

САНКТ-ПЕТЕРБУРГСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ПЕТРА ВЕЛИКОГО

КАФЕДРА КОМПЬЮТЕРНЫХ СИСТЕМ И ПРОГРАММНЫХ ТЕХНОЛОГИЙ

Курсовая работа

Курс: «Администрирование компьютерных сетей»

Тема: «Проектирование корпоративной компьютерной сети для фирмы по юридической консультации»

Выполнил студент:

Ерниязов Тимур Ертлеуевич

Группа: 13541/2

Проверил:

Малышев Игорь Алексеевич

Санкт-Петербург
2019 г.

Содержание

0.1	Цель работы	2
0.2	Постановка задачи	2
0.3	Выполнение работы	2
0.3.1	Создание сети	2
0.3.2	Настройка подсети NET0 (имитация внешней сети)	4
0.3.3	Настройка подсети NET1 (сеть с сайтом компании)	6
0.3.4	Настройка подсети NET2 (пользовательская сеть)	7
0.3.5	Настройка подсети NET3 (служебная сеть)	8
0.3.6	Настройка подсети RT0	8
0.4	Тестирование	9
0.4.1	Проверка Email сервера	9
0.4.2	Проверка TFTP	10
0.4.3	Проверка команды ping по адресу	11
0.4.4	Проверка команды ping по доменному имени	11
0.4.5	Проверка команды ping из изолированной сети	11
0.5	Заключение	13

Введение

В современном мире работа ни одной организации не обходится без помощи сети. Люди всегда стремились сделать свою жизнь проще. Нехватка времени явилась причиной научно технического прогресса, создания различной техники, благодаря работе которой человек мог значительно быстрее решать поставленные перед ним задачи.

Работа сети во многом зависит от рациональной структуры её реализации, то есть актуальным до сих пор является вопрос построения сети. Эта задача и является целью создания данной работы.

0.1 Цель работы

Создать и настроить компьютерную сеть для фирмы юридической консультации средствами **Cisco Packet Tracer**. Установить и сконфигурировать необходимые сервисы. Выполнить проверку работы сети.

0.2 Постановка задачи

Разрабатываемая сеть должна отвечать следующим требованиям:

1. Иметь несколько подсетей:
 - Пользовательская (для сотрудников);
 - Подсеть с сайтом компании и почтовым сервисом;
 - Служебная подсеть, в которой хранятся рабочие файлы компании.
2. Пользовательская сеть должна иметь доступ к другим подсетям, а также к сети "интернет";
3. Служебная подсеть должна быть изолирована от сети "интернет".

Реализуемая функциональность подсетей:

1. Пользовательская (для сотрудников):
 - Настроенный DNS сервер, для автоматического получения адреса сотрудниками.
2. Подсеть с сайтом компании:
 - Email и HTTP сервер с сайтом компании.
3. Служебная подсеть:
 - TFTP сервер для хранения файлов.

0.3 Выполнение работы

0.3.1 Создание сети

Для создания сети, были использованы следующие элементы Cisco Packet Tracer:

- Конечные устройства:
 - **PC-PT** - компьютер;
 - **Server-PT** - сервер;
- Сетевые устройства:
 - **Router-PT** - роутер;
 - **2950-24** - коммутатор на 24 порта;

Связь между устройствами была произведена с использованием инструмента **automatically choose connection type**, который автоматически подключает интерфейсы устройств.

Была спроектирована следующая сеть, приведенная на рисунке 1.

Представленную сеть можно разделить на следующие подсети:

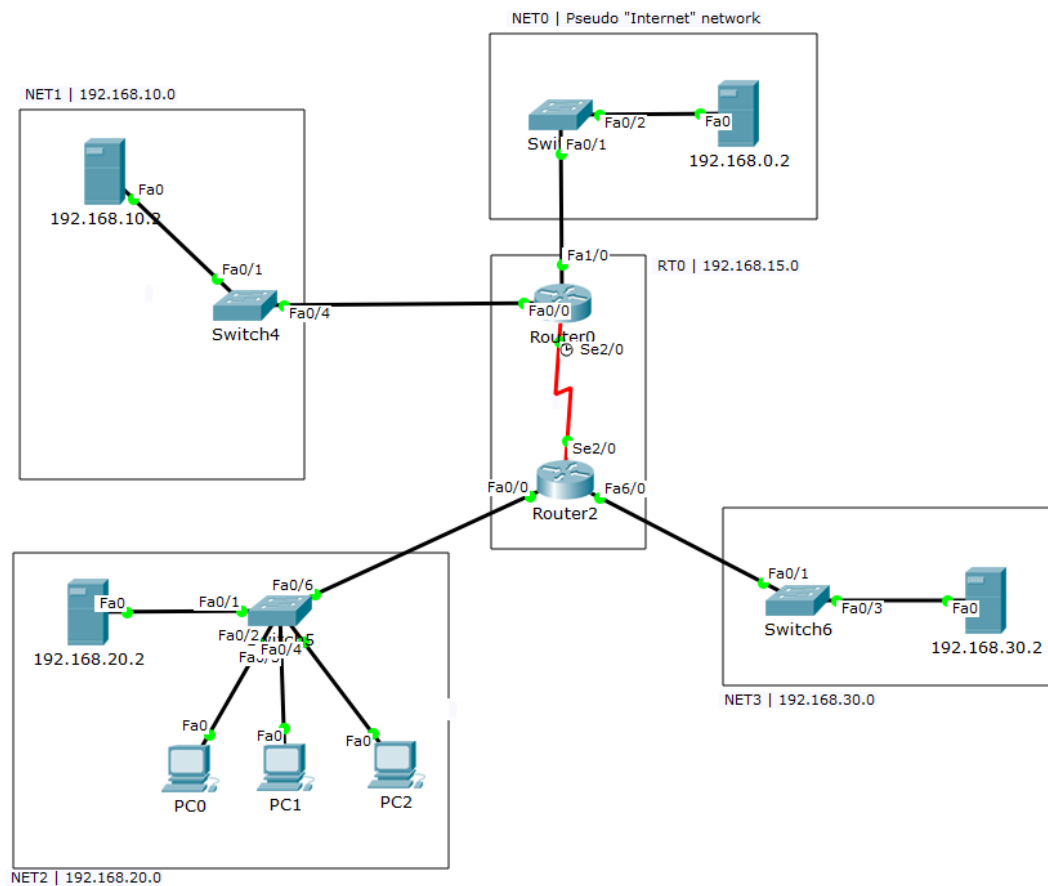


Рис. 1: Вкладка Desktop

- **NET0** - сеть имитирующая работу сети "интернет необходима, так как Cisco Packet Tracer не предоставляет возможность доступа к реальной сети;
- **NET1** - Подсеть с сайтом компании;
- **NET2** - Пользовательская (для сотрудников) подсеть;
- **NET3** - Служебная подсеть;
- **RT0** - Подсеть для связи роутеров. Связь выполнена с помощью порта **serial**. Подобный тип подключения является устаревшим, но другого выбора подключения двух роутеров в программе не представлено, поэтому можно считать это особенностью Cisco Packet Tracer.

0.3.2 Настройка подсети NET0 (имитация внешней сети)

Конфигурирование интерфейсов

В подсети находится один конечный узел. Для настройки интерфейса выберем узел и перейдем на вкладку **Desktop**

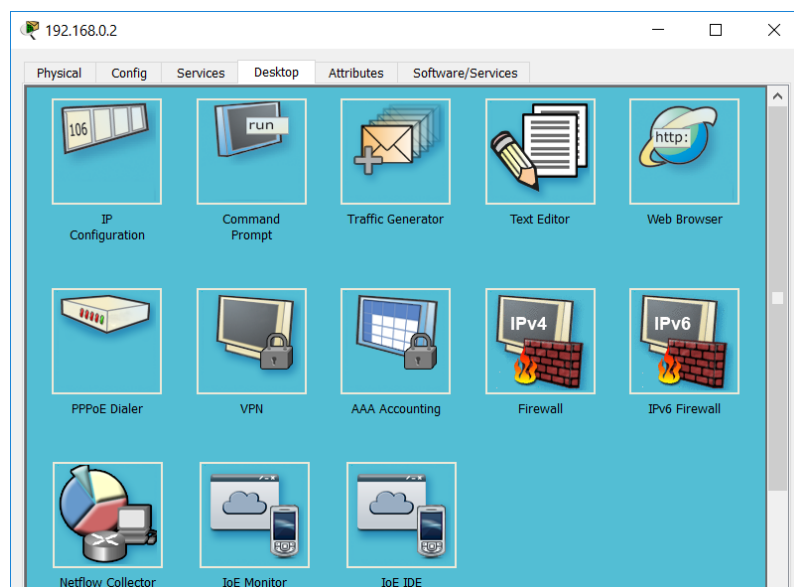


Рис. 2: Вкладка Desktop

Во вкладке представлены различные утилиты. Для настройки интерфейса необходимо выбрать **IP Configuration**

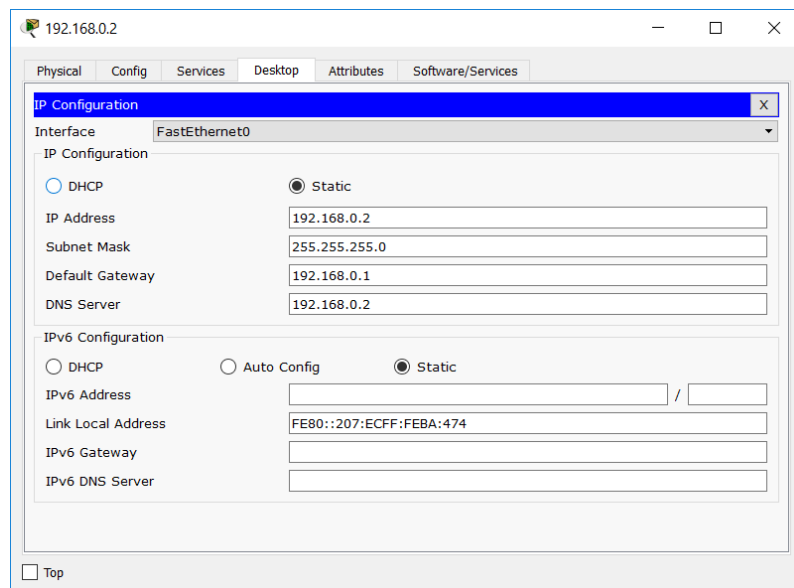


Рис. 3: Сконфигурированный интерфейс FastEthernet0

Интерфейс был сконфигурирован статически. Адрес **192.168.0.1** является интерфейсом роутера, к которому имеется подключение через коммутатор. В качестве DNS сервера выступает этот же конечный узел.

Установка и настройка сетевых сервисов

Доступные сервисы находятся на вкладке **Services**. Для добавления новой записи необходимо указать **Name** - доменное имя, и **Address** - адрес ресурса.

Было добавлено 2 записи:

1. **www.internetpage.com** - имитация сайта в сети "интернет";
2. **www.urcons.com** - сайт компании.

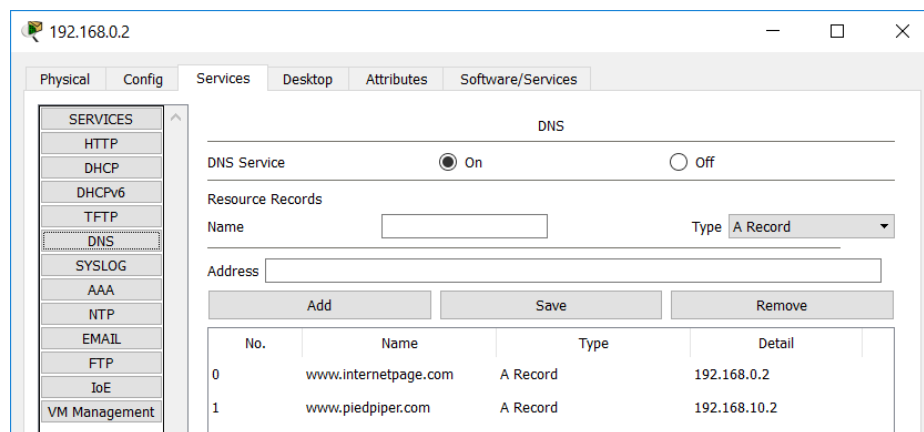


Рис. 4: Сконфигурированный DNS сервис

В конечных узлах типа - сервер, по умолчанию включен HTTP сервис, в котором по умолчанию уже имеются некоторые файлы для работы сайта. Формат web страницы - **html**, что означает возможность использования html-тегов при редактировании сайта.

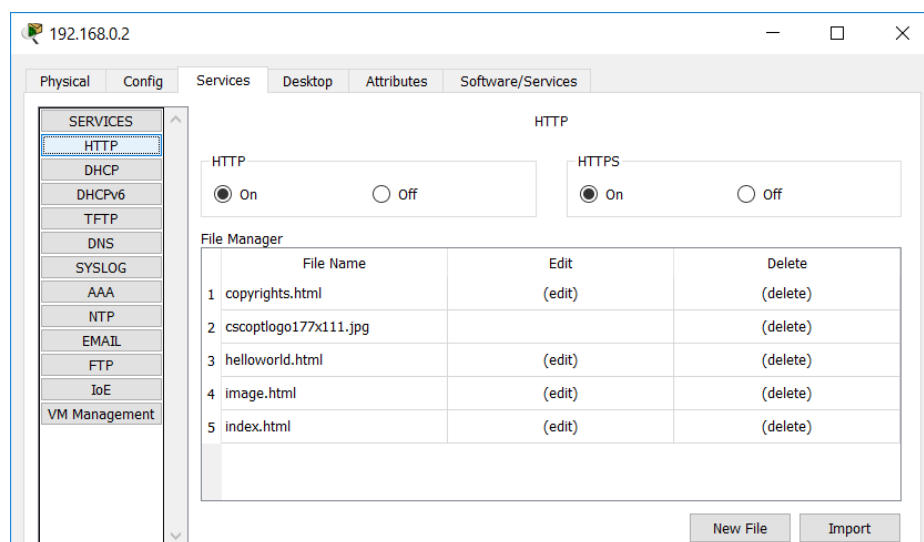


Рис. 5: HTTP сервис

Откроем утилиту - **Web Browser** и введем в строчке адреса - **www.internetpage.com**.

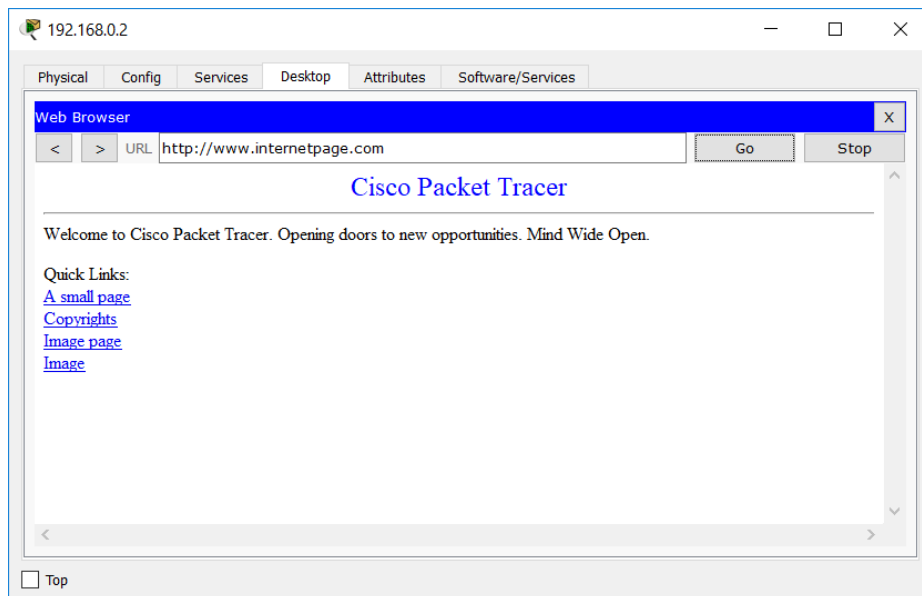


Рис. 6: WEB страница

Для доменного имени был успешно определен адрес, и web страница успешно загрузилась.

0.3.3 Настройка подсети NET1 (сеть с сайтом компании)

Конфигурирование интерфейсов

Интерфейс(Fa0) был задан статически:

- IP Address - 192.168.10.2;
- Subnet Mask - 255.255.255.0
- Default Gateway - 192.168.10.1;
- DNS Server - 192.168.0.2.

Установка и настройка сетевых сервисов

Был настроен HTTP сервис, но в отличии от настройки в подсети NET0.

Страница представляет собой сайт-визитку компании. Доступ к странице также возможен по доменному имени **www.urcons.com**

Примечание: в случае ввода в редактор кириллических символов, утилита **Web Browser** отобразит их некорректно.

Также был настроен Email сервис. В котором:

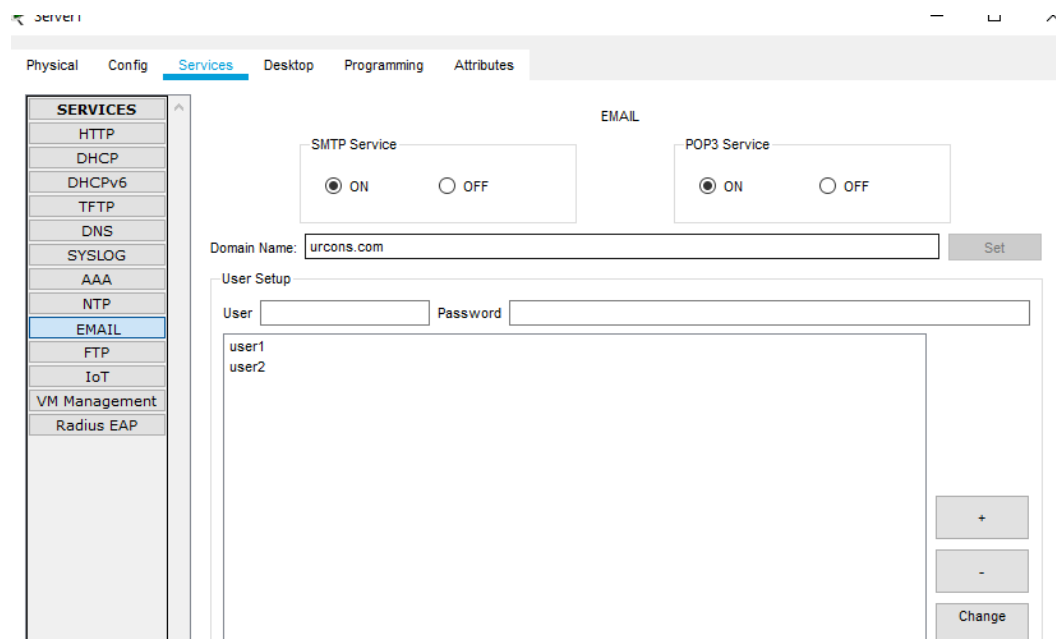


Рис. 7: Email сервис

- Указано доменное имя - **urcons.com**;
- Добавлено 2 пользователя: user1, user2 с паролями password1, password2 соответственно.

0.3.4 Настройка подсети NET2 (пользовательская сеть)

Конфигурирование интерфейсов

Интерфейс сервера(Fa0) был задан статически:

- **IP Address** - 192.168.20.2;
- **Subnet Mask** - 255.255.255.0
- **Default Gateway** - 192.168.20.1;
- **DNS Server** - 192.168.0.2.

У всех прочих узлов, в настройках **IP Configuration** выбирается настройка по DHCP.

Установка и настройка сетевых сервисов

Сервис DhCP был включен на сервере (192.168.20.2), где были заполнены следующие поля:

- **Interface** - FastEthernet0;
 - единственный интерфейс данного узла.
- **Default Gateway** - 192.168.20.1;
 - шлюзом по умолчанию выступает интерфейс роутера, подключенный к данной(NET_2) подсети.
- **DNS Server** - 192.168.0.2;
 - предварительно настроенный DNS сервер из подсети NET_0.
- **Start IP Address** - 192.168.20.5;
 - начала диапазона по выдаче IP-адресов.
- **Subnet Mask** - 255.255.255.0;

— маска подсети.

- **Maximun number of Users** - 100;

— максимальное количество пользователей.

На клиентских узлах, с помощью утилиты **Email** был настроен доступ к Email серверу компании.

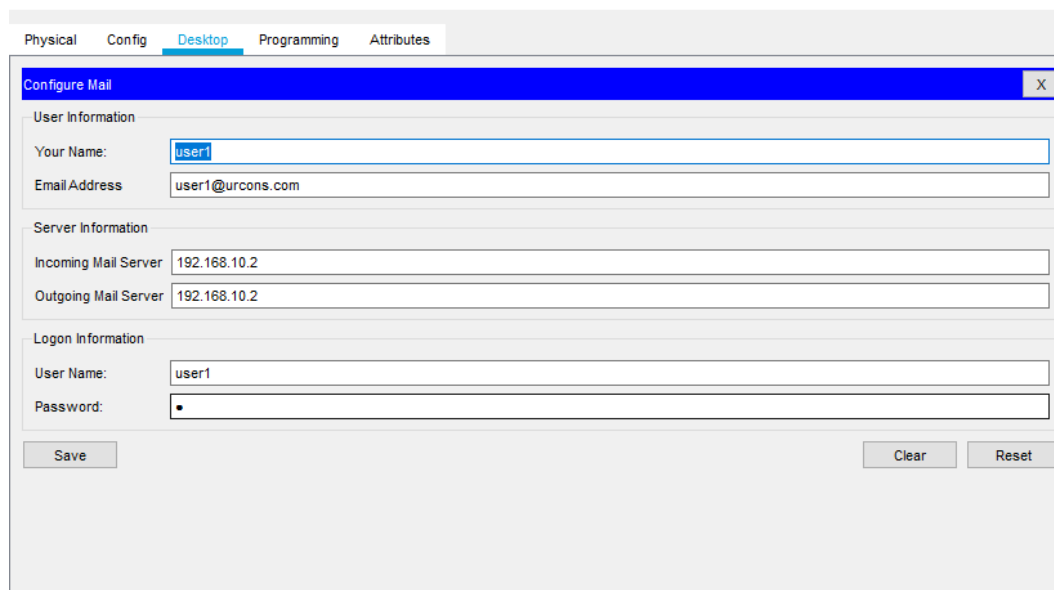


Рис. 8: Настройка доступа к Email серверу на одном из пользовательских узлов

0.3.5 Настройка подсети NET3 (служебная сеть)

Конфигурирование интерфейсов

Интерфейс сервера(Fa0) был задан статически:

- **IP Address** - 192.168.30.2;
- **Subnet Mask** - 255.255.255.0
- **Default Gateway** - 192.168.30.1;
- **DNS Server** - 192.168.0.2.

Установка и настройка сетевых сервисов

Настройка TFTP сервиса была произведена на вкладке **Services**. Где его необходимо было включить, и для удобства удалить предварительно сгенерированные в нем файлы.

0.3.6 Настройка подсети RT0

Конфигурирование интерфейсов

В сети имеются два роутера(**Router 0** и **Router2**), которые выполняют функцию связующего звена между подсетями.

Настройка маршрутизации

Также, для корректной работы сети была добавлена маршрутизация. Для этого на Router 0, в настройках был выбран пункт **RIP Routing**, в который были добавлены следующие подсети:

- 192.168.0.0;
- 192.168.10.0;
- 192.168.15.0.

И для Router 2 соответственно:

- 192.168.15.0;
- 192.168.20.0;
- 192.168.30.0.

Изоляция сети

Сеть NET3 необходимо изолировать от какого-либо внешнего доступа, то-есть доступ к ней должны иметь сотрудники, из пользовательской сети NET2.

Для этого, на Router2 открывается **CLI**(Command Line Interface). В котором, для настройки **ACL**, вводятся следующие команды:

Листинг 1: index.html

```
1 Router> enable
2 Router# conf terminal
3
4 Router(config)#access-list 101 permit ip any 192.168.20.0 0.0.0.255
5 Router(config)#access-list 101 permit ip 192.168.20.0 0.0.0.255 anyВыход
6 /* из настройки нажатием CTRL + Z*/
7 Router(config)#^Z
8 Router#sh access-list
9 Extended IP access list 101
10    10 permit ip any 192.168.20.0 0.0.0.255
11    20 permit ip 192.168.20.0 0.0.0.255 192.168.30.0 0.0.0.255
```

- Командой **enable** был совершен переход в привилегированный режим;
- Командой **conf terminal** начата настройка;

Командами

```
access-list 101 permit ip any 192.168.20.0 0.0.0.255
access-list 101 permit ip 192.168.20.0 0.0.0.255 any
```

и был ограничен доступ всем, кроме пользовательской сети.

Разберем данную команду:

- **101** - означает номер правила. 0-99 - обычные правила, 100-199 расширенные. У расширенных правил, разумеется больший диапазон настройки;
- **permit** - действие которое будет применено, в данном случае разрешение;
- **ip** - тип протокола;
- **any 192.168.20.0 0.0.0.255** - любая сеть может обращаться к сети NET2;
- **192.168.20.0 0.0.0.255 any** - сеть NET2 может обращаться к любой сети.

По умолчанию, все пакеты разрешены(permit), но после включения правил **ACL**, к пакетам которые не подходят не под одно правило, будет применено действие **deny**, то есть они не будут пропущены.

Таким образом, для сети NET3, был сохранен доступ из пользовательской сети, и в тоже время ограничен доступ из прочих сетей

0.4 Тестирование

0.4.1 Проверка Email сервера

От пользователя **user2@urcons.com** создается письмо пользователю **user1@urcons.com**. Для отправки необходимо нажать кнопку **Send**.

Зайдем в утилиту **Email** от пользователя **user1@urcons.com**, и получим почту кнопкой **Receive**.

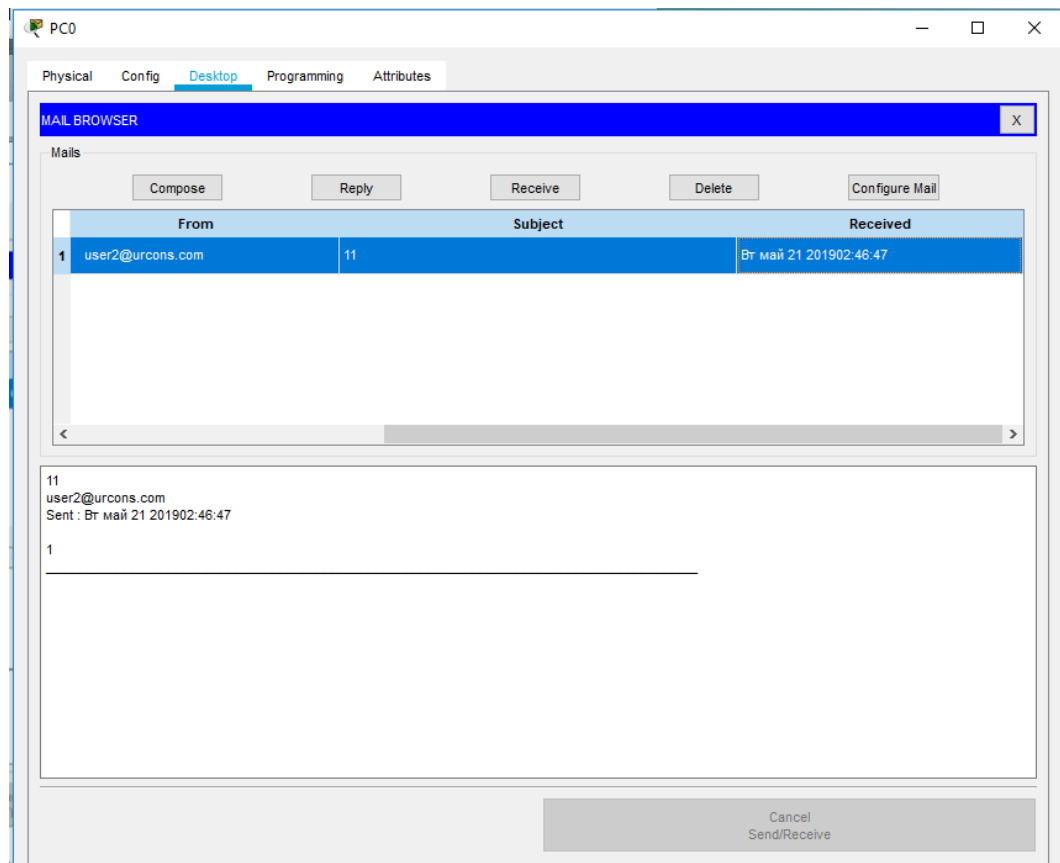


Рис. 9: Получение письма

В списке писем появилось, отправленное ранее, письмо. Также имеется дополнительная информация: дата отправки, протокол по которому письмо было получено, адрес сервера почты.

0.4.2 Проверка TFTP

На Router 2 была открыта консоль, в которой были выполнены следующие команды:

```

1 Router>enable
2 Router#show flash
3
4 System flash directory:
5 File Length Name/status
6 3 5571584 pt1000-i-mz.122-28.bin
7 2 28282 sigdef-category.xml
8 1 227537 sigdef-default.xml
9 [5827403 bytes used, 58188981 available, 64016384 total]
10 63488K bytes of processor board System flash (Read/Write)
11
12 Router#copy flash tftp
13 Source filename []? pt1000-i-mz.122-28.bin
14 Address or name of remote host []? 192.168.30.1
15 Destination filename [pt1000-i-mz.122-28.bin]? temp.file
16
17 Writing pt1000-i-mz.122-28.bin ...!!!!!!!!!!!!!!!!!!!!!!
18 [OK - 5571584 bytes]
19
20 5571584 bytes copied in 0.147 secs (8684467 bytes/sec)

```

Разберем действия:

1. Командой **enable** был совершен переход в привелегированный режим, можно заметить по символу решетки;
2. Командой **show flash** было выведено содержимое флеш-памяти, в данном случае это необходимо для тестовой загрузки по TFTP;

3. Командой **copy flash tftp** сообщаем о начале загрузке файла по tftp, где далее указывается файл(ы), tftp сервер для загрузки, а также новое имя файла(ов).

На TFTP сервере, в настройках TFTP появится выбранный ранее файл с указанным именем.

0.4.3 Проверка команды ping по адресу

Откроем на узле 192.168.20.4(сеть NET2) утилиту **Command Prompt**, в которой введем команды **ipconfig** и **ping** в которой укажем адрес 192.168.0.2(сеть NET0).

```
1 C:\>ipconfig
2 FastEthernet0 Connection:( default port)
3     Link-local IPv6 Address . . . . . : FE80::2E0:A3FF:FEA3:7605
4     IP Address . . . . . : 192.168.20.5
5     Subnet Mask . . . . . : 255.255.255.0
6     Default Gateway . . . . . : 192.168.20.1
7
8 C:\>ping 192.168.0.2
9 Pinging 192.168.0.2 with 32 bytes of data:
10 Reply from 192.168.0.2: bytes=32 time=1ms TTL=127
11 Reply from 192.168.0.2: bytes=32 time=1ms TTL=127
12 Reply from 192.168.0.2: bytes=32 time=1ms TTL=127
13 Reply from 192.168.0.2: bytes=32 time<1ms TTL=127
14
15 Ping statistics for 192.168.0.2:
16     Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
17 Approximate round trip times in milli-seconds:
18     Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Как видно из лога, команда пинг была успешна.

0.4.4 Проверка команды ping по доменному имени

Откроем на узле 192.168.20.2(сеть NET2) утилиту **Command Prompt**, в которой введем команды **ipconfig** и **ping** в которой укажем доменное имя **www.mypage.com**.

```
1 C:\>ipconfig
2 FastEthernet0 Connection:( default port)
3     Link-local IPv6 Address . . . . . : FE80::201:42FF:FE0B:D82B
4     IP Address . . . . . : 192.168.20.5
5     Subnet Mask . . . . . : 255.255.255.0
6     Default Gateway . . . . . : 192.168.20.1
7
8 C:\>ping www.urcons.com
9 Pinging 192.168.10.2 with 32 bytes of data:
10 Reply from 192.168.10.2: bytes=32 time<1ms TTL=126
11 Reply from 192.168.10.2: bytes=32 time=10ms TTL=126
12 Reply from 192.168.10.2: bytes=32 time=11ms TTL=126
13 Reply from 192.168.10.2: bytes=32 time=13ms TTL=126
14
15 Ping statistics for 192.168.10.2:
16     Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
17 Approximate round trip times in milli-seconds:
18     Minimum = 0ms, Maximum = 13ms, Average = 8ms
```

Как видно из лога, доменное имя было преобразовано в адрес, по которому и была произведена команда ping.

0.4.5 Проверка команды ping из изолированной сети

Откроем на узле 192.168.30.2(сеть NET3) утилиту **Command Prompt**, в которой введем команды **ipconfig** и **ping** в которой укажем доменное адрес 192.168.0.2(NET0).

```
1 C:\>ipconfig
2
3 FastEthernet0 Connection:( default port)
4
```

```
5      Link-local IPv6 Address . . . . .: FE80::200:CFF:FECC:E597
6      IP Address . . . . .: 192.168.30.2
7      Subnet Mask . . . . .: 255.255.255.0
8      Default Gateway . . . . .: 192.168.30.1
9
10 C:\>ping 192.168.0.2
11
12 Pinging 192.168.0.2 with 32 bytes of data:
13
14 Reply from 192.168.30.1: Destination host unreachable.
15 Reply from 192.168.30.1: Destination host unreachable.
16 Reply from 192.168.30.1: Destination host unreachable.
17 Reply from 192.168.30.1: Destination host unreachable.
18
19 Ping statistics for 192.168.0.2:
20     Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Как видно из лога, благодаря изоляции внешние сети недоступны.

0.5 Заключение

В данной работе был получен опыт по работе в **Cisco Packet Tracer**(CPT).

Построение и настройка были выполнены с помощью встроенных инструментов, которые в общем виде имитируют реальное оборудование. Если сравнивать построение сети например с VMware, то в нем настройка сети производится на конкретных системах, в то время как в CPT это было сделано на лишь приближенных к реальности устройствах. Однако, решения созданные CPT более легковесны как в настройке, так и в проектировании.

CPT будет полезен как новичкам, так и профессионалам.

Отличительной особенностью является то, что за любым пакетом можно наблюдать по-шагам, что может помочь в определении ситуации, почему сеть работает некорректно.

К недостаткам CPT можно отнести лишь то, что все действия ограничены, то есть установить на устройство какое-либо ПО или сервис которого нет в CPT, не предоставляется возможным.