (т.е. технология DSL работает на основе телефонных линий). Скорость передачи данных между центральным и листовыми узлами может лежать в пределах от 64 Кбит/с до 8 Мбит/с. Эта скорость зависит от характеристик используемого кабеля, количества физических соединений, расстояния, которое проходит сигнал, погодных условий и конкретной используемой технологии DSL.

На данный момент на рынке существует много различных вариантов технологии DSL. В сетевой промышленности эту группу технологий принято называть xDSL. В нее входят технология асимметричной абонентской линии (Asymmetric Digital Subscriber Line — ADSL), технология симметричной абонентской линии (Symmetric DSL — SDSL) и технология сверхскоростной абонентской линии (Very High Data Rate DSL — VDSL).

Для соединения DSL модема и облака используется телефонное соединение. Как и в случае с кабельным модемом, DSL модем не имеет никаких настроек (можно только изменить его имя). Для настройки облака необходимо зайти во вкладку «Config», на левой панели выбрать пункт «Interface» → «Ethernet6» и указать для этого интерфейса тип соединения «DSL». Затем на левой панели следует выбрать «Connections» → «DSL», указать порты, соединенные по данной технологии, и нажать кнопку «Add» (Рис. 5.4).

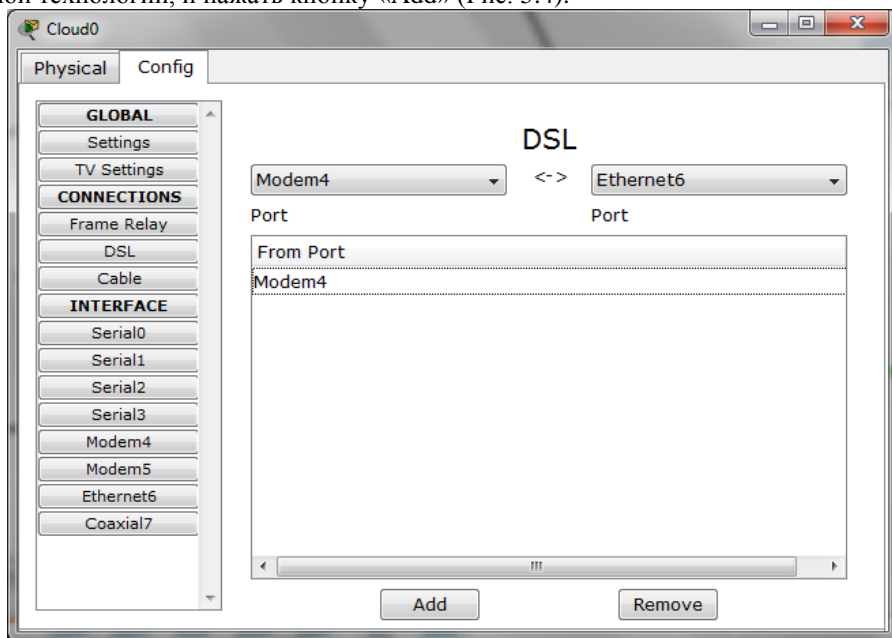


Рис. 5.4. Настройка облака (ветвь IV)

Рассмотрим ветвь V. В нее входят устройства: WiFi роутер Linksys-WRT300N из класса устройств Wireless Devices, ПК и сервер.

Wi-Fi (сокр. от Wireless Fidelity – беспроводная точность) – технология беспроводных сетей. Технология Wi-Fi предназначена для доступа на коротких дистанциях и, в то же время, на достаточно больших скоростях. Ядром такой сети является точка доступа (Access Point). Вокруг неё образуется территория радиусом 50-100 метров, называемая хот-спотом, или зоной Wi-Fi. В принципе, можно связать и просто два устройства, минуя точку доступа, но полной функциональности добиться при этом будет невозможно.

Наиболее распространены три модификации стандарта Wi-Fi – IEEE 802.11a, b и g. Они различаются максимальной возможной скоростью передачи данных и дальностью, на которой может быть установлено соединение.

Для настройки Wireless Router0 необходимо зайти во вкладку «GUI», на верхней панели выбрать пункт «Setup». Сначала настраиваем внешнее соединение (т.е. порт Internet) – подсеть NetE. Для этого в блоке «Internet Setup» выбираем «Static IP», вводим внешний IP адрес данного роутера «Internet IP Address», маску внешней подсети «Subnet Mask» и IP адрес шлюза «Default Gateway» (Рис. 5.5).

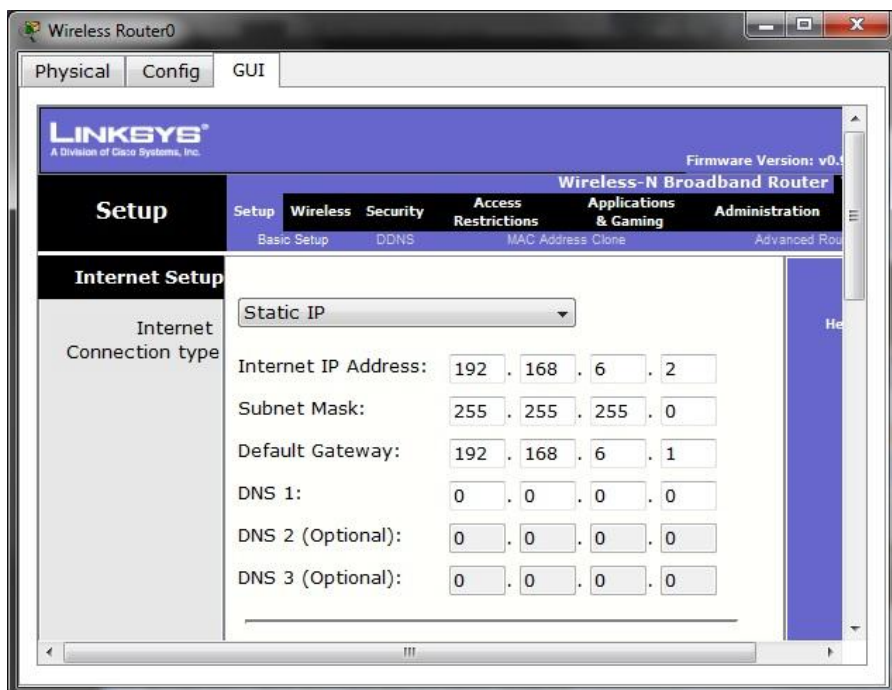


Рис. 5.5. Настройка внешнего соединения Wireless Router

Затем настраиваем подсеть NetG – блок «Network Setup». Настройка производится по DHCP. В поле «IP Address» вводим IP адрес роутера в сети WiFi и выбираем нужную маску подсети. Затем включаем DHCP Server, выбрав пункт «Enable». В поле «Start IP Address» указываем тот же адрес, что и в поле «IP

Address». После выполнения всех настроек необходимо нажать кнопку «Save Settings» внизу страницы (Рис. 5.6).

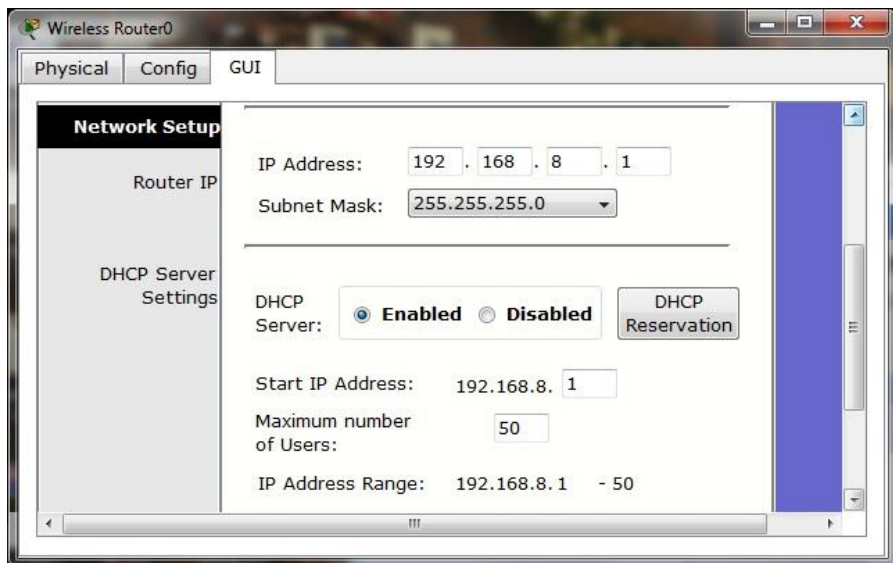


Рис. 5.5. Настройка Wireless Router

Центральному коммутатору (его интерфейсу Vlan1) присвоим IP адрес 192.168.1.1/30.

Чтобы отдельному интерфейсу коммутатора (а не устройству в целом) можно было присвоить IP адрес и использовать его для маршрутизации пакетов на третьем уровне, необходимо настроить порт в качестве порта третьего уровня. Для этого используется команда **no switchport** (в режиме конфигурирования интерфейса), которая отключает функции второго уровня и включает операции третьего уровня. Отключение функций третьего уровня производится командой **switchport**. При вводе данных команд порт отключается, а затем включается снова.

Теперь настроим маршрутизацию в сети. В данной лабораторной работе маршрутизация настраивается по протоколу RIP версии 2 (RIPv2). **RIPv2** является расширением RIP версии 1 (RIPv1). Он обеспечивает передачу дополнительной информации, пользуясь пакетами того же формата, что и RIPv1. Например, RIPv1 не способен передавать информацию о маске сети назначения, а RIPv2 способен. Соответственно, в среде RIPv1 можно использовать сети только с натуральной адресацией, т.е. нельзя использовать подсети, а в RIPv2 можно использовать подсети.

Для перехода к версии 2 протокола RIP необходимо в режиме конфигурирования маршрутизации по данному протоколу ввести команду **version 2**.

Прежде, чем настраивать маршрутизацию на свитче третьего уровня, необходимо включить на нем функцию маршрутизации с помощью команды **ip routing** (в режиме конфигурирования свитча). Даже если маршрутизация уже

была включена, данный шаг позволит убедиться в этом. Далее настройка маршрутизации производится так же, как и на роутере. Как настраивать маршрутизацию на роутере, уже говорилось в лабораторной работе №3.

Сервис **Syslog** – это стандарт отправки сообщений о происходящих в системе событиях (логов), использующийся в компьютерных сетях, работающих по протоколу IP. В сети выделяется один или несколько Syslog серверов, на которые будет производиться отправка сообщений с важных сетевых устройств.

В данной лабораторной работе необходимо настроить Syslog-сервер и отpravку сообщений на него с маршрутизаторов и центрального свитча.

Для настройки сбора сообщений с маршрутизатора Cisco необходимо:

- Указать адрес Syslog сервера, на который будут отсылааться сообщения, командой **logging x.x.x.x**;
- Настроить уровень вывода системных сообщений командой **logging trap**.

Чтобы настроить Syslog сервер в программном эмуляторе Cisco Packet Tracer, необходимо на сервере, адрес которого указывался при настройке Syslog на маршрутизаторе (свитче), зайти во вкладку «Config», на левой панели выбрать вкладку «Services» → «Syslog». Включить «Syslog». В таблице будет собираться информация о логах (Рис. 5.7).

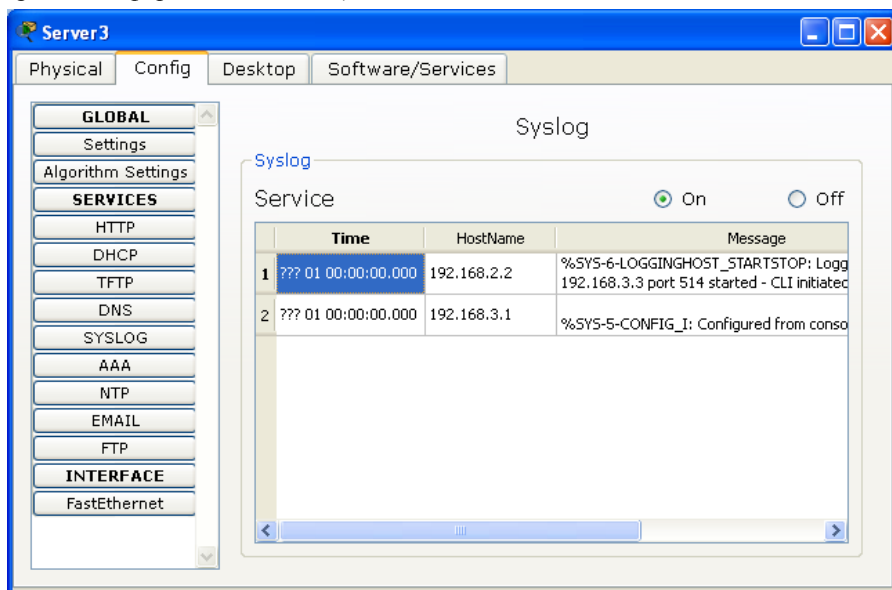


Рис. 5.7. Настройка Syslog сервера

Задание к лабораторной работе:

1. Собрать схему, изображенную на рисунке 5.1;
2. Настроить устройства, настроить маршрутизацию;
3. В соответствии с вариантами настроить списки доступа (только меж-

ду двумя указанными в варианте ветвями, остальные ветви не доступны);

4. Настроить Syslog (в качестве Syslog сервера использовать сервер, указанный в варианте задания).

Варианты заданий:

1. Ветви IV и I
С Server0 не возможен ping на PC2, но возможен на Server2;
С Server2 возможен ping на PC0;
Syslog направляется на Server2.
2. Ветви IV и II
С Server2 не возможен ping на Server3, но возможен на PC3;
С PC2 возможен ping на Server3;
Syslog направляется на Server3.
3. Ветви III и II
С PC4 не возможен ping на PC3, но возможен на Server3;
С Server3 возможен ping на Server4;
Syslog направляется на Server4.
4. Ветви I и III
С PC4 возможен ping на Server0, но не возможен на PC0;
С PC0 возможен ping на Server4;
Syslog направляется на Server0.
5. Ветви I и II
С PC0 не возможен ping на PC3, но возможен на Server3;
С Server0 возможен ping на Server3;
Syslog направляется на Server3.
6. Ветви IV и III
С PC2 не возможен ping на Server4, но возможен на PC4;
С Server2 возможен ping на PC4;
Syslog направляется на Server2.

Контрольные вопросы:

1. Понятие коммутации третьего уровня. Коммутаторы третьего уровня
2. Понятие кабельного модема.
3. Понятие DSL. Перечислите протоколы технологии DSL?
4. Понятие моста.
5. Типы соединений: оптическое, телефонное, коаксиальное.
6. Понятие WiFi. Стандарты WiFi.
7. Различие между протоколами RIPv1 и RIPv2.
8. Понятие сервиса Syslog.

ЛАБОРАТОРНАЯ РАБОТА №6

Виртуальные частные сети передачи данных

Цель: получить представление о средствах информационной безопасности, применяемых в маршрутизаторах Cisco. Научиться настраивать виртуальные частные сети.

Теоретические сведения

VPN (англ. Virtual Private Network — виртуальная частная сеть) — обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, Интернет). Несмотря на то, что коммуникации осуществляются по сетям с меньшим неизвестным уровнем доверия (например, по публичным сетям), уровень доверия к построенной логической сети не зависит от уровня доверия к базовым сетям благодаря использованию средств криптографии (шифрования, аутентификации, инфраструктуры открытых ключей, средств для защиты от повторов и изменений передаваемых по логической сети сообщений).

Обычно VPN развёртывают на уровнях не выше сетевого, так как применение криптографии на этих уровнях позволяет использовать в неизменном виде транспортные протоколы (такие как TCP, UDP).

VPN состоит из двух частей: «внутренняя» (подконтрольная) сеть, которых может быть несколько, и «внешняя» сеть, по которой проходит инкапсулированное соединение (обычно используется Интернет).

IPSec (сокращение от IP Security) — набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP, позволяет осуществлять подтверждение подлинности и/или шифрование IP-пакетов. IPSec также включает в себя протоколы для защищённого обмена ключами в сети Интернет.

Существует два режима работы IPSec: транспортный режим и туннельный режим.

В транспортном режиме шифруется (или подписывается) только информативная часть IP-пакета. Маршрутизация не затрагивается, так как заголовок IP пакета не изменяется (не шифруется). Транспортный режим, как правило, используется для установления соединения между хостами. Он может также использоваться между шлюзами, для защиты туннелей, организованных каким-нибудь другим способом (IP tunnel, GRE и др.).

В туннельном режиме IP-пакет шифруется целиком. Для того чтобы его можно было передать по сети, он помещается в другой IP-пакет. По существу, это защищённый IP-туннель. Туннельный режим может использоваться для подключения удалённых компьютеров к виртуальной частной сети или для организации безопасной передачи данных через открытые каналы связи (например, Интернет) между шлюзами для объединения разных частей виртуальной частной сети.

Рассмотрим схему, изображённую на рисунке 6.1.

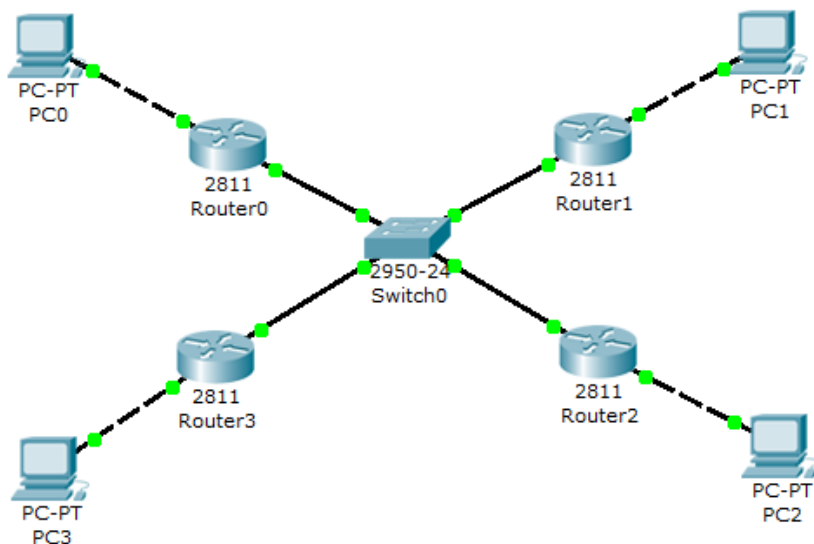


Рис. 6.1. Схема сети

На данной схеме рассмотрены следующие подсети:

1. Порты FastEthernet0/0 маршрутизаторов Router0, Router1, Router2, Router3 представляют собой подсеть NetA;
2. Порт FastEthernet0/1 маршрутизатора Router0 и порт ПК PC0 представляют собой подсеть NetB;
3. Порт FastEthernet0/1 маршрутизатора Router1 и порт ПК PC1 представляют собой подсеть NetC;
4. Порт FastEthernet0/1 маршрутизатора Router2 и порт ПК PC2 представляют собой подсеть NetD;
5. Порт FastEthernet0/1 маршрутизатора Router3 и порт ПК PC3 представляют собой подсеть NetE.

Начальным этапом защиты оборудования является закрытие свободного доступа на маршрутизаторы и коммутаторы. Доступ может быть закрыт как на telnet подключение к оборудованию (рассматривалось в лабораторной работе №2), так и на привилегированный режим.

Привилегированный режим закрывается в режиме конфигурирования командой **enable password пароль**. Но в таком случае, пароль будет храниться в конфигурации в открытом виде. Для того чтобы в конфигурацию сохранялся не сам пароль, а его хэш-вектор, необходимо ввести команду **enable secret пароль**.

Доступ к консоли оборудования может быть произведен как для удаленных пользователей, так и для пользователей, подключенных к оборудованию напрямую. В последнем случае, необходимо набрать команды:

```
line console 0
login
password пароль.
```

Здесь так же в случае использования ключевого слова **password** – пароль будет храниться в открытом виде, в обратном случае – в виде хэш-вектора. Для того чтобы проверить наличие пароля, необходимо выйти командой **logout** и нажать ENTER для инициирования нового входа.

Оборудование Cisco поддерживает создание виртуальных частных сетей с шифрованием с помощью IPsec.

Для примера рассмотрим подсети NetA: 192.168.1.0/24, NetB: 192.168.2.0/24, NetC: 192.168.3.0/24, NetD: 192.168.4.0/24, NetE: 192.168.5.0/24.

С помощью описанных ранее в данной лабораторной работе команд поставьте пароли на доступы к маршрутизаторам и на переходы в привилегированный режим.

Далее настроим туннель между сетями NetB и NetD.

Настройка туннеля начинается с того, что на шлюзе для ПК PC0 (им является Router0) выставляется политика шифрования (ISAKMP policy):

```
crypto isakmp policy 1  
hash md5  
authentication pre-share  
encryption des  
group 1.
```

С помощью команды ? после ключевых слов политики вы можете узнать, какие еще методы шифрования, хэширования, аутентификации и передачи ключей поддерживает оборудование Cisco.

Далее создадим лист доступа, разрешающий доступ по протоколу IP подсети 192.168.2.0 к 192.168.4.0 (подключать список доступа к какому-либо интерфейсу не нужно):

```
access-list 110 permit ip 192.168.2.0 0.0.0.255 192.168.4.0 0.0.0.255.
```

После этого выставляется ключ для аутентификации шлюзов и схема функционирования IPsec (аутентификация AH-SHA-HMAC, шифрование ESP-DES):

```
crypto isakmp key cisco address 192.168.1.3  
crypto ipsec transform-set set_1 ah-sha-hmac esp-des.
```

И, наконец, открываем туннель на шлюз с ранее созданными настройками:

```
crypto map crypto_map 1 ipsec-isakmp  
set peer 192.168.1.3  
set transform-set set_1  
match address 110.
```

Следует отметить, что ключ аутентификации и схема функционирования IPsec выставляются на внешний интерфейс, т.е. в нашем случае – на интерфейс, находящийся в сети NetA.

Последним этапом является применение схемы шифрования туннеля к необходимому сетевому интерфейсу (в режиме его конфигурирования):

```
crypto map crypto_map.
```


Аналогично настраивается и противоположный шлюз Router2 (настройки зеркальные).

После настройки туннелей PC0 и PC2 должны быть доступны при использовании утилиты *ping*. Количество шифрованных пакетов, прошедших через шлюз можно посмотреть с помощью команды *show crypto ipsec sa*.

Задание к лабораторной работе:

1. Собрать схему, изображенную на рисунке 6.1;
2. Установить пароли на маршрутизаторах;
3. В соответствии с вариантами настроить туннели между маршрутизаторами.

Варианты заданий:

1. Подсеть NETb и NETc;
2. Подсеть NETb и NETd;
3. Подсеть NETb и NETe;
4. Подсеть NETc и NETd;
5. Подсеть NETc и NETe;
6. Подсеть NETd и NETe.

Контрольные вопросы:

1. Понятие VPN. На каких уровнях модели OSI развертывают?
2. Понятие IPSec. Режимы работы IPSec.
3. Понятие туннелирования, инкапсуляции.
4. Шифрование и аутентификация в сетях.

ЛАБОРАТОРНАЯ РАБОТА №7

Агрегирование каналов передачи данных

Цель: получить представление и настроить оборудование Cisco для работы с использованием технологии агрегирования каналов передачи данных.

Теоретические сведения

Агрегирование каналов (агрегация каналов, англ. link aggregation) — технология, которая позволяет объединить несколько физических каналов в один логический. Агрегирование каналов может быть настроено между двумя коммутаторами, коммутатором и маршрутизатором, между коммутатором и хостом.

Агрегирование каналов позволяет решить две задачи:

- повысить пропускную способность канала;
- обеспечить резерв на случай выхода из строя одного из каналов.

В рамках данной лабораторной работы будет рассматриваться только первая задача.

EtherChannel — технология агрегирования каналов в Cisco.

Для агрегирования каналов в Cisco может быть использован один из трёх вариантов:

- LACP (Link Aggregation Control Protocol) – стандартный протокол;
- PAgP (Port Aggregation Protocol) – проприетарный протокол Cisco;
- Статическое агрегирование без использования протоколов.

Так как LACP и PAgP решают одни и те же задачи (с небольшими отличиями по возможностям), то лучше использовать стандартный протокол. Фактически остается выбор между LACP и статическим агрегированием.

Преимущества статического агрегирования:

- Не вносит дополнительную задержку при поднятии агрегированного канала или изменении его настроек;
- Вариант, который рекомендует использовать Cisco.

Недостатки статического агрегирования:

- Нет согласования настроек с удаленной стороной. Ошибки в настройке могут привести к образованию петель.

Преимущества агрегирования с помощью LACP:

- Согласование настроек с удаленной стороной позволяет избежать ошибок и петель в сети;
- Поддержка standby-интерфейсов позволяет агрегировать до 16-ти портов, 8 из которых будут активными, а остальные в режиме standby.

Недостатки агрегирования с помощью LACP:

- Вносит дополнительную задержку при поднятии агрегированного канала или изменении его настроек.

Рассмотрим схему, изображённую на рисунке 7.1.

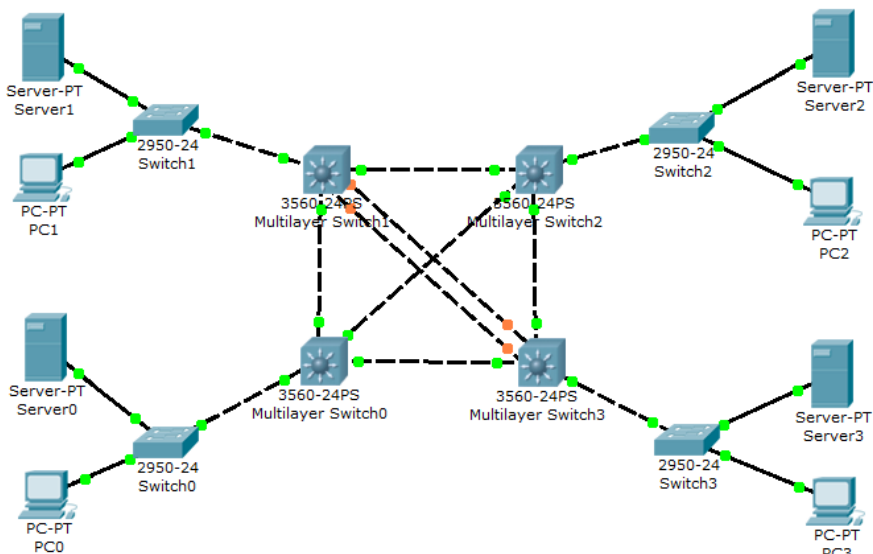


Рис. 7.1. Схема сети

На данной схеме рассмотрены следующие подсети:

1. Порт FastEthernet0/4 коммутатора Multilayer Switch0 и порты ПК PC0, сервера Server0 представляют собой подсеть NetA;
2. Порт FastEthernet0/4 коммутатора Multilayer Switch1 и порты ПК PC1, сервера Server1 представляют собой подсеть NetB;
3. Порт FastEthernet0/4 коммутатора Multilayer Switch2 и порты ПК PC2, сервера Server2 представляют собой подсеть NetC;
4. Порт FastEthernet0/4 маршрутизатора Multilayer Switch4 и порты ПК PC3, сервера Server3 представляют собой подсеть NetD;
5. Порты FastEthernet0/1, FastEthernet0/2, FastEthernet0/3 коммутатора Multilayer Switch0, порты FastEthernet0/1, FastEthernet0/2 коммутатора Multilayer Switch1, порты FastEthernet0/1, FastEthernet0/2, FastEthernet0/3 коммутатора Multilayer Switch2 и порты FastEthernet0/1, FastEthernet0/2 коммутатора Multilayer Switch3 представляют собой подсеть NetE;
6. Порты FastEthernet0/3, FastEthernet0/5 коммутаторов Multilayer Switch1, Multilayer Switch3 представляют собой подсеть NetF.

Для примера рассмотрим подсети NetA: 192.168.1.0/24, NetB: 192.168.2.0/24, NetC: 192.168.3.0/24, NetD: 192.168.4.0/24, NetE: 192.168.5.0/24, NetF: 192.168.6.0/30.

Подсеть NetF необходимо настроить по технологии EtherChannel. Остальные сети настраиваются, как в предыдущих лабораторных работах.

Чтобы настроить EtherChannel, необходимо сначала настроить каждый интерфейс в отдельности: перевести на третий уровень, добавить интерфейс в группу port channel командой **channel-group 1 mode active**, где 1 – номер группы

port channel, *active* – параметр протокола LACP. В результате создается новый логический интерфейс port channel 1, который необходимо перевести на третий уровень и присвоить ему IP адрес. Данная настройка производится на обоих коммутаторах.

Просмотреть информацию об EtherChannel можно при помощи команды ***show etherchannel summary***.

Задание к лабораторной работе:

1. Собрать схему, изображенную на рисунке 7.1;
2. Настроить устройства (по вариантам);
3. Настроить EtherChannel на подсети NetF;
4. Настроить маршрутизацию (по вариантам);
5. Настроить листы доступа (по вариантам);
6. Проверить возможности ***ping***, ***tracert***, работу листов доступа.

Варианты заданий:

1. *Подсети:* NetA – 192.168.11.0/24, NetB – 192.168.12.0/24, NetC – 192.168.13.0/24, NetD – 192.168.14.0/24, NetE – 192.168.15.0/24, NetF – 192.168.16.0/30;

Маршрутизация:

Трафик из NetA в NetC идет через каскад Multilayer Switch0 → Multilayer Switch1 → Multilayer Switch2;

Трафик из NetA в NetB идет через каскад Multilayer Switch0 → Multilayer Switch2 → Multilayer Switch1;

Остальной трафик маршрутизируется по кратчайшему пути.

Списки доступа:

Multilayer Switch0 может выгружать конфигурацию при помощи FTP на Server0, но не может – на Server1;

С PC3 возможен ping на PC0 и PC2, но не возможен – на Server0.

2. *Подсети:* NetA – 172.168.11.0/24, NetB – 172.168.12.0/24, NetC – 172.168.13.0/24, NetD – 172.168.14.0/24, NetE – 172.168.15.0/24, NetF – 172.168.16.0/30;

Маршрутизация:

Трафик из NetA в NetC идет через каскад Multilayer Switch0 → Multilayer Switch3 → Multilayer Switch2;

Трафик из NetA в NetB идет через каскад Multilayer Switch0 → Multilayer Switch3 → Multilayer Switch1;

Остальной трафик маршрутизируется по кратчайшему пути.

Списки доступа:

Multilayer Switch1 может выгружать конфигурацию при помощи FTP на Server1, но не может – на Server3;

С PC0 возможен ping на PC2 и Server1, но не возможен – на Server3.

3. *Подсети:* NetA – 172.20.21.0/24, NetB – 172.20.22.0/24, NetC – 172.20.23.0/24, NetD – 172.20.24.0/24, NetE – 172.20.25.0/24, NetF – 172.20.26.0/30;

Маршрутизация:

Трафик из NetB в NetD идет через каскад Multilayer Switch1 → Multilayer Switch0 → Multilayer Switch3;

Трафик из NetB в NetC идет через каскад Multilayer Switch1 → Multilayer Switch3 → Multilayer Switch2;

Остальной трафик маршрутизируется по кратчайшему пути.

Списки доступа:

Multilayer Switch2 может выгружать конфигурацию при помощи FTP на Server1, но не может – на Server0;

С PC1 возможен ping на PC3 и Server2, но не возможен – на Server3.

4. *Подсети:* NetA – 10.20.21.0/24, NetB – 10.20.22.0/24, NetC – 10.20.23.0/24, NetD – 10.20.24.0/24, NetE – 10.20.25.0/24, NetF – 10.20.26.0/30;

Маршрутизация:

Трафик из NetC в NetD идет через каскад Multilayer Switch2 → Multilayer Switch1 → Multilayer Switch3;

Трафик из NetC в NetA идет через каскад Multilayer Switch2 → Multilayer Switch1 → Multilayer Switch0;

Остальной трафик маршрутизируется по кратчайшему пути.

Списки доступа:

Multilayer Switch3 может выгружать конфигурацию при помощи FTP на Server3, но не может – на Server0;

С Server2 возможен ping на PC3 и Server0, но не возможен – на PC1.

5. *Подсети:* NetA – 10.10.11.0/24, NetB – 10.10.12.0/24, NetC – 10.10.13.0/24, NetD – 10.10.14.0/24, NetE – 10.10.15.0/24, NetF – 10.10.16.0/30;

Маршрутизация:

Трафик из NetD в NetB идет через каскад Multilayer Switch3 → Multilayer Switch2 → Multilayer Switch1;

Трафик из NetD в NetA идет через каскад Multilayer Switch3 → Multilayer Switch1 → Multilayer Switch0;

Остальной трафик маршрутизируется по кратчайшему пути.

Списки доступа:

Multilayer Switch0 может выгружать конфигурацию при помощи FTP на Server3, но не может – на Server1;

С Server3 возможен ping на PC0 и Server1, но не возможен – на PC2.

6. *Подсети:* NetA – 10.1.1.0/24, NetB – 10.1.2.0/24, NetC – 10.1.3.0/24, NetD – 10.1.4.0/24, NetE – 10.1.5.0/24, NetF – 10.1.6.0/30;

Маршрутизация:

Трафик из NetC в NetB идет через каскад Multilayer Switch3 → Multilayer Switch3 → Multilayer Switch1;

Трафик из NetB в NetD идет через каскад Multilayer Switch1 → Multilayer Switch0 → Multilayer Switch3;

Остальной трафик маршрутизируется по кратчайшему пути.

Списки доступа:

Multilayer Switch1 может выгружать конфигурацию при помощи FTP на Server1, но не может – на Server0;

С Server3 возможен ping на PC1 и Server2, но не возможен – на PC2.

Контрольные вопросы:

1. Понятие агрегирования каналов.
2. Какие варианты агрегирования используются в EtherChannel?
3. Преимущества и недостатки статического агрегирования.
4. Преимущества и недостатки LACP.

ДЛЯ ЗАМЕТОК

