SWINBURNE UNIVERSITY OF TECHNOLOGY

TNE20003 – Internet and Cybersecurity for Engineering Applications

Portfolio Task – Lab 5 Pass Task

Aims:

- To observe and investigate the functionality of the TCP and UDP protocols at the transport layer.
- Observe NAT at work and understand the translation process

Preparation:

- View "Transport Layer Services" & "NAT & DHCP"

Due Date:

- All tasks in this lab are to be completed and demonstrated to your Lab instructor preferably during or at the end of the current lab, but if you do not complete the tasks you may demonstrate it at the beginning of your next lab class.

Task 1.

Build the network provided in figure 1 with Cisco Packet Tracer

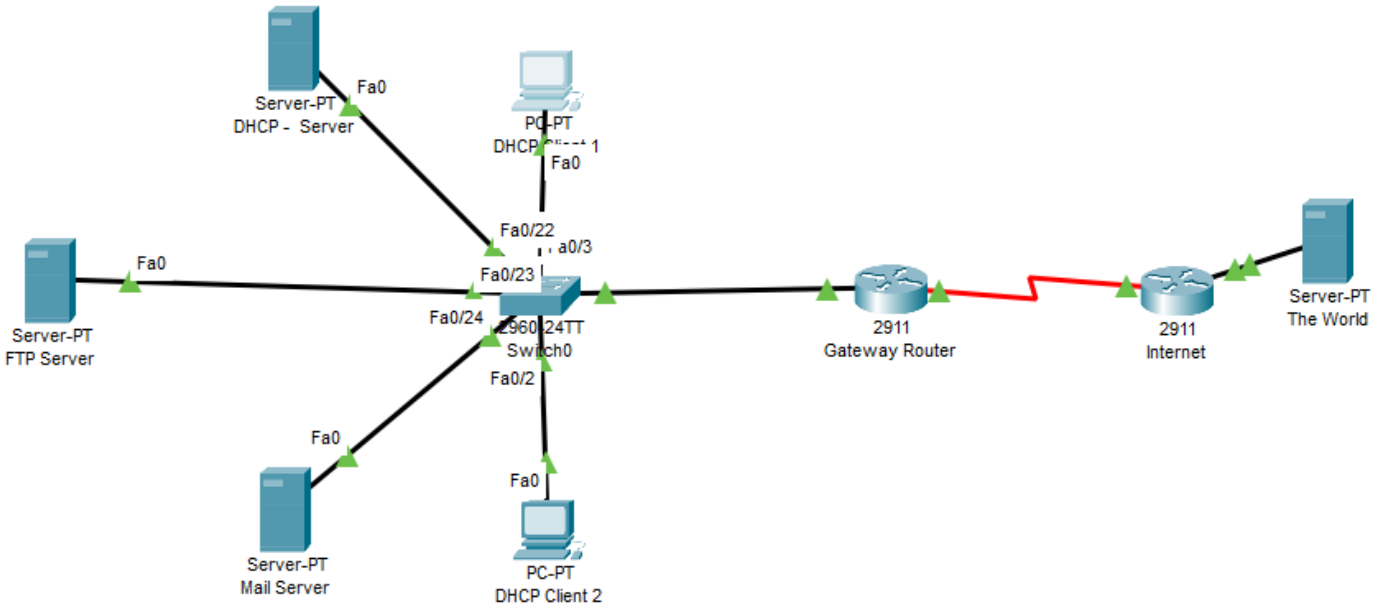
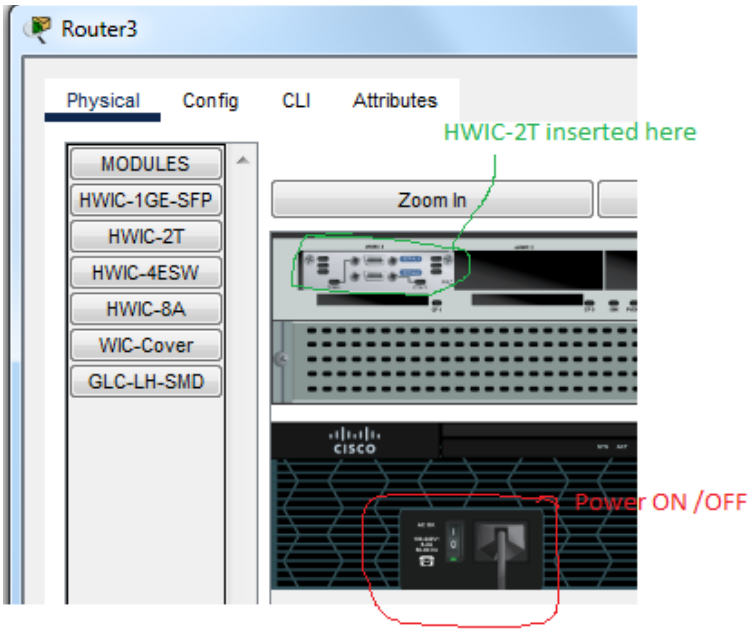


Figure 1

Task 2.

1. Implement the network shown in figure 1 above, labelling all devices as in the diagram.

   If you need help creating the diagram refer to the instructions in labs 1 & 2. Note that the serial link between **Gateway** router and **Internet** router cannot be connected until you put in HWIC-2T cards into the routers. See pic below for final connected view, but to get to this state you must follow these steps.



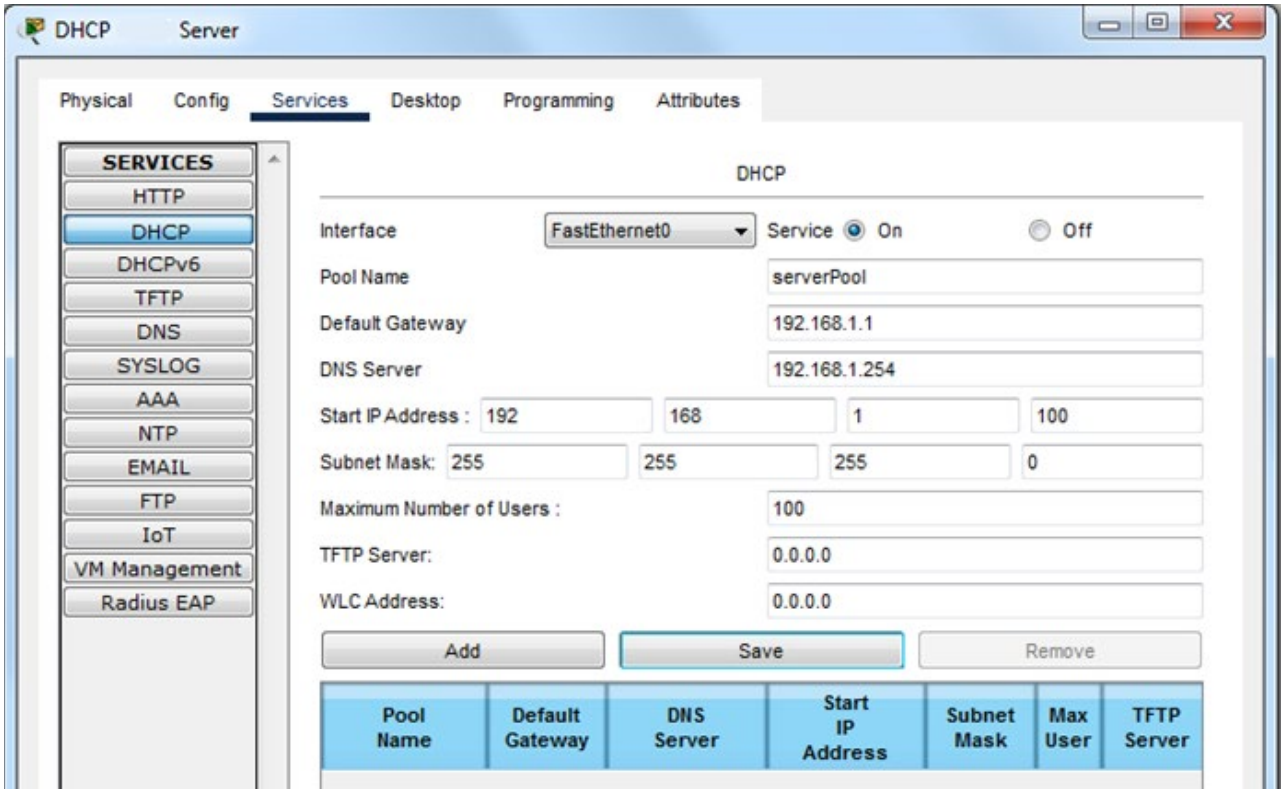
a. On both routers go the physical tab and turn off the power. Then click on the HWIC-2T card under the "modules" and place it as in the pic.

b. Now turn on the routers and then choose a serial cable from the cable section and connect the 2 routers. Notice the link lights will be red. This is because we have not configured or turned the interfaces on yet. In my picture they have been configured hence they are green.

Task 3.

1. Click on the **Gateway** router and assign it the address of 192.168.1.1/24
2. Click on the **Mail** server and assign it the address of 192.168.1.253/24
3. Click on the **DHCP** server and assign it the address of 192.168.1.254/24

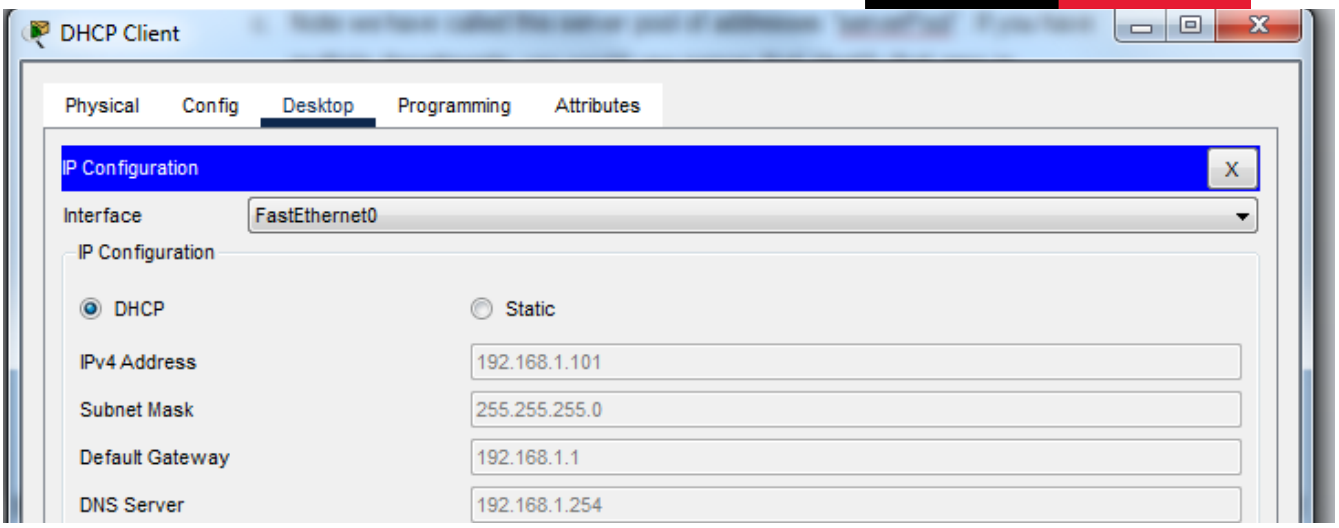
    a. Whilst in the DHCP server configure the DHCP service. Under the "**Services**" tab choose "**DHCP**" as in the pic below and fill out of the details as shown in the pic.



b. Note that we are setting up specific IP addresses to important servers which are not part of the range of IP addresses used in the DHCP pool. Our pool will start at 192.168.1.100 and we will allow a maximum of 100 users to get an IP at any one time. If user 101 requests an IP address they will be rejected until one of the used 100 IP addresses gets released.

c. Note we have called this server pool of IP addresses "**serverPool**". If you have multiple departments you might use names that identify those areas ie EngineeringPool, AccountingPool, …….

d. Now test to see if the server works. Go to **DHCP Client 1** and under the **Desktop** tab click on **IP Configuration** and then choose **DHCP** as in the picture below.



e. Observe that PC has the IP address of 192.168.1.1XX (where XX=00 to 99). In addition it has been given the identity of the **Default Gateway & DNS Server.**

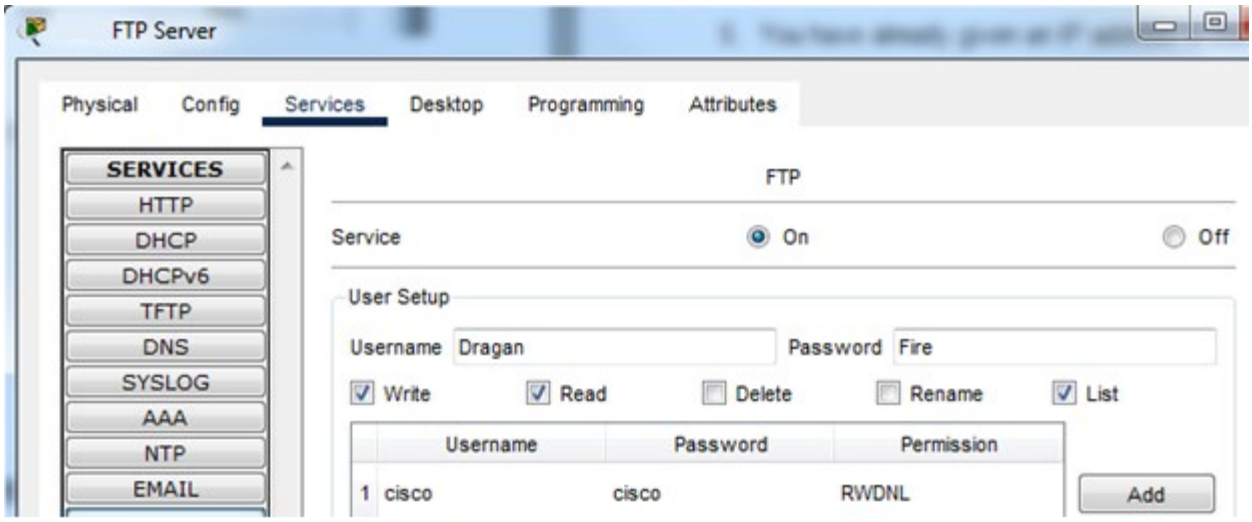
f. Go to the command prompt and ping to the **Mail** server to see you have connectivity. If it doesn't work troubleshoot to fix the problem.

g. Repeat **d-f** on **DHCP Client 2** and again verify that an IP address is assigned and that PC can ping all other devices in that LAN.

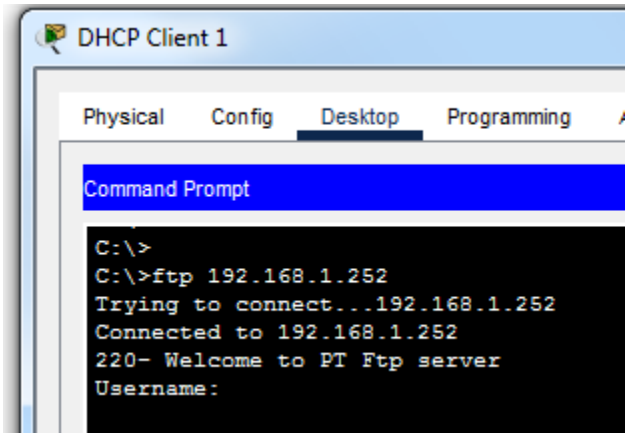
4. Click on the **FTP** server and assign it the address 192.168.1.252/24

a. Once the **FTP** server is addressed go to the "**Services**" tab and then click "**FTP**".

b. Ensure that the service is "ON" and then add a new user with the **username Dragan** and **password Fire** with the permissions to read, write and list files as in the picture below.



c. Now go to **DHCP Client 1** and open up a command prompt and in that prompt type "**ftp 192.168.1.252"**. You should see the following output.



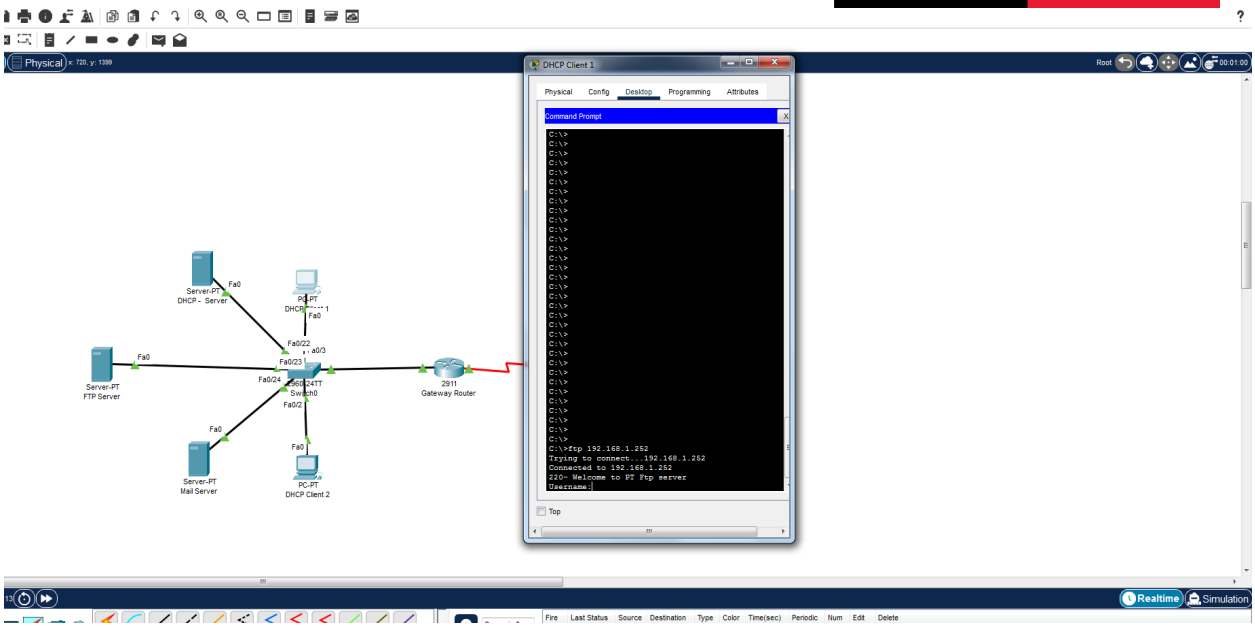
d. Enter the username and password that we created and you should be in. Type "**dir**" to see what files are available for copying.

e. If you want you can use the **"get"** to copy files from the ftp server onto your PC or the **"put"** command to upload files onto the ftp server. Try "getting" one file and observe that it appears in your PC.

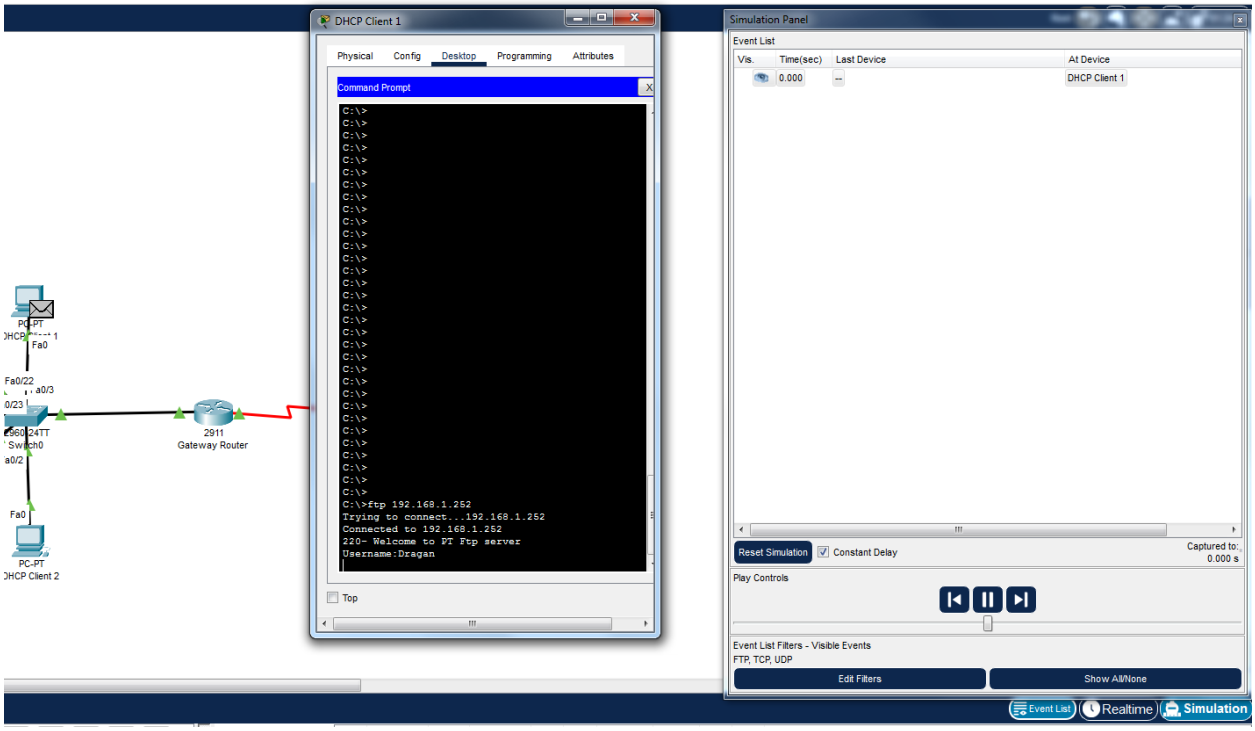
5. Observe the transport layer at work.

a. In PT click on Simulation and then under the filters section choose All/None until no filters are chosen. Then only activate the **FTP**, **TCP** and **UDP** filters. Then click the Realtime mode on PT.

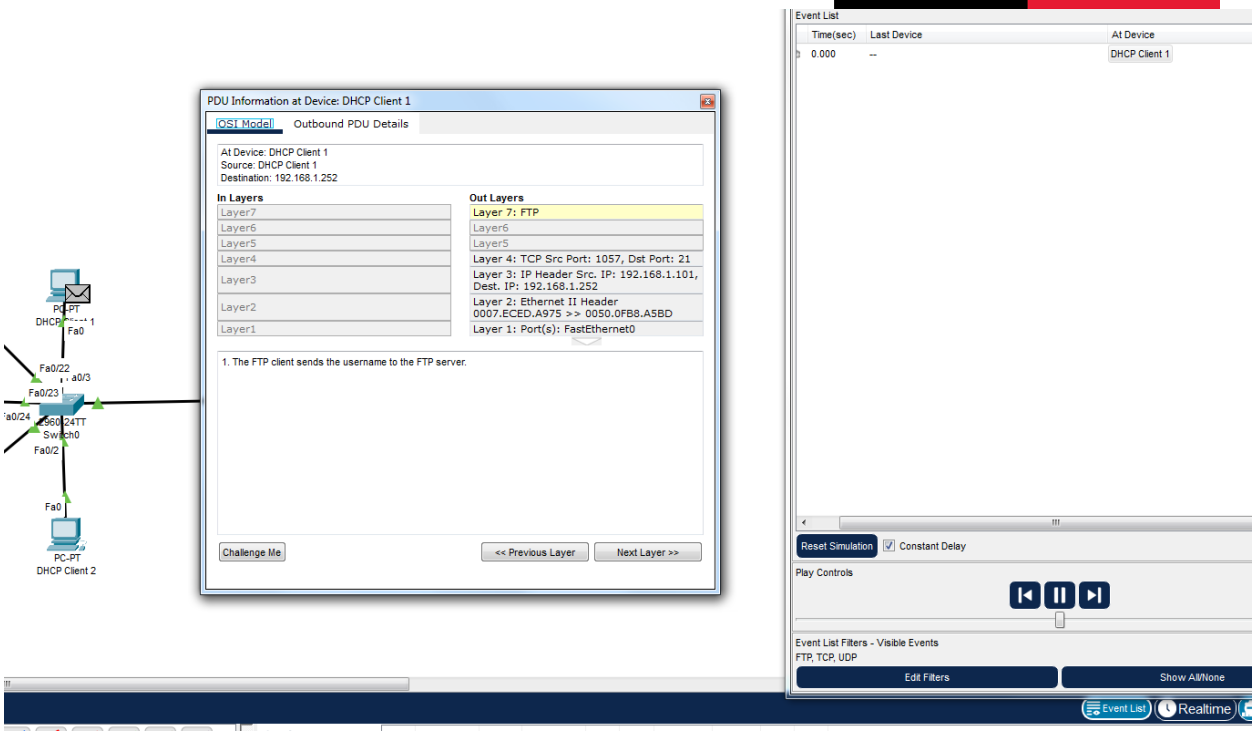
b. Go to **DHCP Client 1** and under the **Desktop** tab click on command prompt and type "**ftp 192.168.1.252"**. You should see the picture below. Notice the PC is waiting for you to enter the username and the PT is in Realtime mode. Now enter the simulation mode and then enter the username "**Dragan"**. Observe what happens in the events field.



c. After entering the username you should see an entry in the events list as shown below:



d. Now click on the envelope at the client PC or on the “DHCP Client 1” tab in the events list on the right. You should see the following:



e. Here you can see whether TCP or UDP is used as the transport protocol. Also you can see the port numbers.

f. What is the port number used for FTP? 21

g. Click on “Outbound PDU details”. What are the source (src) and destination (dst) MAC addresses and IP addresses? What are the src and dst port numbers?

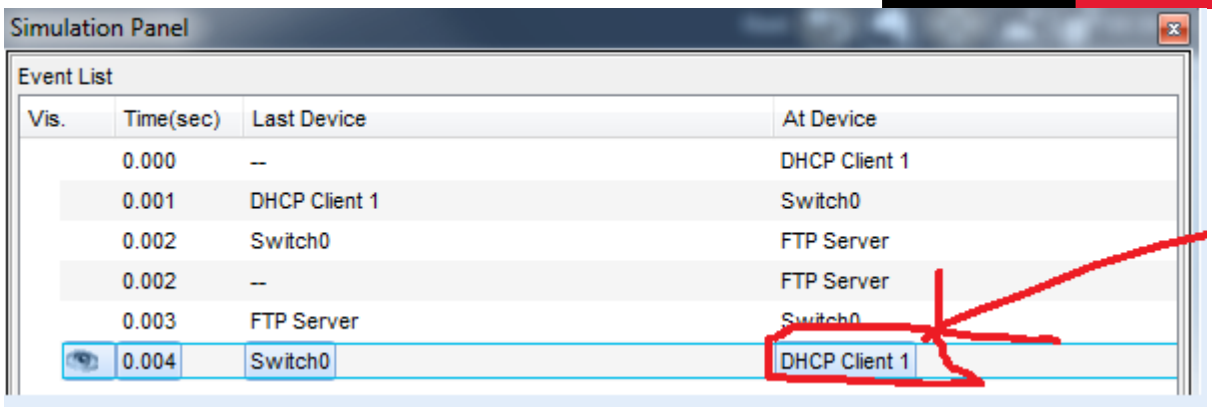
h. What is the sequence number and the acknowledgment number?

i. What do you see at the bottom of this window?

g. Source MAC address: 00D0.BA7D.9653.
Destination MAC address: 0006.2A33.C70E. Source port: 1030, Destination port: 21

h. Sequence number: 1,
Acknowledge number: 53

i. The FTP layer, which consist of username and password



k. Click on the packet circled in red. When it opens up what do you see? An OSI Layer

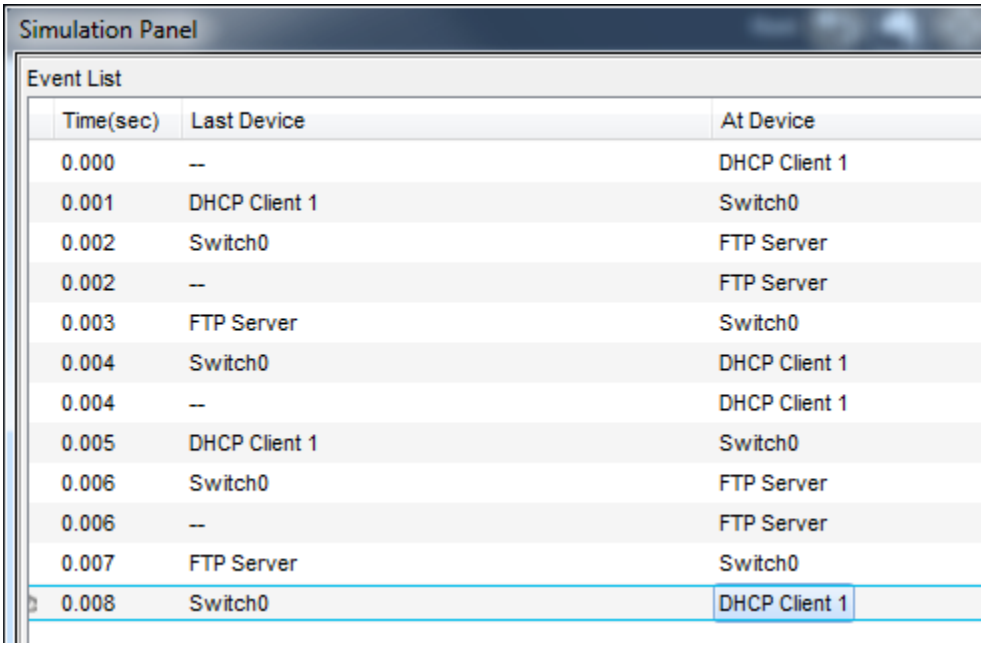
l. What has happened to the src and dst port numbers? Reversed

m. What are the sequence number and acknowledgment numbers? What can you say about them? Does it make sense? SEQ: 53, ACK: 38. The ACK number -> SEQ and ACK has new number

n. Scroll down to the bottom. What do you see? Response from FTP server with Code 331

o. Now go back to the client and put in the password.

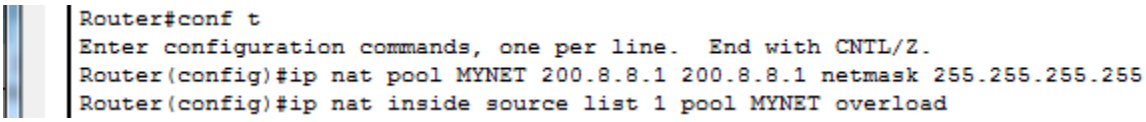
p. You will have to forward/advance the communication until you get the following output in the events list:



q. Click on the last event and see that you are logged in and ready to view/get/put files.

6. Next we will implement and investigate NAT.

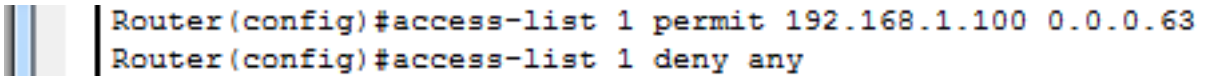
   a. On the **Gateway** router type in the following commands as in the picture below:



```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip nat pool MYNET 200.8.8.1 200.8.8.1 netmask 255.255.255.255
Router(config)#ip nat inside source list 1 pool MYNET overload
```

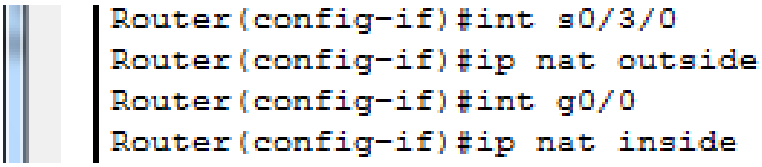
   This configures the real/global address we have bought to be used in the overload mode meaning that each of our connections will have a different port associated with each connection. “MYNET” is a word that you can choose to be anything you want and is only used locally in that router. The line containing the “source list” links to a filter, known as an ACL, which allows us to choose which IP addresses will be translated.

   b. Create the ACL to decide which IPs will be translated. See pic below.



```
Router(config)#access-list 1 permit 192.168.1.100 0.0.0.63
Router(config)#access-list 1 deny any
```

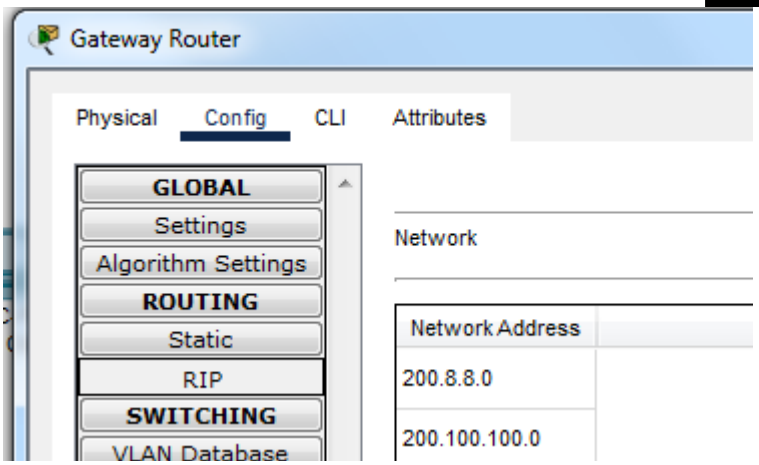
   c. Next we need to tell our system which addresses are private (inside) and which are public (outside). See pic below:



```
Router(config-if)#int s0/3/0
Router(config-if)#ip nat outside
Router(config-if)#int g0/0
Router(config-if)#ip nat inside
```

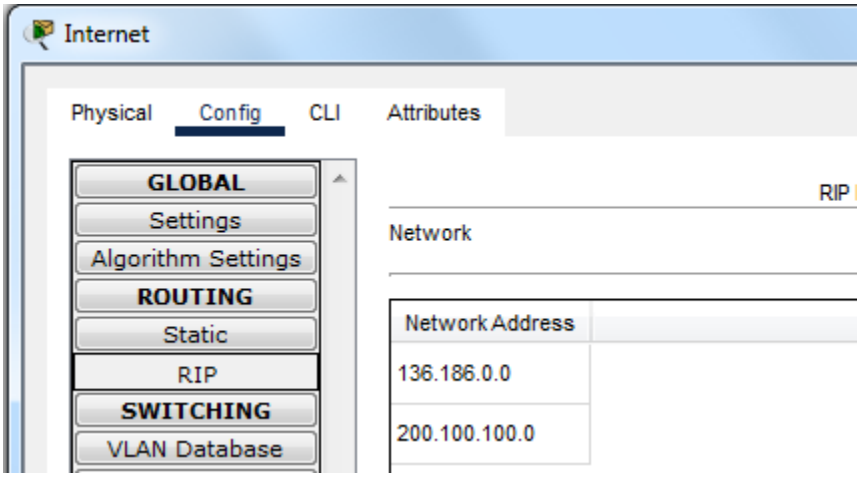
   d. Let’s set up the routing so that traffic from our network can make it’s way to **The World** server connected to the **Internet** router. Configure the serial interface S0/3/0 with ip address of 200.100.100.1/24.

   e. The global address we purchased is 200.8.8.1/32. This is what is used when traffic is sent out of our network. Hence this must be advertised to any neighbours that the **Gateway** router is connected to. Configure RIP routing as in the pic below:



f. Configure the G0/0 interface of the **Internet** router with ip address of 136.186.100.1/24. Then add **The World** server and connect to Fa0/0 with ip address of 136.186.100.2/24 using 136.186.100.1/24 as the gateway address.

g. Next configure the **Internet** router's serial interface S0/3/0 with the ip address of 200.100.100.2/24. Now configure router rip as shown below:

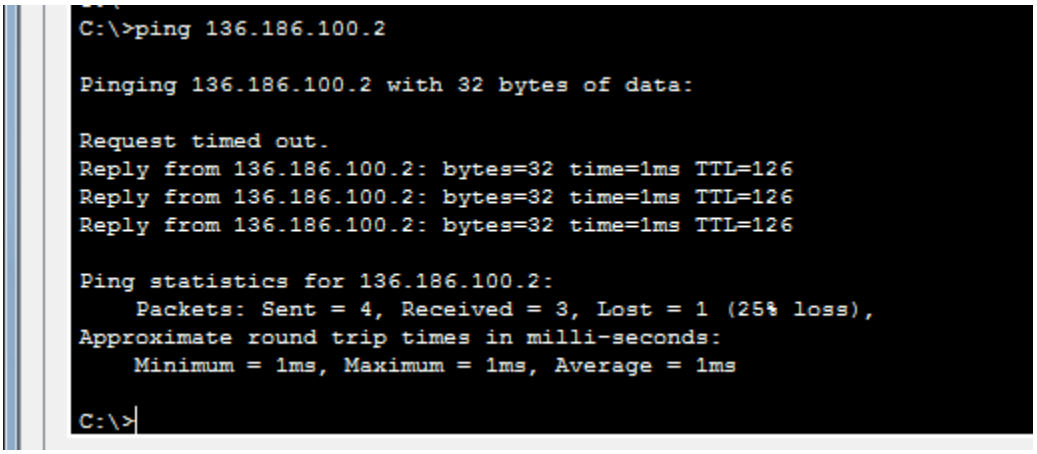


h. Lastly on the **Internet** router configure a static route pointing to the public address of 200.8.8.0/24 by issuing the command **ip route 200.8.8.0 255.255.255.0 200.100.100.1**.

i. With no interesting traffic there should NOT be any translations. Check by issuing the command **"sh ip nat tran"** under the global Router# prompt on the Gateway device. You should see this:

```
Router#sh ip nat tran
Router#
```

j. Now let's generate some traffic by pinging from one of the DHCP clients to **The World** server located at 136.186.100.2.



k. Let us check the translation table again by issuing the command **"sh ip nat tran" on the Gateway** router. What do you see???? It should be something similar to the pic below.

```
Router#sh ip nat tran
Pro  Inside global     Inside local       Outside local      Outside global
icmp 200.8.8.1:63      192.168.1.101:63   136.186.100.2:63   136.186.100.2:63
icmp 200.8.8.1:64      192.168.1.101:64   136.186.100.2:64   136.186.100.2:64
icmp 200.8.8.1:65      192.168.1.101:65   136.186.100.2:65   136.186.100.2:65
icmp 200.8.8.1:66      192.168.1.101:66   136.186.100.2:66   136.186.100.2:66
```

SAVE THIS FILE IF YOU WANT TO DO THE CREDIT OR DISTINCTION TASK & for lab 6 as well!!

~~~~~ End of Lab ~~~~~