

## Лабораторная работа №1. Режим симуляции в Cisco Packet Tracer.

Состав сети: 4 узла, сервер, принтер и два концентратора. Концентраторы между собой соединяются кроссоверным кабелем (рис.2.1).

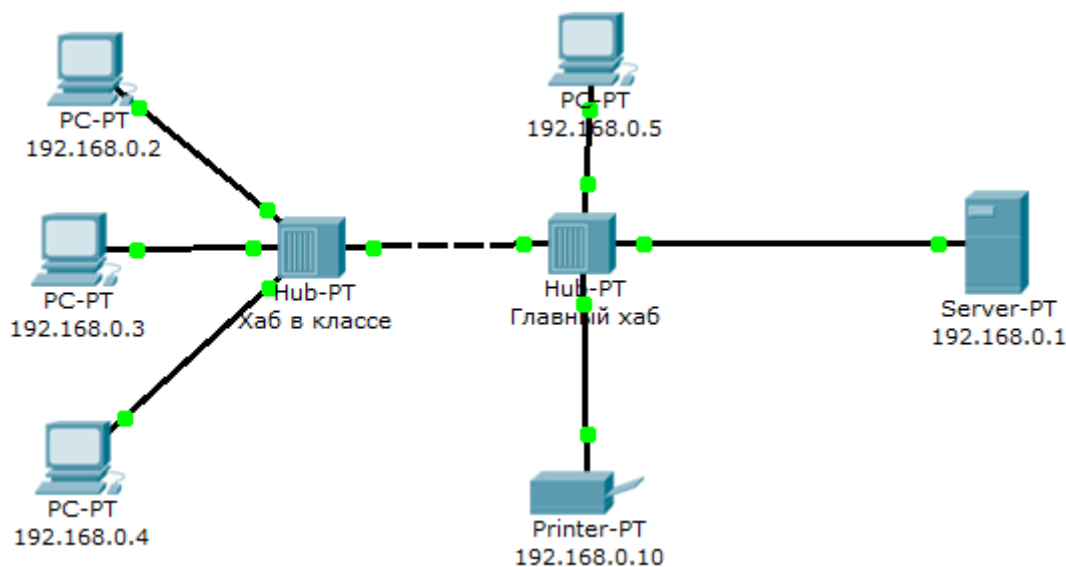


Рис.2.1. Схема сети.

Нужно перейти в режим симуляции (Shift+S), либо кликнув на иконку симуляции в правом нижнем углу рабочего пространства. Здесь мы видим окно событий, кнопка сброса (очищает список событий), управление воспроизведением и фильтр протоколов. Предложено много протоколов, но отфильтруем пока только ICMP, это исключит случайный трафик между узлами.

Для перехода к следующему событию используем кнопку "Вперёд", либо автоматика (рис.2.2).

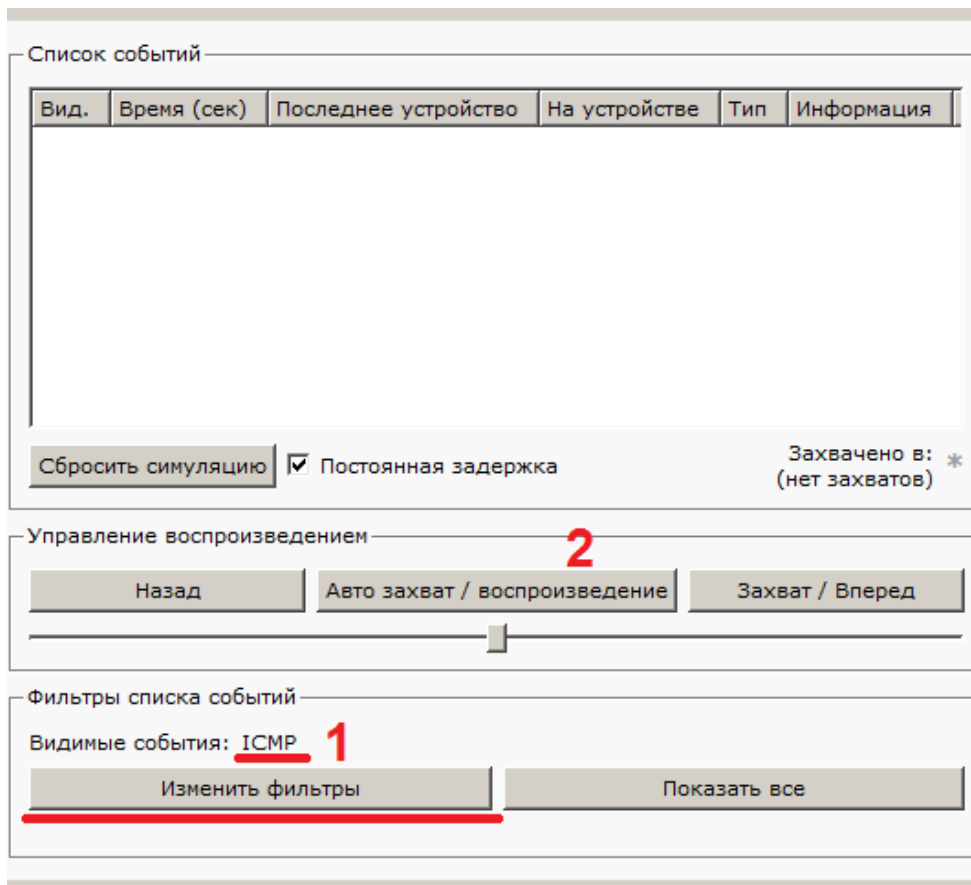


Рис.2.2. Интерфейс симулятора.

Посылаем PING-запрос.

С одного из узлов попробуем пропинговать другой узел. Выбираем далеко расположенные узлы, чтобы наглядней увидеть как будут проходить пакеты по сети в режиме симуляции. Итак, входим на узел .4 и пошлём пинг-запрос на узел .5.

С розового узла пингуем зелёный. На розовом узле образовался пакет (конвертик), который ждёт (иконка паузы на нём). Запустить пакет в сеть можно нажав кнопку "Вперёд" в окне симуляции (рис.2.3).

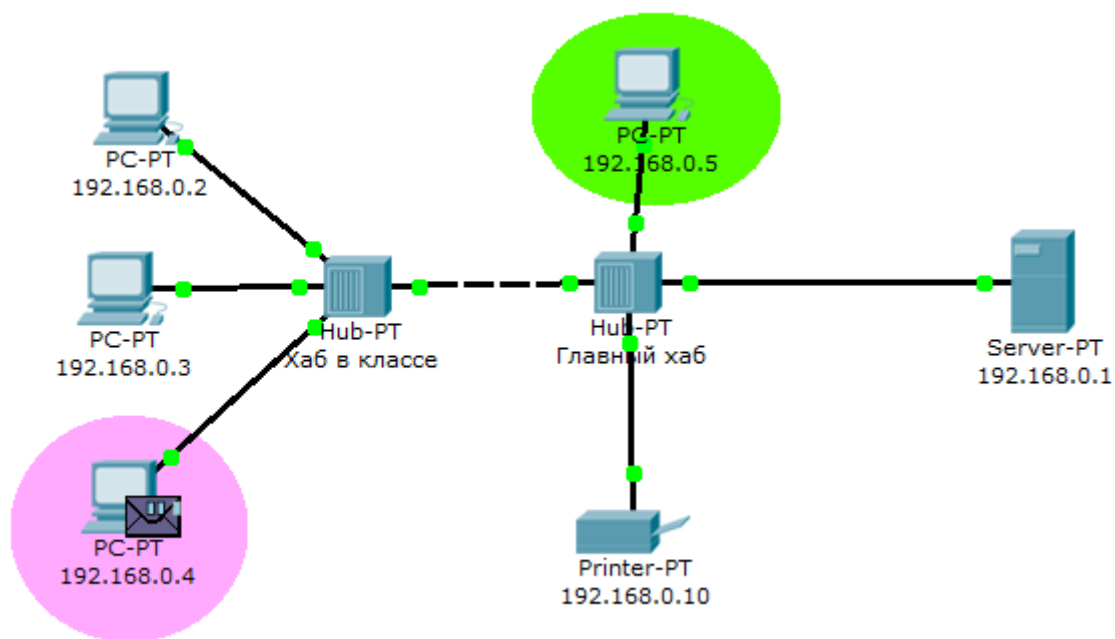


Рис.2.3. Демонстрация работы симулятора.

Так же в окне симуляции мы увидим этот пакет, отметив его тип (ICMP) и источник (192.168.0.4) – рис.2.4.

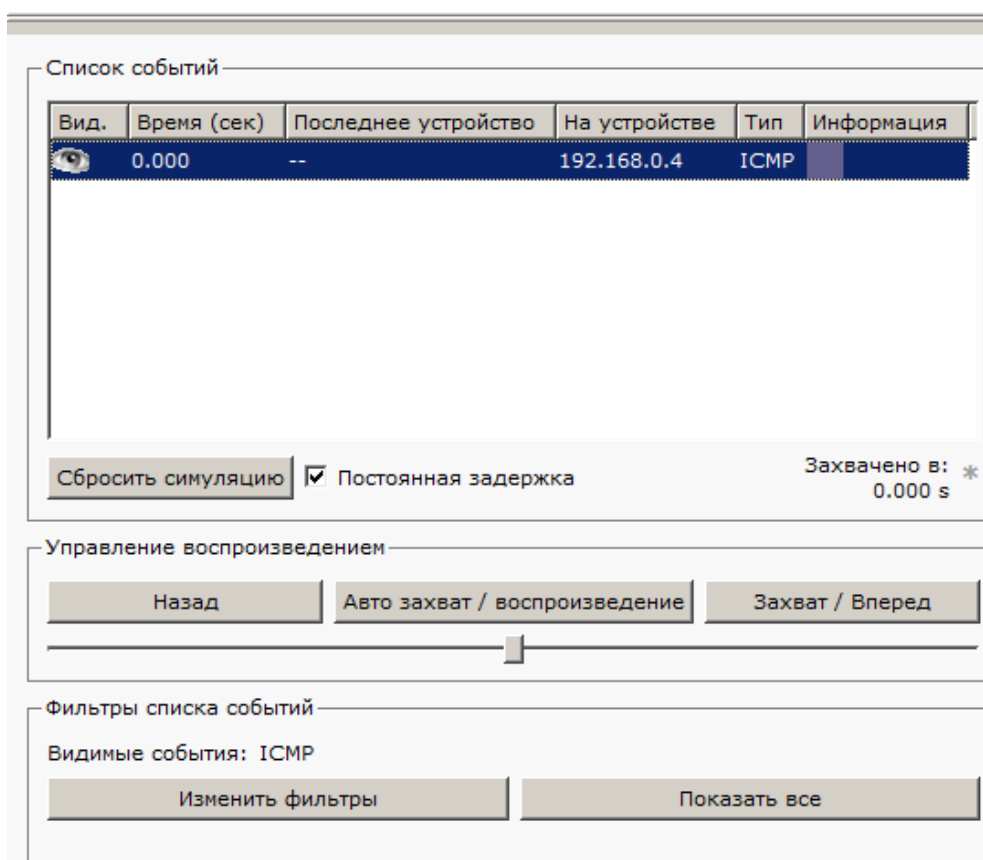


Рис.2.4. Мониторинг работы протоколов.

Клик на пакете покажет нам подробную информацию. При этом мы увидим модель OSI. Сразу видно, что на 3-ем уровне (сетевой) возник пакет на исходящем направлении, который пойдёт до второго уровня, затем до первого, на физическую среду и передастся на следующий узел (рис.2.5).

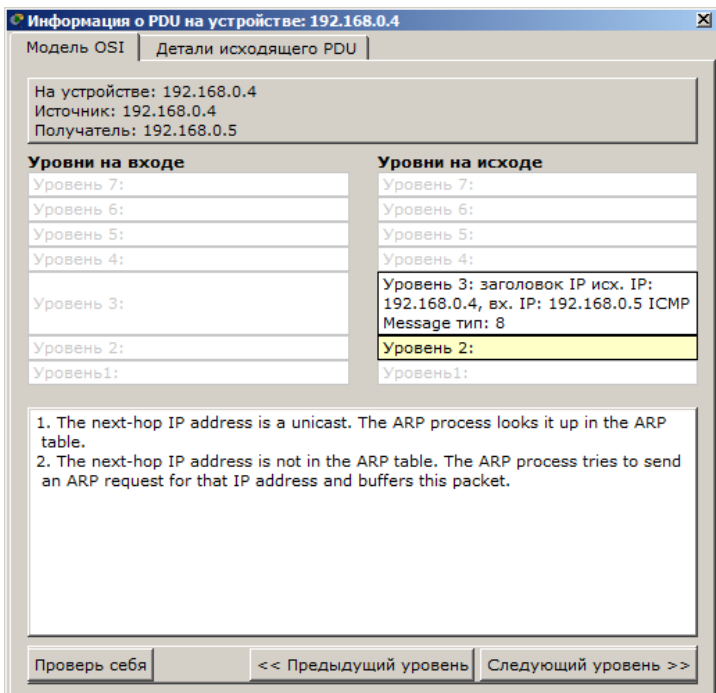


Рис.2.5. Мониторинг работы на модели OSI.

А на другой вкладке можно посмотреть структуру пакета (рис.2.6).

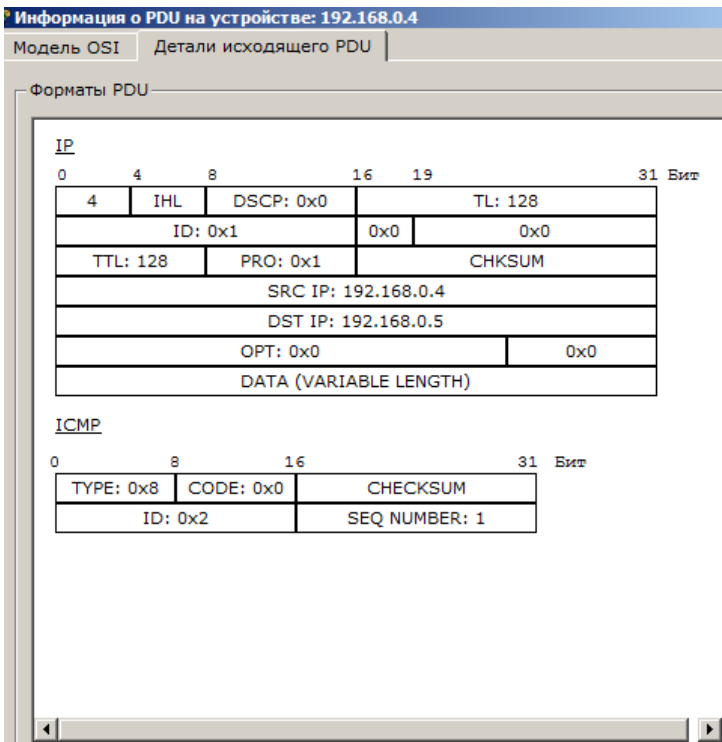


Рис.2.6. Структура пакета.

Нажмём кнопку "Вперёд". И пакет тут же двинется к концентратору. Это единственное сетевое подключение с этой стороны (2.7).

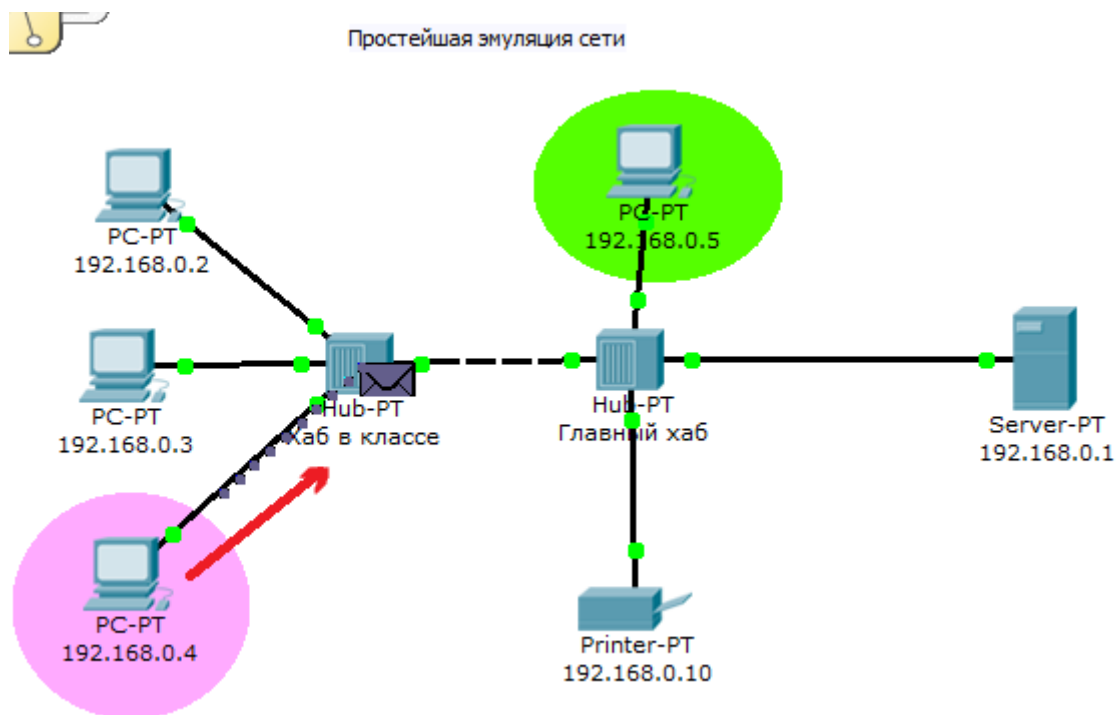


Рис.2.7. Прохождение пакета. Первый этап.

Концентратор повторяет пакет на всех остальных портах в надежде, что на одном из них есть адресат (рис.2.8)

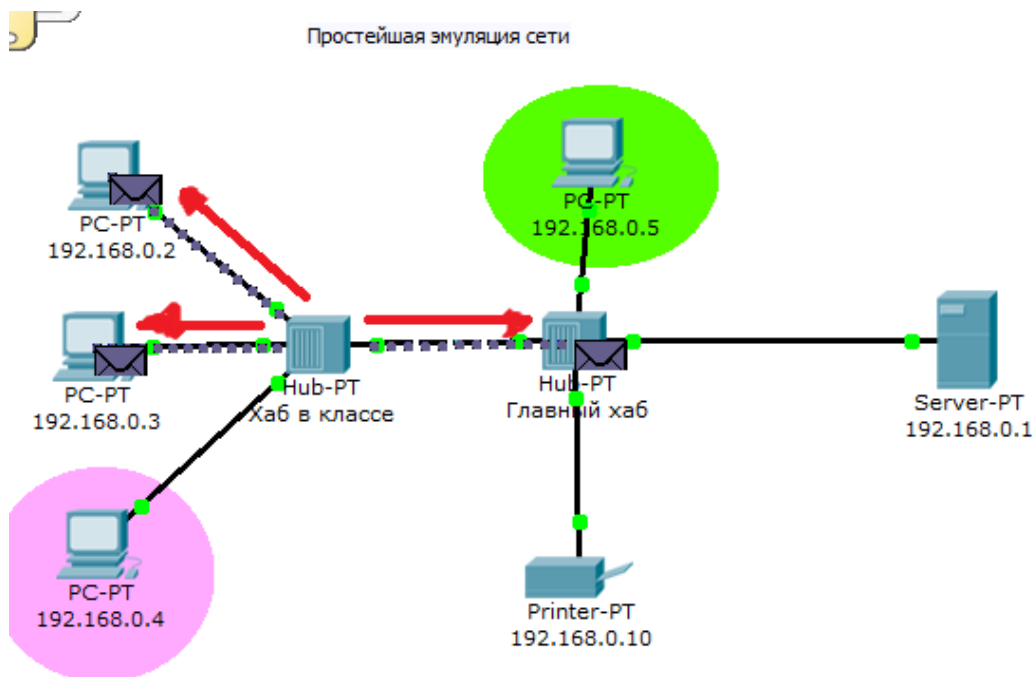


Рис.2.8. Прохождение пакета. Второй этап.

Если пакеты каким то узлам не предназначенные, они просто игнорируют их (рис.2.9).

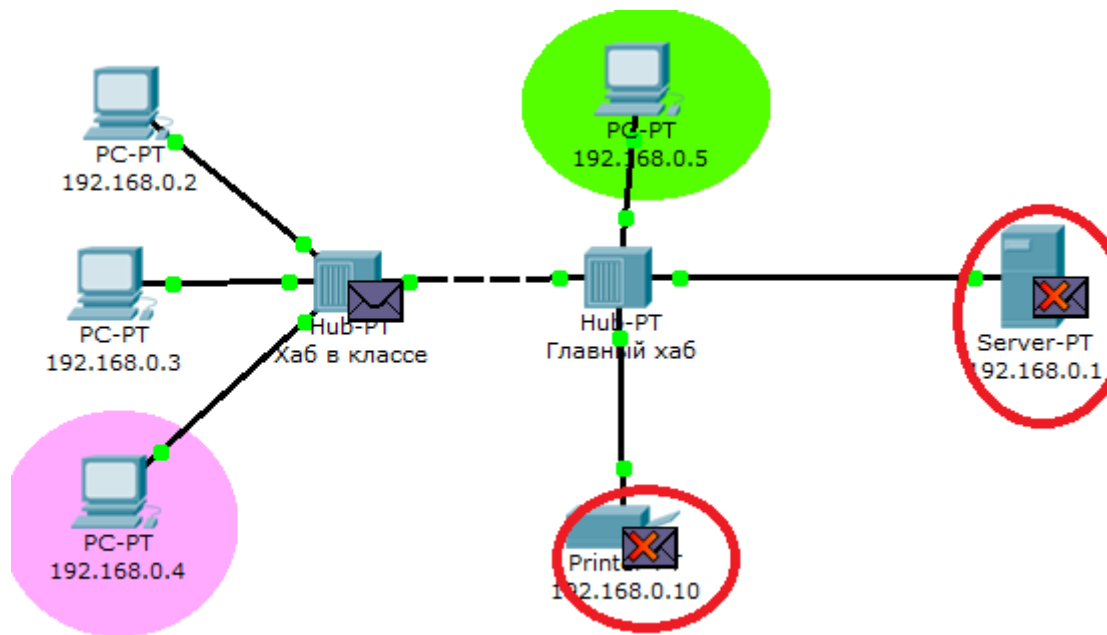


Рис.2.9. Прохождение пакета. Третий этап.

Когда пакет вернётся обратно, то увидим подтверждение соединения.

Контрольные вопросы.

1. Для чего используется режим симуляции?
2. Как просмотреть прохождение пакета по уровням модели OSI?
3. Можно ли определить причину того, что посланный в режиме симуляции пакет не дошел до адресата и на каком этапе произошел сбой работы сети?
4. Укажите в составе пакета IP адреса отправителя и получателя.
5. Как изменить фильтры списка событий?
6. Как в режиме симуляции определить, какие протоколы были задействованы в работе сети?
7. Как в режиме симуляции проследить изменение содержимого пакета при прохождении его по сети?
8. Перечислите основные возможности режима симуляции.

**Лабораторная работа №2. Настройка сетевых сервисов.**

Создайте следующую схему сети, представленную на рис. 3.1:

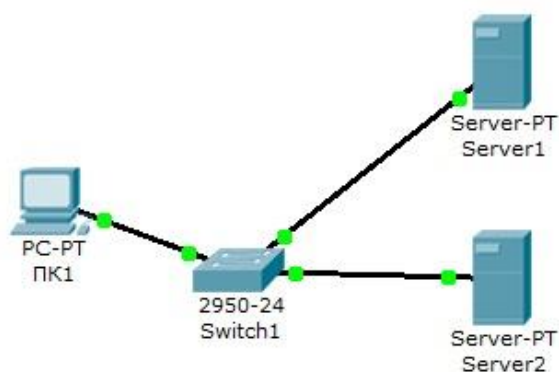


Рис.3.1. Схема сети.

Задача:

Настроить сеть следующим образом:

- 1 - Server1 – DNS и Web сервер;
- 2 - Server2 – DHCP сервер;
- 3 - Компьютер ПК1 получает параметры протокола TCP/IP с DHCP сервера и открывает сайт [www.rambler.ru](http://www.rambler.ru) на Server1.

Этап 1.

Задайте параметры протокола TCP/IP на ПК1 и серверах.

Войдите в конфигурацию ПК1 и установите настройку IP через DHCP сервер рис.3.2.

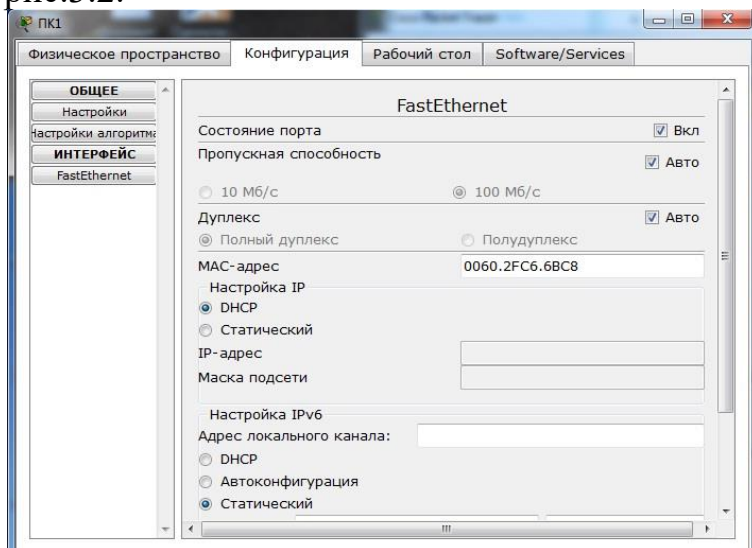


Рис. 3.2. Настройка IP на ПК1.

Задайте в конфигурации серверов следующие настройки IP:

Server1: IP адрес – 10.0.0.1, маска подсети – 255.0.0.0

Server2: IP адрес – 10.0.0.2, маска подсети – 255.0.0.0

## Этап 2. Настройте службу DNS на Server1.

Для этого в конфигурации Server1 войдите на вкладку DNS и задайте две ресурсные записи в прямой зоне DNS:

1 – в ресурсной записи типа A свяжите доменное имя компьютера с его IP адресом рис.3.3 и нажмите кнопку ДОБАВИТЬ:

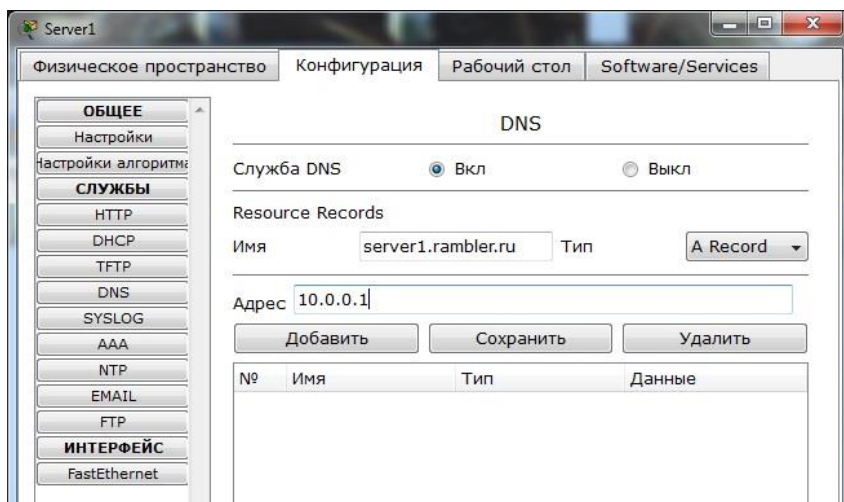


Рис.3.3. Ввод ресурсной записи типа A.

2 – в ресурсной записи типа CNAME свяжите псевдоним сайта с компьютером (рис.3.4):

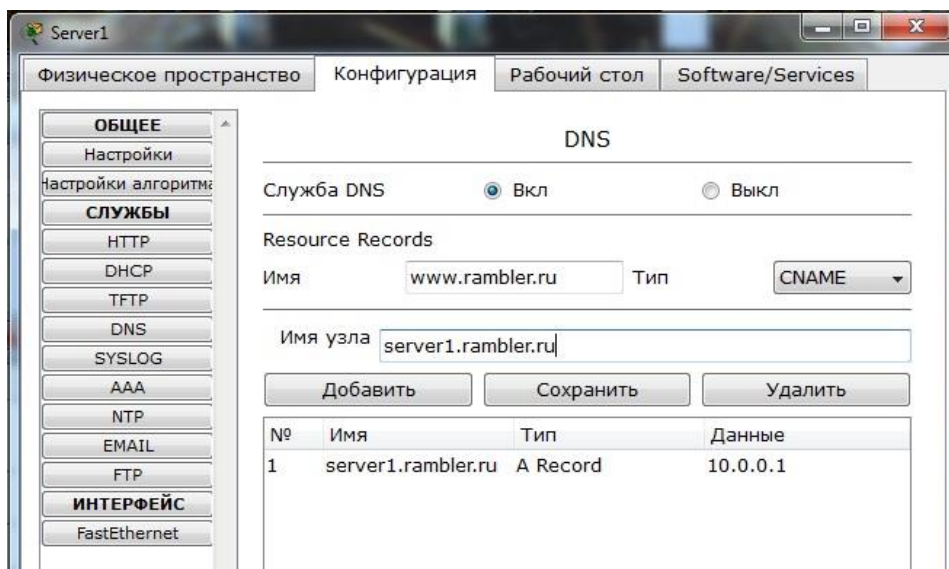


Рис.3.4. Ввод ресурсной записи типа CNAME.

В конфигурации Server1 войдите на вкладку HTTP и задайте стартовую страницу сайта WWW.RAMBLER.RU (рис.3.5):



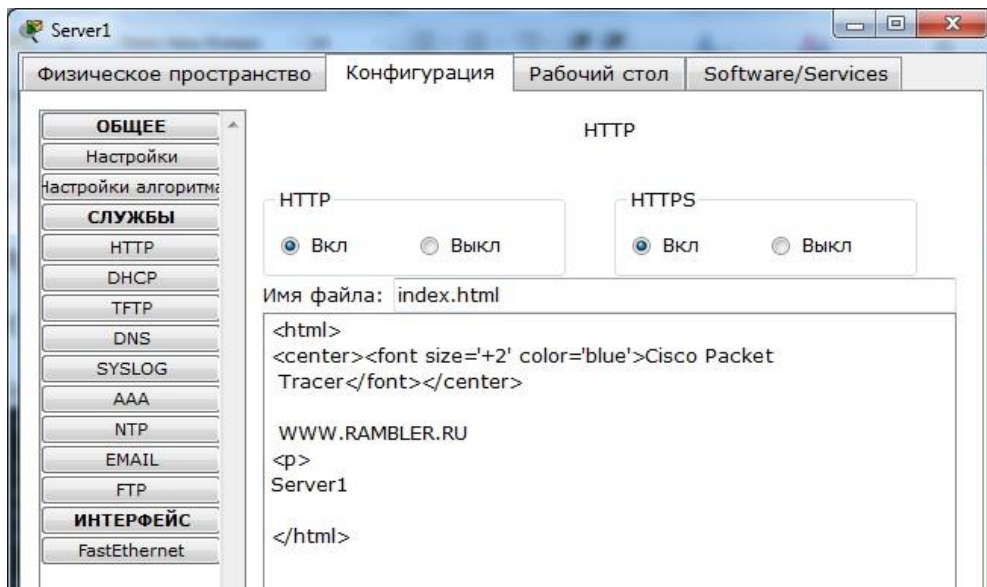


Рис.3.5. Стартовая страница сайта.

Включите командную строку на Server1 и проверьте работу службы DNS. Для проверки прямой зоны DNS сервера введите команду

**SERVER>nslookup www Rambler.ru**

Если все правильно, то вы получите отклик, представленный на рис.3.6, с указанием полного доменного имени DNS сервера в сети и его IP адрес.

```
SERVER>nslookup www Rambler.ru

Server: [10.0.0.1]
Address: 10.0.0.1

Non-authoritative answer:
Name:   server1.Rambler.ru
Address: 10.0.0.1

Aliases:   server1.Rambler.ru

SERVER>
```

Рис. 3.6. Проверка прямой зоны DNS.

Этап 3. Настройте DHCP службу на Server2.

Для этого войдите в конфигурацию Server2 и на вкладке DHCP настройте службу (рис.3.7):

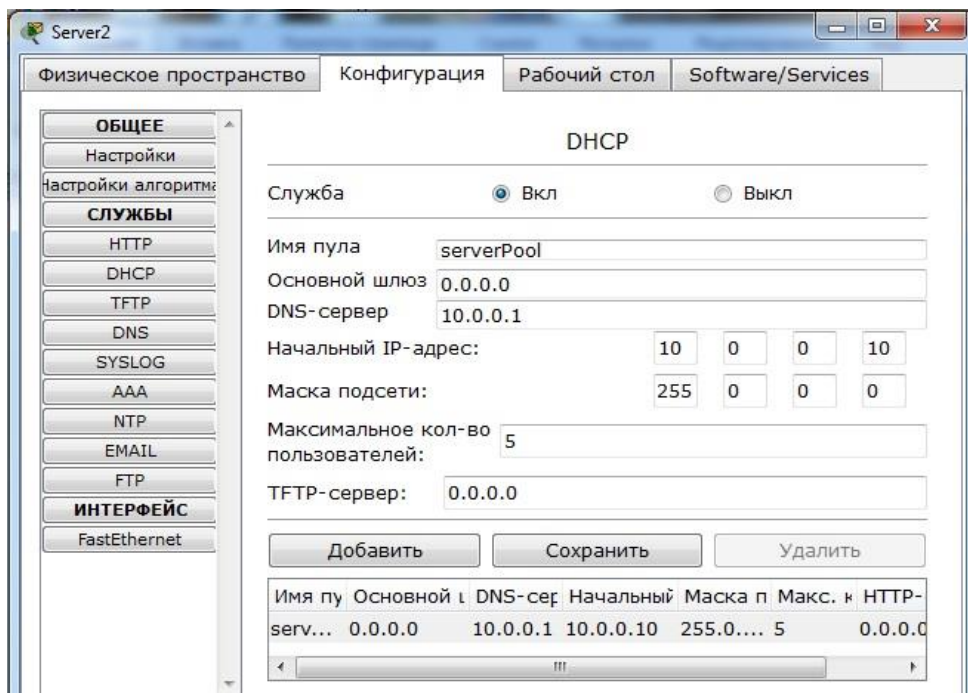


Рис. 3.7. Настройка DHCP сервера.

Этап 3. Проверка работы клиента.

Войдите в конфигурации хоста ПК1 на рабочий стол и в командной строке сконфигурируйте протокол TCP/IP.

Командой

**PC>ipconfig /release**

сбросьте старые параметры IP адреса, а командой:

**PC>ipconfig /renew**

получите новые параметры с DHCP сервера (рис.3.8):

```
PC>ipconfig /release

IP Address. . . . .: 0.0.0.0
Subnet Mask. . . . .: 0.0.0.0
Default Gateway. . . . .: 0.0.0.0
DNS Server. . . . .: 0.0.0.0

PC>ipconfig /renew

IP Address. . . . .: 10.0.0.10
Subnet Mask. . . . .: 255.0.0.0
Default Gateway. . . . .: 0.0.0.0
DNS Server. . . . .: 10.0.0.1

PC>
```

Рис.3.8. Конфигурация протокол TCP/IP клиента.

Откройте сайт WWW.RAMBLER.RU в браузере на клиенте (рис.3.9):

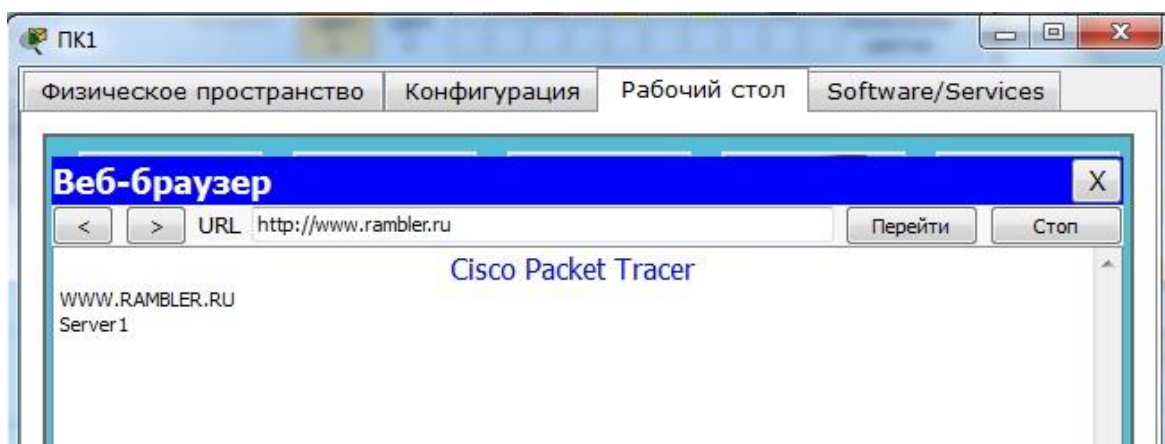


Рис.3.9. Проверка работы клиента.

Контрольные вопросы.

1. Что такое рекурсивный запрос DNS и какова схема его работы?
2. Укажите назначение типов ресурсных записей в прямой и обратной зонах DNS.
3. Как на DNS сервере настраивается пересылка пакетов на другие DNS сервера?
4. Опишите работу службы DHCP.
5. Как настраивается клиент DHCP?
6. Укажите местоположения папки с контентом Web-узла и FTP сервера.
7. Как определяется состав обратных зон DNS сервера в корпоративной сети?

**Лабораторная работа №3. Знакомство с командами IOS.**

## Основные команды сетевого устройства

1. Войдите в сетевое устройство Router1

```
Router>
```

2. Мы хотим увидеть список всех доступных команд в этом режиме. Введите команду, которая используется для просмотра всех доступных команд:

```
Router>?
```

Клавишу Enter нажимать не надо.

3. Теперь войдите в привилегированный режим

```
Router>enable
```

```
Router#
```

4. Просмотрите список доступных команд в привилегированном режиме

```
Router#?
```

5. Перейдём в режим конфигурации

```
Router#config terminal
```

```
Router(config)#
```

6. Имя хоста сетевого устройства используется для локальной идентификации. Когда вы входите в сетевое устройство, вы видите Имя хоста перед символом режима (">" или "#"). Это имя может быть использовано для определения места нахождения.

Установите "Router1" как имя вашего сетевого устройства.

```
Router(config)#hostname Router1
```

```
Router1(config)#
```

7. Пароль доступа позволяет вам контролировать доступ в привилегированный режим. Это очень важный пароль, потому что в привилегированном режиме можно вносить конфигурационные изменения. Установите пароль доступа "parol".

```
Router1(config)#enable password parol
```

1. Давайте испытаем этот пароль. Выйдите из сетевого устройства и попытайтесь зайти в привилегированный режим.

2.

```
Router1>en
```

```
Password:*****  
Router1#
```

Здесь знаки: \*\*\*\*\* - это ваш ввод пароля. Эти знаки на экране не видны.

## Основные Show команды.

Перейдите в пользовательский режим командой `disable`. Введите команду для просмотра всех доступных show команд.

```
Router1>show ?
```

1. Команда `show version` используется для получения типа платформы сетевого устройства, версии операционной системы, имени файла образа операционной системы, время работы системы, объём памяти, количество интерфейсов и конфигурационный регистр.

2. Просмотр времени:

```
Router1>show clock
```

3. Во флеш-памяти сетевого устройства сохраняется файл-образ операционной системы Cisco IOS. В отличие от оперативной памяти, в реальных устройствах флеш память сохраняет файл-образ даже при сбое питания.

```
Router1>show flash
```

4. ИКС сетевого устройства по умолчанию сохраняет 10 последних введенных команд

```
Router1>show history
```

5. Две команды позволят вам вернуться к командам, введенным ранее. Нажмите на стрелку вверх или `<ctrl> P`.

6. Две команды позволят вам перейти к следующей команде, сохранённой в буфере.

Нажмите на стрелку вниз или `<ctrl> N`

7. Можно увидеть список хостов и IP-Адреса всех их интерфейсов

```
Router1>show hosts
```

8. Следующая команда выведет детальную информацию о каждом интерфейсе

```
Router1>show interfaces
```

9. Следующая команда выведет информацию о каждой telnet сессии:

```
Router1>show sessions
```

10. Следующая команда показывает конфигурационные параметры терминала:

```
Router1>show terminal
```

11. Можно увидеть список всех пользователей, подсоединённых к устройству по терминальным линиям:

```
Router1>show users
```

12. Команда

```
Router1>show controllers
```

показывает состояние контроллеров интерфейсов.

13. Перейдём в привилегированный режим.

```
Router1>en
```

14. Введите команду для просмотра всех доступных show команд.

```
Router1#show ?
```

Привилегированный режим включает в себя все show команды пользовательского режима и ряд новых.

15. Посмотрим активную конфигурацию в памяти сетевого устройства. Необходим привилегированный режим. Активная конфигурация автоматически не сохраняется и будет потеряна в случае сбоя электропитания. Чтобы сохранить настройки роутера используйте следующие команды:

сохранение текущей конфигурации:

```
Router# write memory
```

Или

```
Router# copy run start
```

Просмотр сохраненной конфигурации:

```
Router# Show configuration
```

или

```
Router1#show running-config
```

В строке `more`, нажмите на клавишу пробел для просмотра следующей страницы информации.

16. Следующая команда позволит вам увидеть текущее состояние протоколов третьего уровня:

```
Router#show protocols
```

### **Введение в конфигурацию интерфейсов.**

Рассмотрим команды настройки интерфейсов сетевого устройства.

На сетевом устройстве Router1 войдём в режим конфигурации:

```
Router1#conf t  
Router1( config) #
```

2. Теперь мы хотим настроить Ethernet интерфейс. Для этого мы должны зайти в режим конфигурации интерфейса:

```
Router1( config) #interface FastEthernet0/0  
Router1( config-if) #
```

3. Посмотрим все доступные в этом режиме команды:

```
Router1( config-if) #?
```

Для выхода в режим глобальной конфигурации наберите `exit`. Снова войдите в режим конфигурации интерфейса:

```
Router1( config) #int fa0/0
```

Мы использовали сокращенное имя интерфейса.

4. Для каждой команды мы можем выполнить противоположную команду, поставив перед ней слово `no`. Следующая команда включает этот интерфейс:

```
Router1( config-if) #no shutdown
```

5. Добавим к интерфейсу описание:

```
Router1( config-if) #description Ethernet interface on Router 1
```

Чтобы увидеть описание этого интерфейса, перейдите в привилегированный режим и выполните команду `show interface` :

```
Router1 (config-if) #end  
Router1#show interface
```

6. Теперь присоединитесь к сетевому устройству Router 2 и поменяйте имя его хоста на Router2:

```
Router#conf t  
Router (config) #hostname Router2
```

Войдём на интерфейс FastEthernet 0/0:

```
Router2 (config) #interface fa0/0
```

Включите интерфейс:

```
Router2 (config-if) #no shutdown
```

Теперь, когда интерфейсы на двух концах нашего Ethernet соединения включены на экране появится сообщение о смене состояния интерфейса на активное.

7. Перейдём к конфигурации последовательных интерфейсов. Зайдём на Router1.

Проверим, каким устройством выступает наш маршрутизатор для последовательной линии связи: окончательным устройством DTE (data terminal equipment), либо устройством связи DCE (data circuit):

```
Router1#show controllers fa0/1
```

Если видим сообщение:

```
DCE cable
```

то наш маршрутизатор является устройством связи и он должен задавать частоту синхронизации тактовых импульсов, используемых при передаче данных. Частота берётся из определённого ряда частот.

```
Router1#conf t  
Router1 (config) #int fa0/1  
Router1 (config-if) #clock rate ?
```

Выберем частоту 64000

```
Router1 (config-if) #clock rate 64000
```



и включаем интерфейс

```
Router1 (config-if) #no shut
```

Контрольные вопросы.

1. Какой командой можно посмотреть текущие настройки роутера?
2. Какими командами настраивается сетевой интерфейс роутера.
3. Как просмотреть конфигурационные настройки коммутатора?
4. Как определить распределение VLN по портам коммутатора?
5. Перечислите основные режимы конфигурации при настройке коммутатора.
6. Перечислите основные режимы конфигурации при настройке роутера.
7. Как посмотреть таблицу маршрутизации на роутере?
8. Какие команды формируют таблицу маршрутизации роутера?
9. Какими командами настраиваются VLN на коммутаторе?
10. Какими командами настраивается взаимодействие между VLN?

#### **Лабораторная работа №4. Настройка протокола RIP.**

Создайте схему, представленную на рис.4.1.

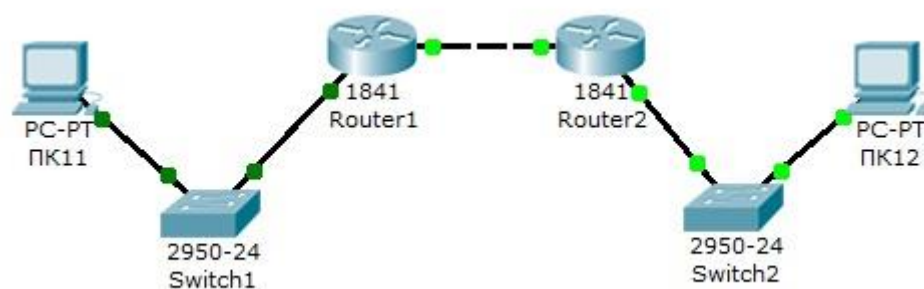


Рис.4.1. Схема сети.

На схеме представлены следующие три сети:

Switch1 – сеть 10.11.0.0/16.

Switch2 – сеть 10.12.0.0/16.

Сеть для роутеров - 10.10.0.0/16.

Введите на устройствах следующую адресацию:

Маршрутизаторы имеют по два интерфейса:

Router1 – 10.11.0.1/16 и 10.10.0.1/16.

Router2 – 10.10.0.2/16 и 10.12.0.1/16.

ПК11 - 10.11.0.11/16 .

ПК12 - 10.12.0.12/16 .

Проведем настройку протокола RIP на маршрутизаторе Router1.

Войдите в конфигурации в консоль роутера и выполните следующие настройки (при вводе команд маску подсети можно не указывать, т.к. она будет браться автоматически из настроек интерфейса роутера):

Войдите в привилегированный режим:

Router1>**enable**

Войдите в режим конфигурации:

Router1>**#conf t**

Войдите в режим конфигурирования протокола RIP:

Router1 (config) **#router rip**

Подключите клиентскую сеть к роутеру:

Router1 (config-router) **#network 10.11.0.0**

Подключите вторую сеть к роутеру:

Router1 (config-router) **#network 10.10.0.0**

Задайте использование второй версии протокол RIP:

Router1 (config-router) **#version 2**

Выйдите из режима конфигурирования протокола RIP:

Router1 (config-router) **#exit**

Выйдите из консоли настроек:

Router1 (config) **#exit**

Сохраните настройки в память маршрутизатора:

Router1>**#write memory**

Аналогично проведите настройку протокола RIP на маршрутизаторе Router2.

Проверьте связь между компьютерами ПК11 и ПК12 командой **ping**.

Если связь есть – все настройки сделаны верно.

## **Лабораторная работа № 5. Многопользовательский режим работы.**

В данной работе будет продемонстрировано создание объединенной сети на основе двух разных сетей, созданных в двух отдельно запущенных сессиях программы Cisco Packet Tracer на одном компьютере.

Вы создадите две одновременно работающие сессии программы Cisco Packet Tracer, дважды запустив ее на выполнение.

В первой открытой сессии программы будет создана и настроены две сети: сеть 1 - 11.0.0.0 и сеть 2 - 12.0.0.0. Во второй сессии программы – сеть 11.0.0.0.

### Работа в сессии 1.

Запустите программу Cisco Packet Tracer (первая сессия) и создайте две сети (сеть 11.0.0.0 и 12.0.0.0) по схеме, представленной на рис.5.1:

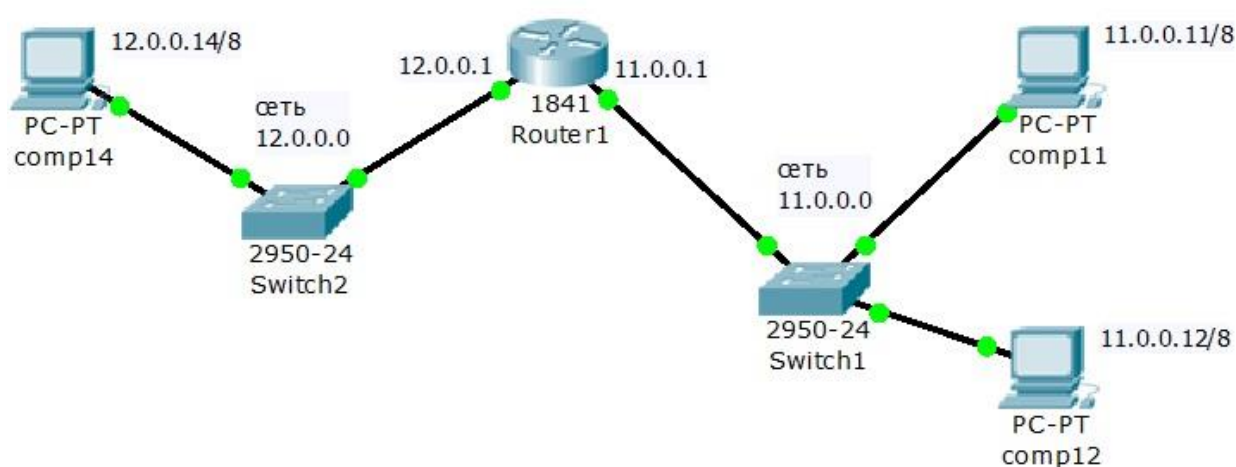


Рис.5.1. Первая сессия – сети 11.0.0.0 и 12.0.0.0.

Задайте названия устройств, как показано на схеме.

Задайте параметры протокола TCP/IP и шлюзы для компьютеров comp11, comp12 и comp14, как показано на схеме (рис.5.1).

### Работа в сессии 2.

Не выключая текущую сессию работающей программы, создайте вторую сессию работы программы, запустив повторно Cisco Packet Tracer и создайте сеть по схеме, представленной на рис.5.2:

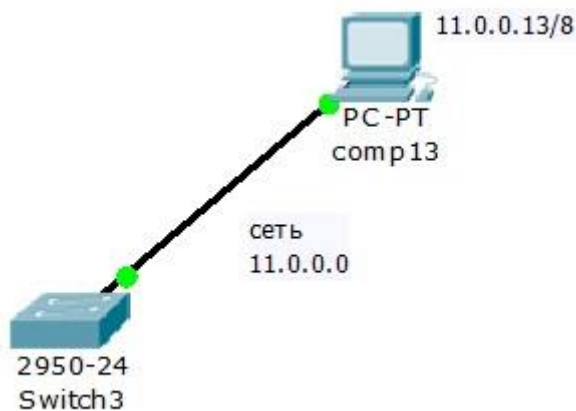


Рис.5.2. Вторая сессия – сеть 11.0.0.0.

Задайте названия устройств и параметры протокола TCP/IP для компьютера comp13, как показано на схеме (рис.5.2).

В результате вы получите работающие сети в разных сессиях программы Cisco Packet Tracer (рис.5.3):

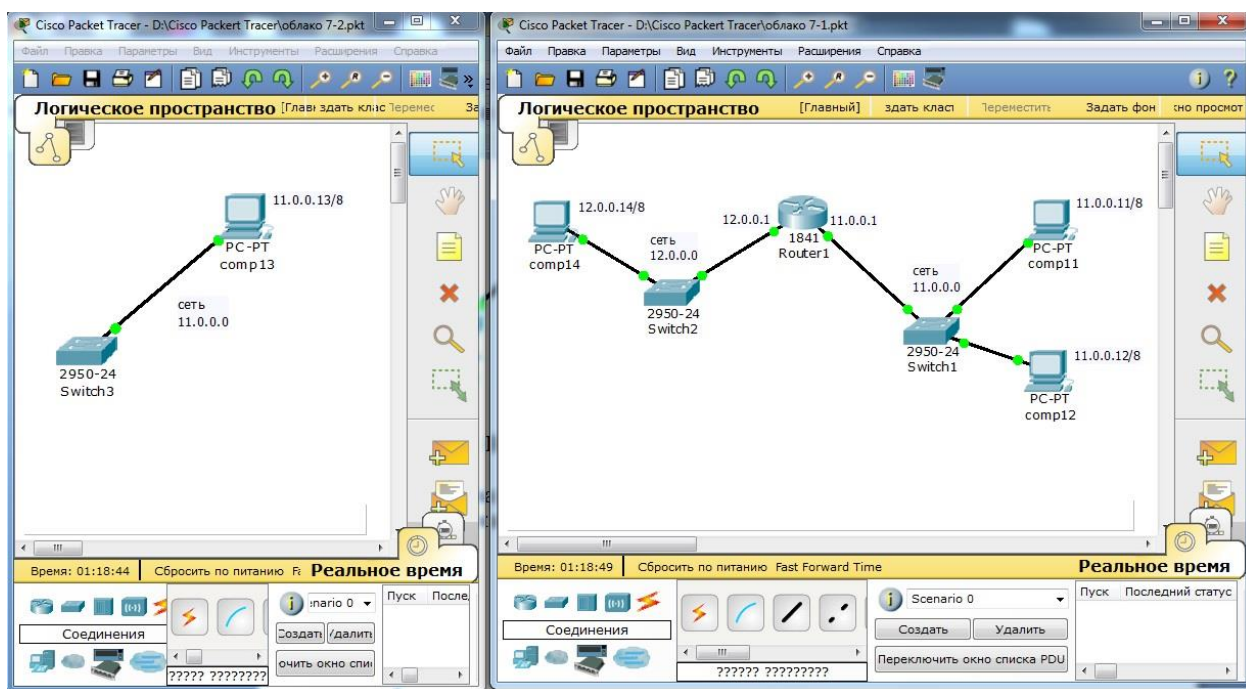


Рис.5.3. Исходные настройки.

### Создание многопользовательского соединения.

Для создания многопользовательского соединения необходимо соединить сети, созданных в разных сессиях запущенной программы Cisco Packet Tracer. Для этого выбирается общая сеть (сеть 11.0.0.0), через которую будет проходить соединение и указываются порты соединения: для одной сети

– входящий порт, а для другой – выходящий порт. Объединение сетей в разных сессиях проведем через коммутаторы Switch1 (первая сессия) и Switch3 (вторая сессия).

Для создания многопользовательского соединения необходимо провести следующие этапы настройки:

Этап 1 – подключение к многопользовательскому облаку.

Этап 2 – открытие портов на устройствах, через которые проводится подключение (Switch1 и Switch3).

Этап 3 – создание общего канала связи многопользовательского подключения.

Этап 1 – подключение к многопользовательскому облаку.

Откройте первую сессию. Создайте многопользовательское подключение. Для этого в инструментах выберите группу «пользовательское соединение» и внесите на схему сети устройство «Multiuser» (рис.9.4):

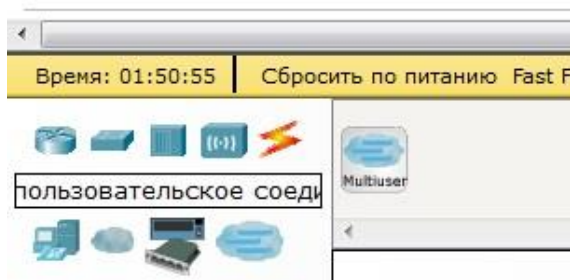


Рис.5.4. Создание многопользовательского подключения.

Соедините коммутатор Switch1 с новым устройством (рис. 5.5). Для этого в группе «Соединения» выберите тип кабеля «Медный кроссовер» и соедините четвертый порт коммутатора FastEthernet0/4 с облаком многопользовательского соединения. При этом задействуйте функцию «Создать новый канал».

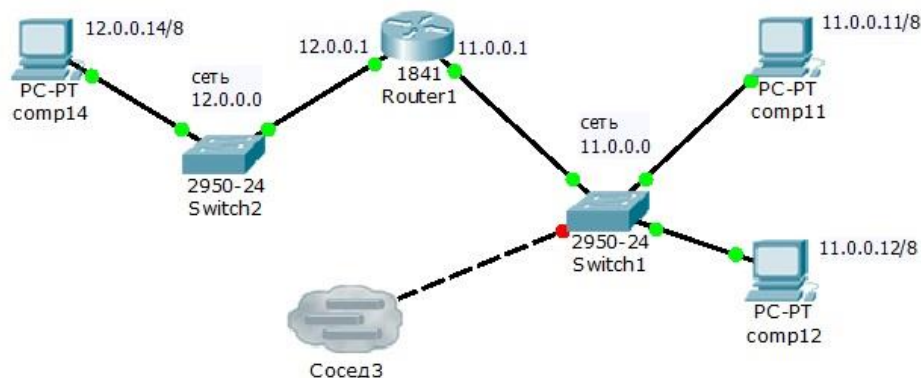


Рис.5.5. Подключение коммутатора к многопользовательскому каналу.

Этап 2 – открытие портов на устройствах, через которые проводится подключение.

Теперь для объединения сетей в разных сессиях необходимо открыть порты на коммутаторах. Пусть это будет четвертый порт на Switch1 и Switch3.

Для этого в каждой сессии в главном меню выберите «Расширения» – «Многопользовательский режим» - «Видимость порта» (рис. 5.6).

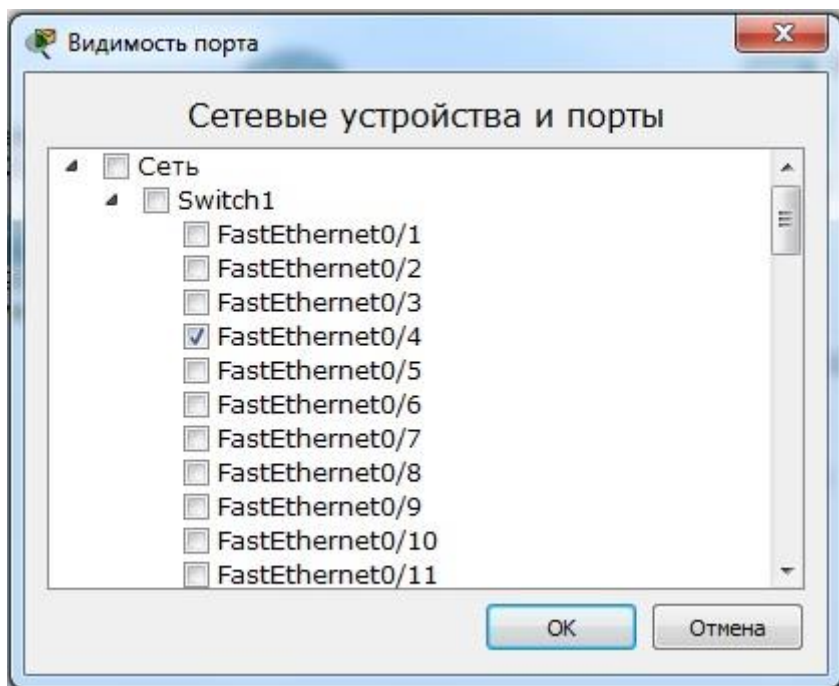


Рис. 5.6. Включение четвертого порта коммутатора.

Этап 3 – создание общего канала доступа многопользовательского подключения.

Необходимо выбрать реально работающую сеть для создания общего канала доступа. Возможны два варианта:

вариант 1 – вы делаете многопользовательское соединение на разных компьютерах;

вариант 2 - вы делаете многопользовательское соединение на одном компьютере в разных сессиях программы

В первом случае подключение ведется через реальный IP адрес компьютера в локальной сети.

Во втором случае возможны два варианта подключения:

- через Localhost по адресу 127.0.0.1;

- через реальный IP адрес компьютера в локальной сети.

Переключитесь во вторую сессию.

Для этого в главном меню выберите «Расширения» – «Многопользовательский режим» - «Прослушивание» (рис. 9.7). Уберите пароль и в разделах «Существующие удаленные сети» и «Новые удаленные сети» включите режим «Напоминание».

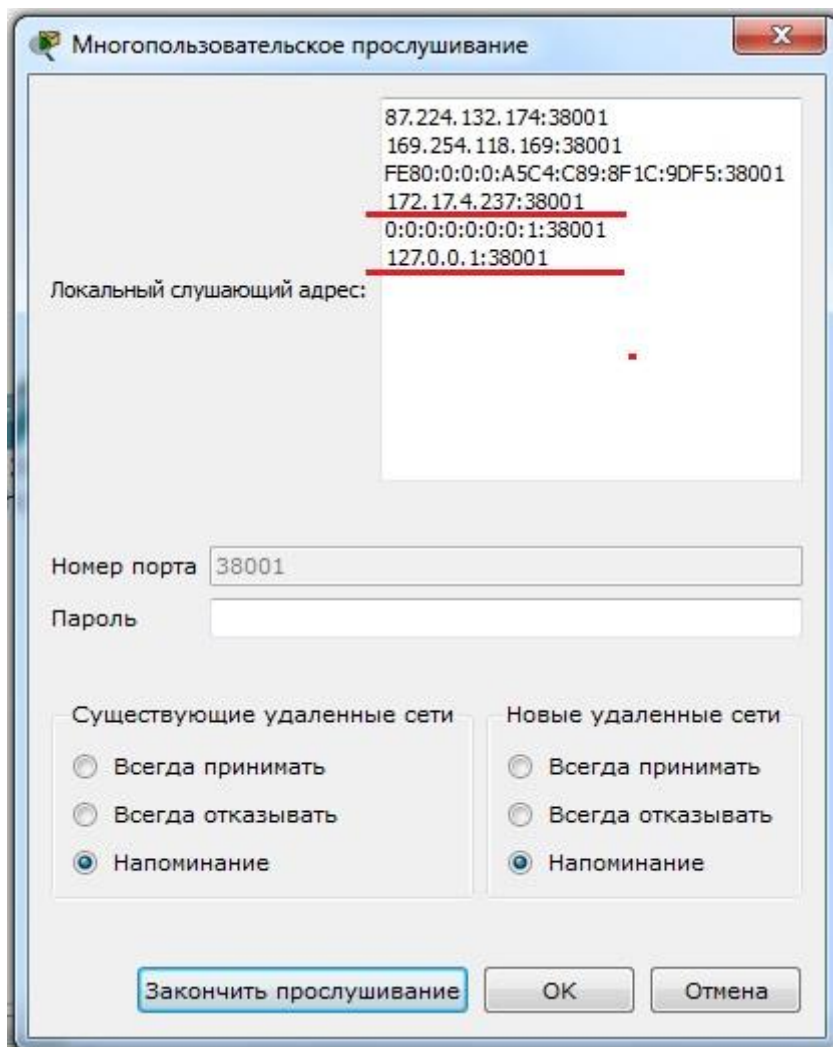


Рис. 5.7. Настройка общего канала доступа.

В верхней части показаны прослушиваемые сети. В нашем случае это сеть 172.17.0.0 и localhost.

Сеть 172.17.0.0 – локальная сеть, к которой подключен наш компьютер.

Точка входа задается ip адресом и портом: ip адрес 172.17.4.237, порт входа 38001.

Localhost – сеть 127.0.0.0, ip адрес 127.0.0.1, порт 38001.

Сделаем подключение через localhost.

Переключитесь в первую сессию.



Зайдите в настройки устройства «Сосед3».

Выберите тип соединения «Исходящее» и задайте имя общей сети в вашей топологии «Lan 11.0.0.0», задайте точку входа в сеть 2 - localhost:38001 и нажмите кнопку «Соединить» (рис. 5.8):

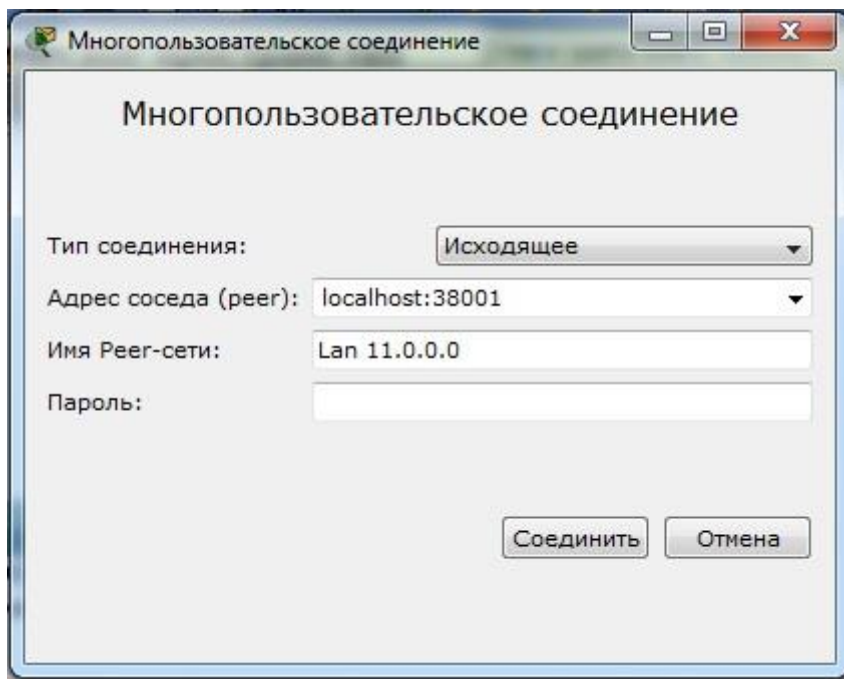


Рис. 5.8. Выбор точки входа.

В результате во второй сессии появится уведомление о соединении (рис.5.9):

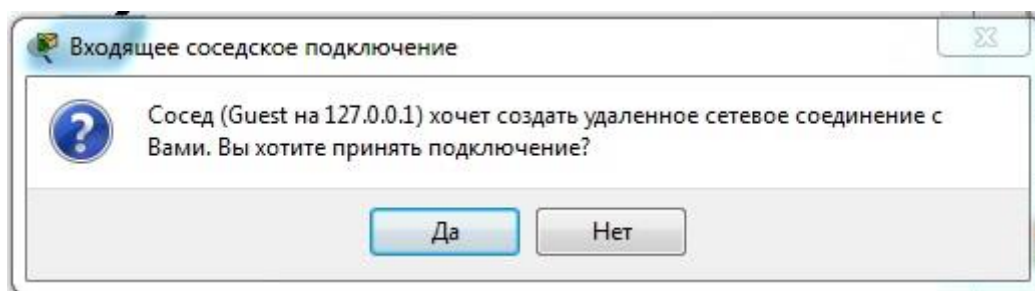


Рис. 5.9.Создание соединения.

В результате во второй сессии появится облако многопользовательского соединения.

Соедините созданное облако с коммутатором Switch3.

Для этого в группе «Соединения» выберите тип кабеля «Медный кроссовер» и соедините четвертый порт FastEthernet0/4 на Switch3 с облаком многопользовательского соединения через Канал0 (рис.5.10):

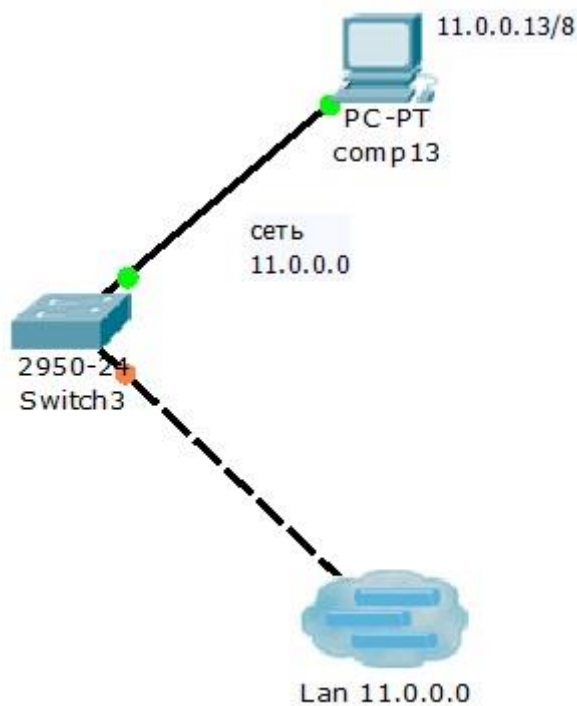


Рис.5.10. Подключение второй сессии к общему каналу.

Проверьте командой **ping** связь всех компьютеров во всех сетях между собой.

## Лабораторная работа № 6. Протоколы SMTP и POP3.

### 1. Построение топологии сети

Для исследования заданных прикладных протоколов построим тестовую топологию сети следующего вида (рис. 6.1):

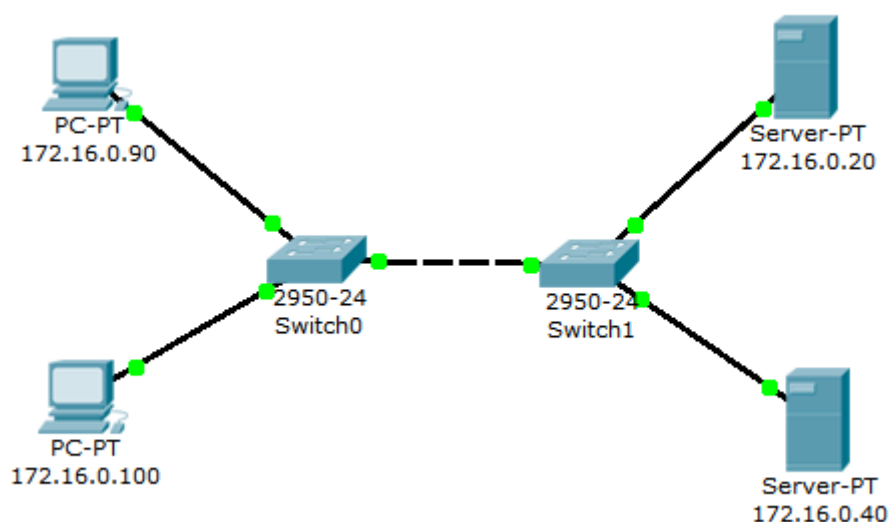


Рис. 6.1. Тестовая топология сети

Производим настройку сетевых устройств согласно заданным параметрам (таблица 6.2, таблица 6.3):

Таблица 6.2

Конечные узлы	IP-адрес	Маска сети	IP-адрес DNS-сервера
PC0	172.16.0.90	255.255.0.0	172.16.0.20
PC1	172.16.0.100	255.255.0.0	172.16.0.20

Таблица 6.3

Серверы	IP-адрес	Маска сети	IP-адрес DNS-сервера
Server0	172.16.0.20	255.255.0.0	172.16.0.20
Server1	172.16.0.40	255.255.0.0	172.16.0.20

Все устройства расположены в одном сегменте локальной сети, поэтому маршрутизация пакетов не используется, значит, IP-адрес шлюза по умолчанию указывать необязательно.

## 2. Настройка почтового сервера

В качестве серверов электронной почты выступают сервер 172.16.0.20 и сервер 172.16.0.40. Схема взаимодействия с прикладными почтовыми протоколами применительно к построенной сети представлена на рис. 6.4:

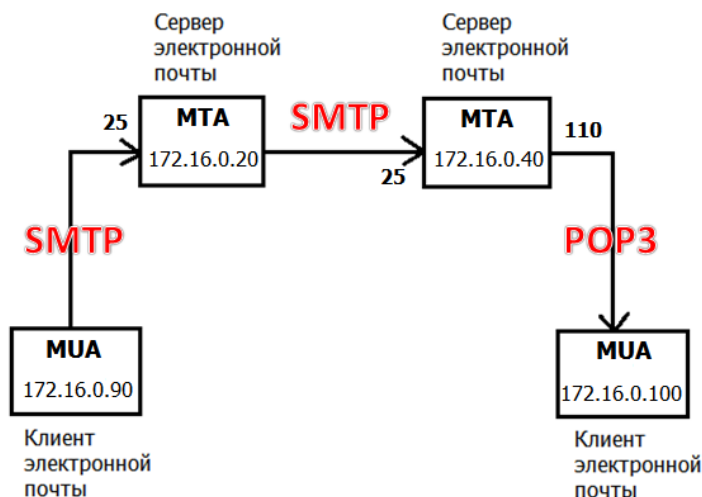


Рис. 6.4. Схема взаимодействия с прикладными почтовыми протоколами в исследуемой сети

На каждом из MTA будет поддерживаться smtp- и pop3-сервер. Подключиться к серверу может любой зарегистрированный пользователь. Чтобы отправить письмо, пользователь на сервере проходит авторизацию, после чего сервер готов отправлять письма от имени пользователя. По адресу назначения письма сервер определяет, кому следует передать его дальше. Нужный адрес сервер определяет с помощью службы DNS, в которой содержится соответствующая ресурсная адресная запись, преобразовывающая имя домена в IP-адрес.

Подключим службу DNS на сервере 172.16.0.20:

- 1) Один клик по выбранному устройству.
- 2) Выбираем вкладку *Config*, *Services* -> *DNS* (рис. 6.5). Заносим данные о новой ресурсной записи: имя домена, IP-адрес, тип ресурсной записи. Симулятор не поддерживает ресурсную запись, предназначенную для почтовых серверов, MX, но ее можно заменить адресной (тип A).

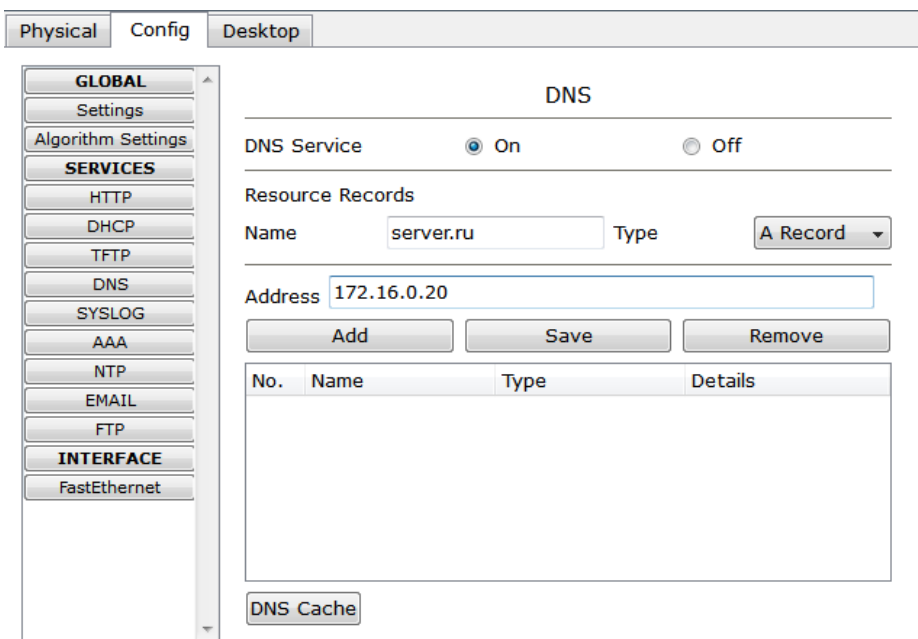


Рис. 6.5. Настройка службы DNS на сервере

- 3) Нажимаем на кнопку “Add” будет добавлена новая запись в службу DNS (рис. 6.6).

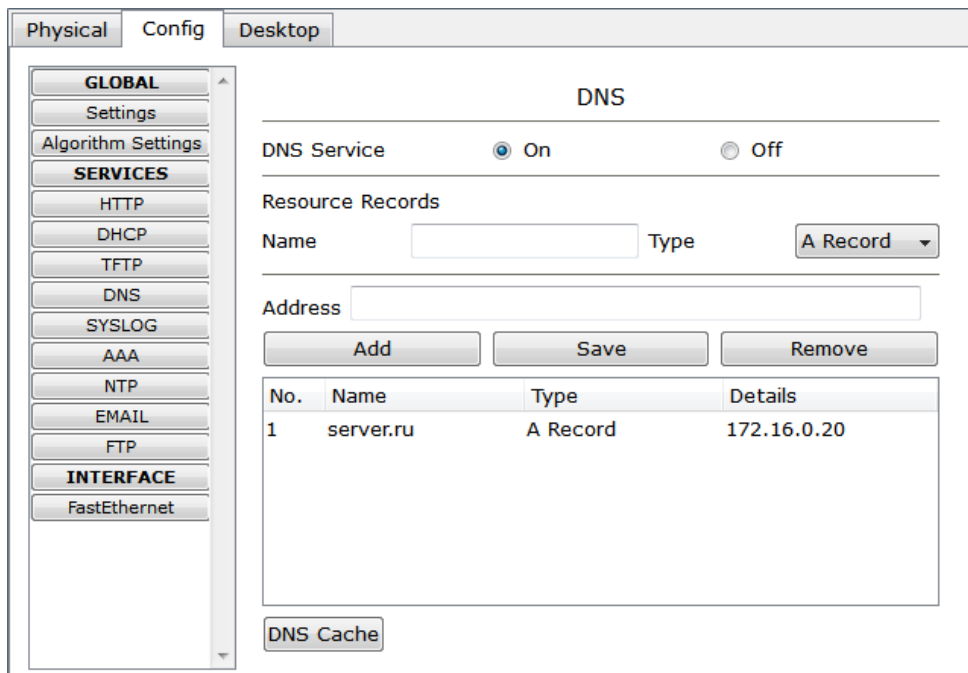


Рис. 6.6. Настройка службы DNS на сервере

Повторим предыдущие действия и добавим еще одну ресурсную запись о почтовом сервере 172.16.0.40 (рис. 6.7).

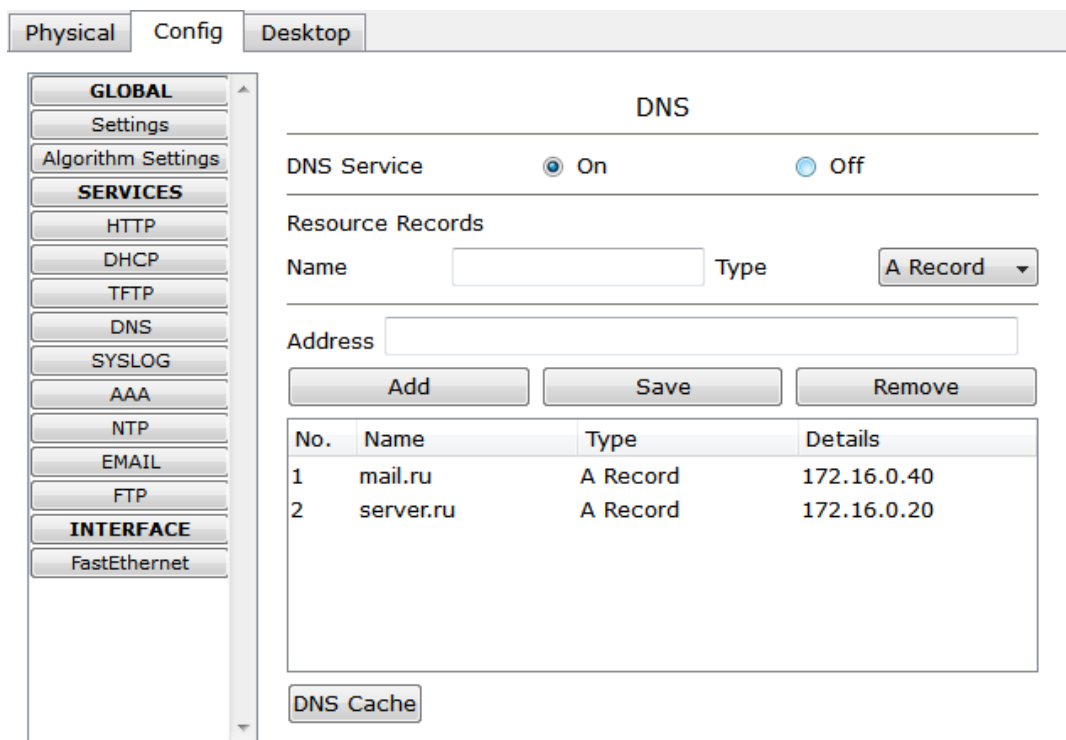


Рис. 6.7. Настройка службы DNS на сервере

Теперь сконфигурируем почтовый сервер 172.16.0.20 с поддержкой smtp- и pop3-сервера:

- 1) Один клик по выбранному устройству.
- 2) Выбираем вкладку “Config”, Services -> EMAIL
- 3) Подключаем протоколы SMTP и POP3 и вводим имя домена электронной почты. Нажимаем кнопку “Set” (рис. 6.8).

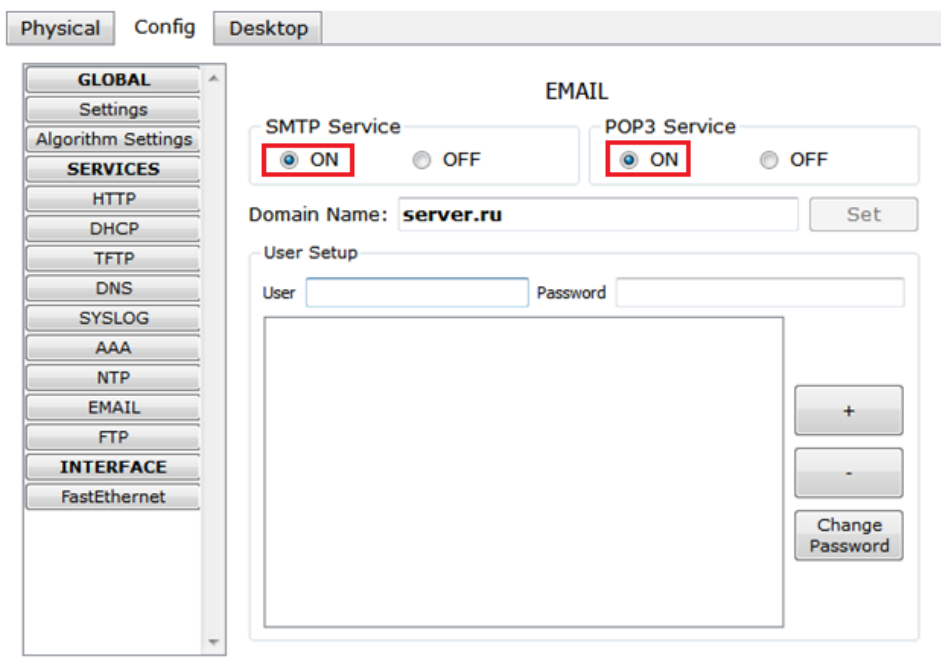


Рис. 6.8. Конфигурация smtp- и pop3-сервера

4) Создадим учетную запись для одного пользователя, вводим логин и пароль. Занести запись в службу можно с помощью кнопки “+” (рис. 6.9).

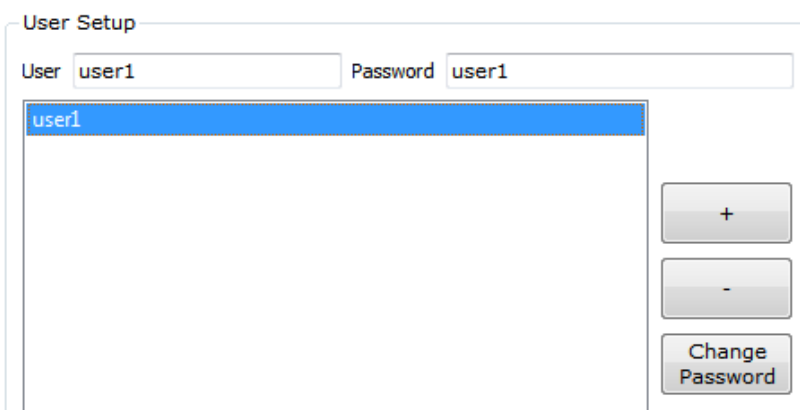


Рис. 6.9. Создание учетной записи

Smtp-сервер и pop3-сервер на машине 172.16.0.20 сконфигурированы, имеют одного зарегистрированного пользователя. Так же на нем поддерживается служба DNS, в которой есть две ресурсных записи.

На сервере 172.16.0.40 так же необходимо настроить почтовый сервер с поддержкой SMTP и POP3 (рис. 6.10). В качестве DNS для него выступает сервер 172.16.0.20.

- 1) Один клик по выбранному устройству.
- 2) Выбираем вкладку “Config”, Services -> EMAIL
- 3) Подключаем протоколы SMTP и POP3 и вводим имя домена электронной почты - *mail.ru*. Нажимаем кнопку “Set”.
- 4) Создадим учетную запись для одного пользователя, вводим логин и пароль. Занести запись в службу можно с помощью кнопки “+”.

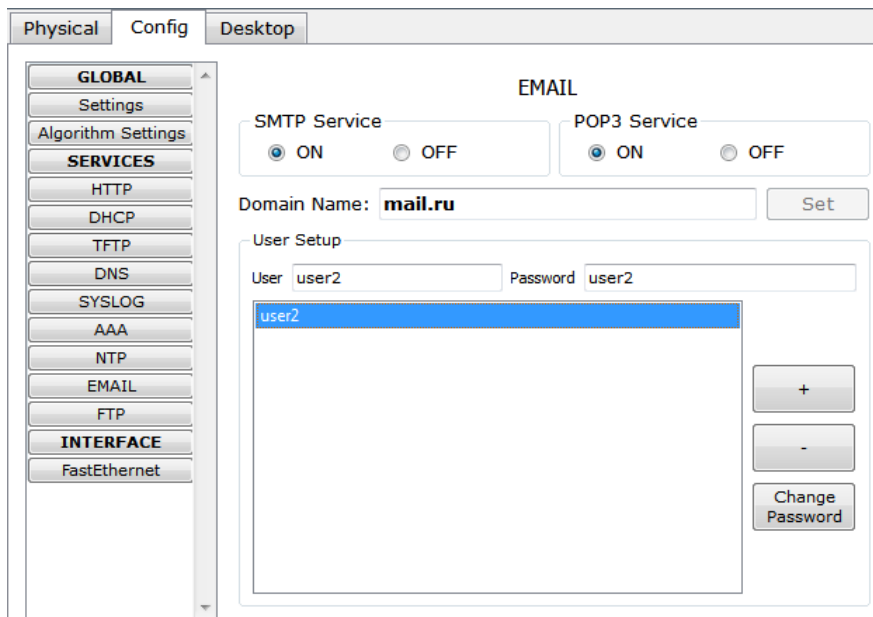


Рис. 6.10. Конфигурация smtp- и pop3-сервера

### 3. Настройка почтовой службы на конечных узлах

Для работы с почтовым smtp- или pop3-сервером на компьютере пользователя должен быть настроен клиент электронной почты, который и будет взаимодействовать с сервером (см. рис. 4.83).

Настроим на хосте 172.16.0.90 клиент электронной почты (рис. 6.11):

- 1) Один клик на хосте с IP-адресом 172.16.0.90.
- 2) Выбираем вкладку *Desktop*, программу “E-mail”. Появится окно конфигурации почтового сервиса. Вводим пользовательские данные в форму.

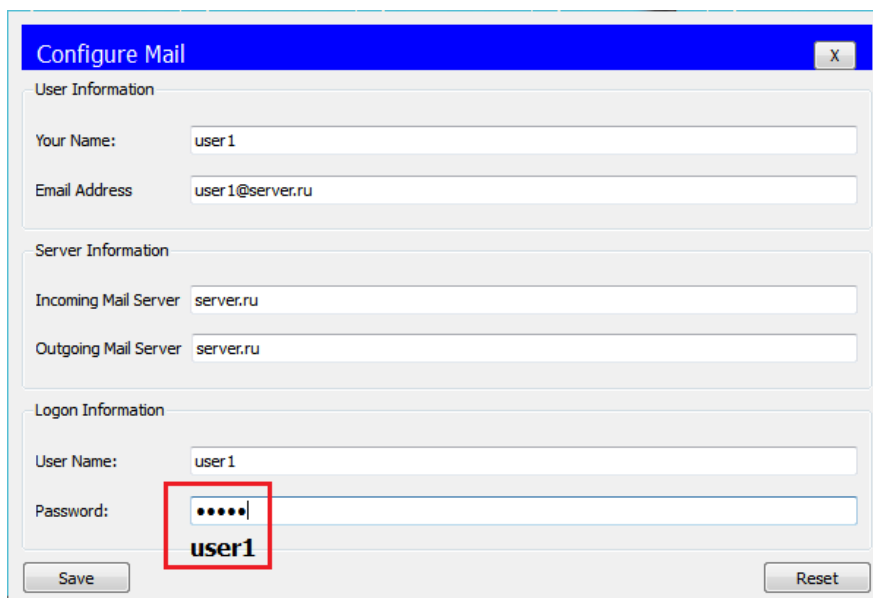


Рис. 6.11. Настройка клиента электронной почты

Нажимаем кнопку “Save”, закрываем окно, конфигурация клиента электронной почты завершена. Теперь для пользователя *user1* доступен почтовый сервис в домене *server.ru*: отправка и получение писем.

Настроим почтовый сервис и на хосте 172.16.0.100, выполнив предыдущие действия (рис. 6.12). Вводим следующие пользовательские данные:

**Configure Mail**

User Information

Your Name: user2

Email Address: user2@mail.ru

Server Information

Incoming Mail Server: mail.ru

Outgoing Mail Server: mail.ru

Logon Information

User Name: user2

Password: .....  
user2

Save Reset

Рис. 6.12. Настройка клиента электронной почты

Теперь для пользователя *user2* доступен почтовый сервис в домене *mail.ru*: отправка и получение писем.

Настройка всех устройств и необходимых служб завершена.

#### 4. Исследование прикладных почтовых протоколов в режиме симуляции

Переходим в режим симуляции Cisco Packet Tracer. Добавляем фильтры на 2 протокола: SMTP и POP3 (рис. 6.13). Это значит, что пакеты только фильтруемых протоколов будут отображаться в сети.

**Event List**

Vis.	Time (sec)	Last Device	At Device	Type	Info
------	------------	-------------	-----------	------	------

Reset Simulation ☒ Constant Delay Captured to: \* (no captures)

**Play Controls**

Back Auto Capture / Play Capture / Forward

**Event List Filters**

Visible Events: POP3, SMTP

Edit Filters Show All

Рис. 6.13. Окно событий режима симуляции



Отправим письмо с хоста 172.16.0.90 от *user1* на хост 172.16.0.100 *user2* (рис. 6.14):

- 1) Один клик по выбранному узлу (172.16.0.90).
- 2) Выбираем на вкладке “Desktop” программу “E-mail”.
- 3) Чтобы написать и отправить письмо, нажимаем на кнопку “Compose”. Появится форма, которую следует заполнить. В поле “To” задается адрес электронной почты, кому вы отправляете письмо. Поле “Subject” содержит заголовок письма. Текст письма можете сочинить самостоятельно.

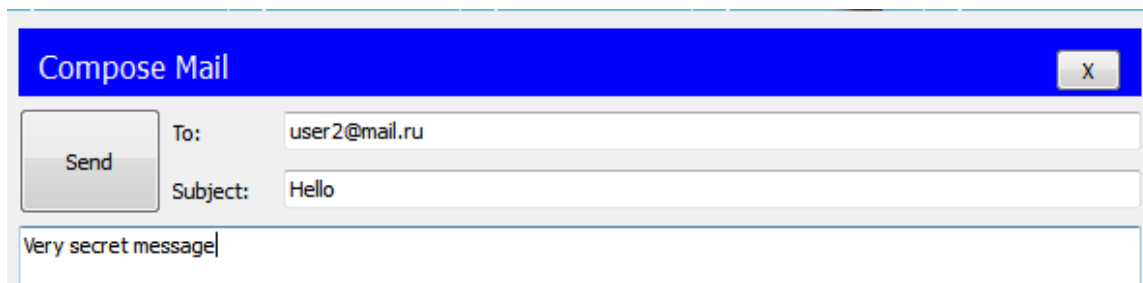


Рис. 6.14. Форма для отправления письма

Нажимаем на кнопку “Send”, начнется отправление письма.

Видим, что на хосте 172.16.0.90 сформировался пакет SMTP (рис. 6.15). Воспользовавшись кнопкой “Capture/Forward”, проследим за маршрутом пакета от устройства к устройству.

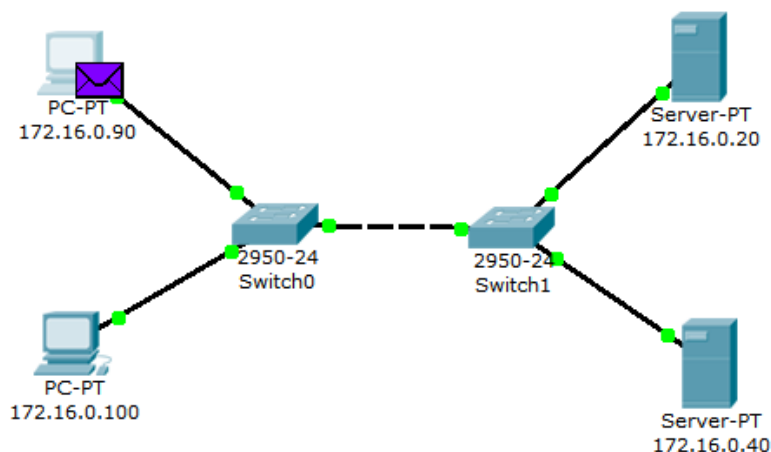


Рис. 6.15. Вид рабочей области

Посмотрим содержимое пакета, сформированного на узле (рис. 6.16).

### IP

0	4	8	16	19	31 Bits
4	IHL	DSCP: 0x0	TL: 101		
ID: 0x10			0x2	0x0	
TTL: 128		PRO: 0x6	CHKSUM		
SRC IP: 172.16.0.90					
DST IP: 172.16.0.20					
OPT: 0x0				0x0	
DATA (VARIABLE LENGTH)					

### TCP

0	16	31 Bits
SRC PORT: 1027		DEST PORT: 25
SEQUENCE NUM: 1		
ACK NUM: 1		
OFF.	RES.	PSH + ACK
CHECKSUM: 0x0		URGENT POINTER
OPTION		PADDING
DATA (VARIABLE)		

### SMTP

SMTP DATA
-----------

Рис. 6.16. Формат пакета SMTP

Пакет адресован почтовому серверу по IP-адресу 172.16.0.20. В заголовке TCP содержится порт назначения – 25. Можно сделать вывод, что пакет сформирован верно. Пакет на пути своего следования к серверу проходит через два коммутатора (рис. 6.17). Убедитесь, что это так.

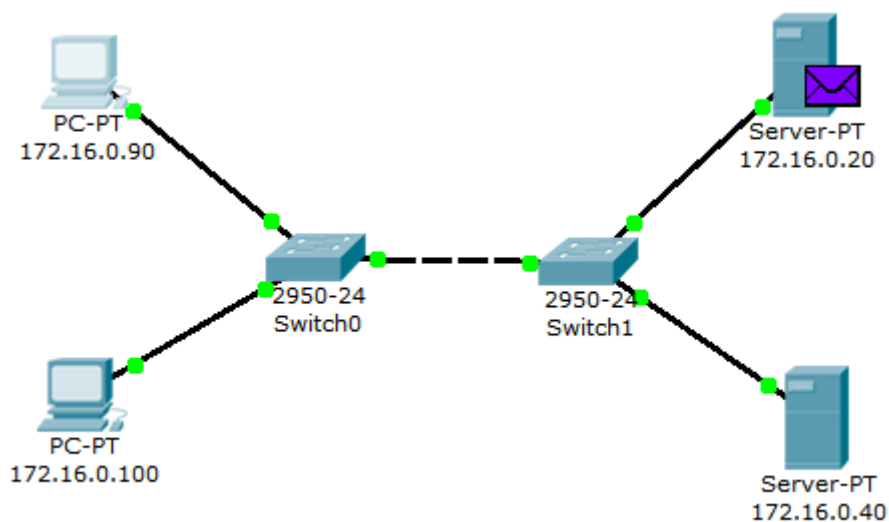


Рис. 6.17. Вид рабочей области

Когда пакет приходит на сервер, тот, обрабатывая его, определяет, что письмо адресовано домену *mail.ru*. Сервер 172.16.0.20 обращается к службе DNS за IP-адресом заданного сервера. По указанному адресу письмо перенаправляется на соответствующий почтовый сервер (рис. 6.18).

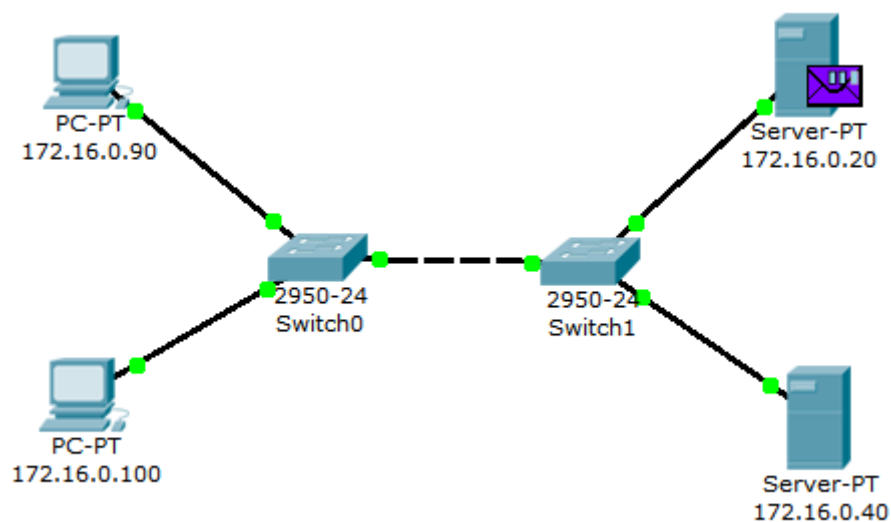


Рис. 6.18. Вид рабочей области

SMTP-пакет, сформированный сервером 172.16.0.20, содержит следующую информацию: IP-адрес назначения – 172.16.0.40, порт назначения – 25 (рис. 6.19).

### IP

0	4	8	16	19	31 Bits
4	IHL	DSCP: 0x0	TL: 101		
ID: 0x11			0x2	0x0	
TTL: 128		PRO: 0x6	CHKSUM		
SRC IP: 172.16.0.20					
DST IP: 172.16.0.40					
OPT: 0x0				0x0	
DATA (VARIABLE LENGTH)					

### TCP

0	16	31 Bits
SRC PORT: 1025		DEST PORT: 25
SEQUENCE NUM: 1		
ACK NUM: 1		
OFF.	RES.	PSH + ACK
CHECKSUM: 0x0		URGENT POINTER
OPTION		PADDING
DATA (VARIABLE)		

### SMTP

SMTP DATA
-----------

Рис. 6.19. Формат пакета SMTP

Пакет проходит через коммутатор Switch1 и доставляется серверу 172.16.0.40 (рис. 6.20).

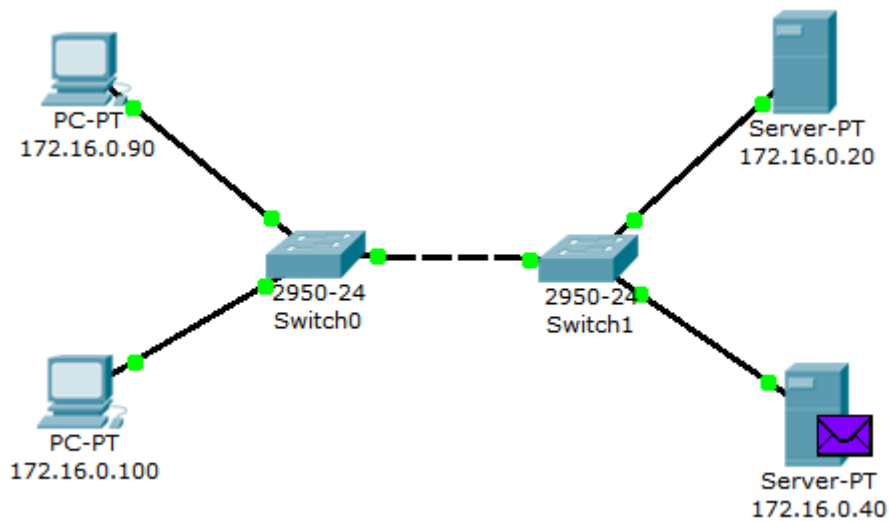


Рис. 6.20. Вид рабочей области

На сервере 172.16.0.40 формируется SMTP-ответ серверу 172.16.0.20 и отправляется на указанный адрес (рис. 6.21).

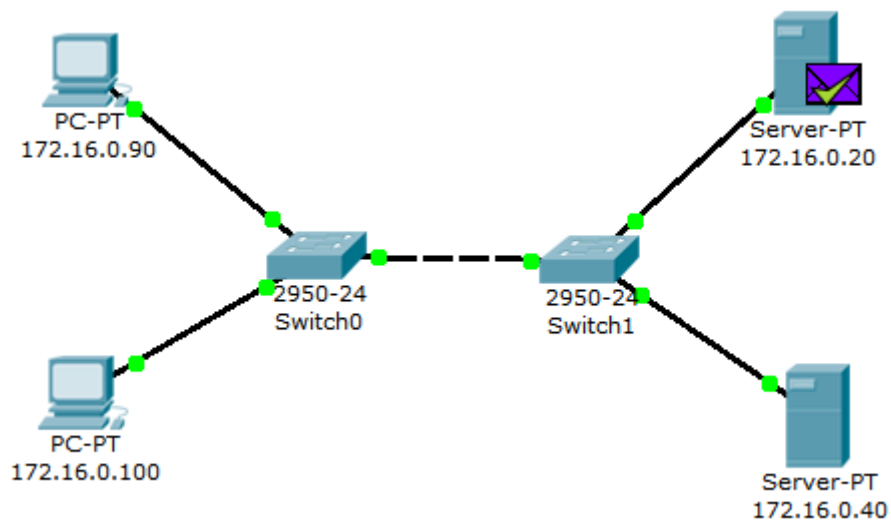


Рис. 6.21. Вид рабочей области

Из содержимого пакета, пришедшего обратно на сервер 172.16.0.20: IP-адрес источника – 172.16.0.40, порт источника – 25 (рис. 6.22).

### IP

0	4	8	16	19	31 Bits
4	IHL	DSCP: 0x0	TL: 44		
ID: 0x4			0x2	0x0	
TTL: 128		PRO: 0x6	CHKSUM		
SRC IP: 172.16.0.40					
DST IP: 172.16.0.20					
OPT: 0x0				0x0	
DATA (VARIABLE LENGTH)					

### TCP

0	16	31 Bits
SRC PORT: 25		DEST PORT: 1025
SEQUENCE NUM: 1		
ACK NUM: 82		
OFF.	RES.	PSH + ACK
CHECKSUM: 0x0		URGENT POINTER
OPTION		PADDING
DATA (VARIABLE)		

### SMTP

SMTP DATA
-----------

Рис. 6.22. Формат пакета SMTP

С помощью протокола SMTP мы отправили письмо на сервер *mail.ru*, теперь оно хранится там.

Наш адресат (узел 172.16.0.100) еще не получил отправленное письмо, так как на сервер он еще не обратился по протоколу POP3. Для получения письма необходимо проделать следующие действия:

- 1) Один клик по узлу 172.16.0.100.
- 2) Выбираем на вкладке “Desktop” программу “E-mail”.
- 3) Нажимаем на кнопку “Receive”, чтобы прочитать письмо.

На хосте формируется пакет протокола POP3 (рис. 6.23). Воспользовавшись кнопкой “Capture/Forward”, проследим за маршрутом пакета от устройства к устройству.

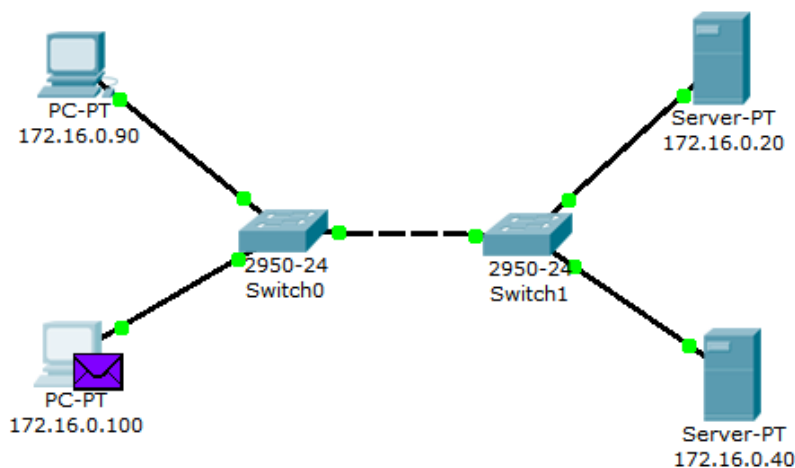


Рис. 6.23. Вид рабочей области

Посмотрим содержимое пакета, сформированного на узле (рис. 6.24).

<u>IP</u>									
0	4	8	16	19	31 Bits				
4	IHL	DSCP: 0x0	TL: 42						
ID: 0x4				0x2	0x0				
TTL: 128		PRO: 0x6		CHKSUM					
SRC IP: 172.16.0.100									
DST IP: 172.16.0.40									
OPT: 0x0								0x0	
DATA (VARIABLE LENGTH)									

<u>TCP</u>									
0	16				31 Bits				
SRC PORT: 1025				DEST PORT: 110					
SEQUENCE NUM: 1									
ACK NUM: 1									
OFF.	RES.	PSH + ACK		WINDOW					
CHECKSUM: 0x0				URGENT POINTER					
OPTION							PADDING		
DATA (VARIABLE)									

<u>POP3</u>									
POP3 DATA									

Рис. 6.24. Формат пакета POP3

Пакет адресован почтовому серверу по IP-адресу 172.16.0.40. В заголовке TCP содержится порт назначения – 110. Можно сделать вывод, что пакет сформирован верно. Пакет на пути своего следования к серверу проходит через два коммутатора. Убедитесь, что это так. Когда пакет приходит на сервер, тот обрабатывает его и формирует пакет-ответ (рис. 6.25).

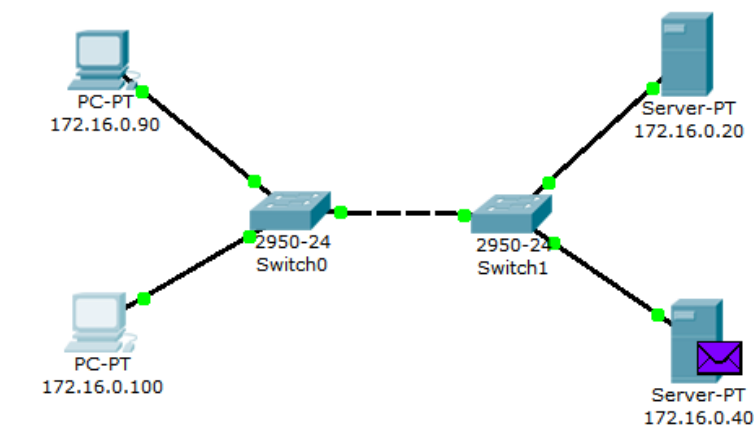
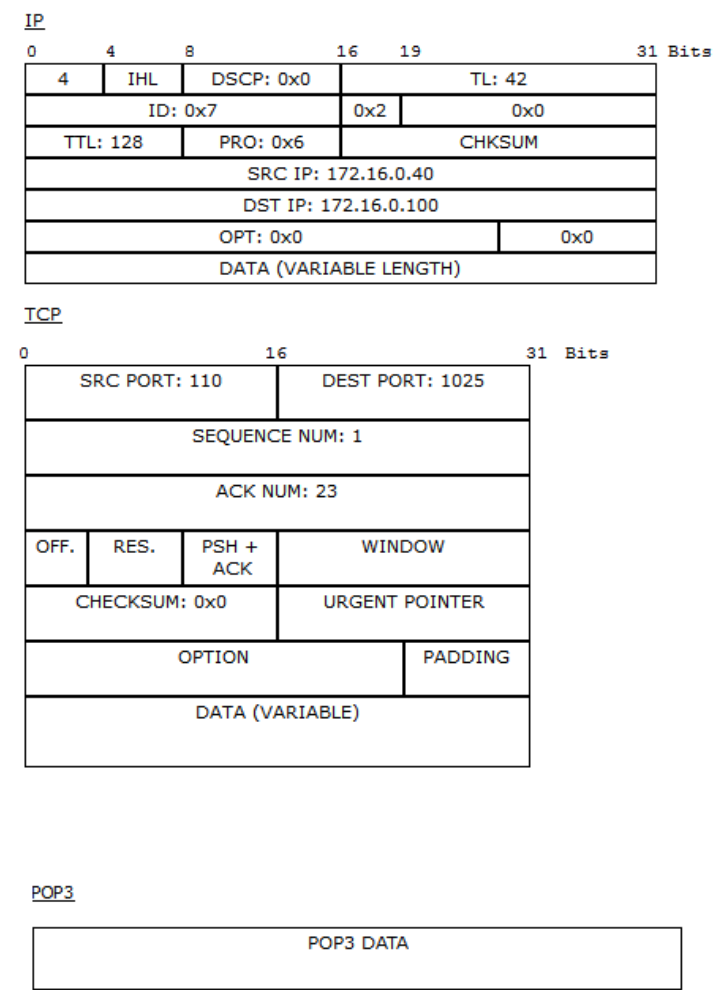


Рис. 6.25. Вид рабочей области

Пакет по тому же маршруту возвращается на узел 172.16.0.100 с ответом (письмом) от сервера. Посмотрим содержимое ответа (рис. 6.26).





Порт-источник – 110. Ответ пришел от сервера 172.16.0.40 с некоторыми POP3-данными. С помощью протокола POP3 узел 172.16.0.100 получил письмо с сервера, отправленное туда узлом 172.16.0.90 (рис. 6.27).

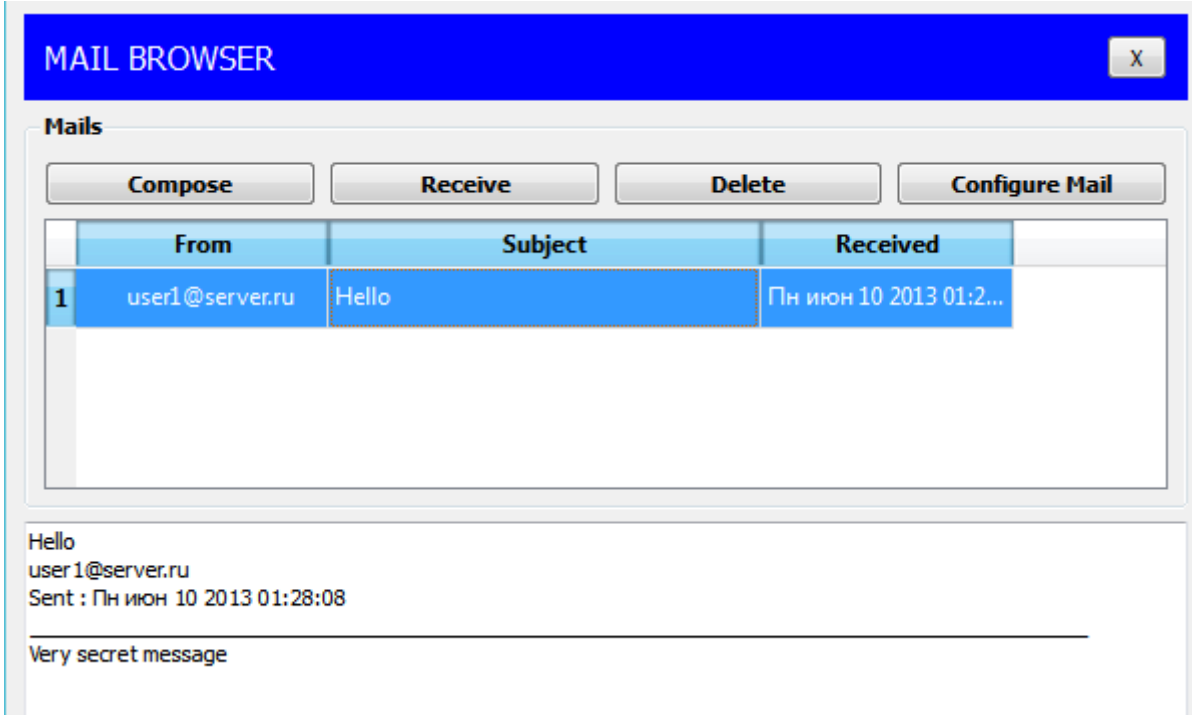


Рис. 6.27. Форма чтения входящих писем

Как уже упоминалось в теоретических сведениях, почтовые протоколы SMTP и POP3 обмениваются информацией с помощью команд. Клиенту электронной почты, чтобы установить соединение с сервером, отправить письмо, разорвать соединение необходимо отправлять серверу соответствующие команды. Сервер электронной почты, в свою очередь, обрабатывает эти команды и формирует отклики для клиента. Отклики smtp-сервера содержат цифровой код ответа: успешно или с ошибкой обработана команда. Отклики pop3-сервера так же содержат два типа сообщений: успех или ошибка.

Обращая внимание на содержимое пакета SMTP или POP3 протокола, видно, что на прикладном уровне пакет детально не рассматривается.

Пример приведен на рис. 6.28.

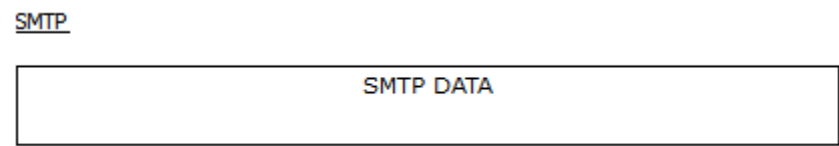


Рис. 6.28. Данные прикладного уровня

Поэтому эксперимент послыки письма несуществующему пользователю не является содержательным, т.к. подробно увидеть ответ от smtp-сервера нам не удастся. Для подробного изучения взаимодействия между клиентом и smtp- или pop3-сервером следует обратиться к предложенной спецификации RFC 2821 и RFC 1939.