NATIONAL UNIVERSITY OF COMPUTER & EMERGING SCIENCE
Computer Network Lab (CL3001)
Lab Session 11

Objective:

- Introduction to Wireless Network
- Importance of Wireless Technology
- Working of Wireless Network
- Configuration of Wireless Network
- Introduction to NAT & its Types
- Configuration of NAT
- Wireshark of NAT
- Lab Exercise

Wireless Network

1. Introduction to Wireless Network

A wireless network allows devices to stay connected to the network while roaming without the need for wires. Because access points amplify Wi-Fi signals, a computer may be far away from a router and still be connected to the network. When you connect to a Wi-Fi hotspot at a café or similar public area, you are connecting to that organization's wireless network.

The main difference between a wireless and a wired network is that a wired network requires wires to connect devices, such as laptops or desktop computers, to the Internet or another network. A wired network, as opposed to a wireless network, has numerous disadvantages. The primary disadvantage is that a router is permanently connected to your computer. The most common wired networks employ cables connected to an Ethernet port on the network router and a computer or other equipment on the other end.

2. Importance of Wireless:

However, delving into a specific technology at this point is getting ahead of the tale. Regardless of how the protocols are constructed or what sort of data they carry, wireless networks have some important advantages.

The most obvious benefit of wireless networking is mobility. Users of wireless networks can connect to existing networks and then roam freely. Because the phone connects the user via cell towers, a mobile phone user can travel kilometers in a single call.

Initially, mobile telephone was prohibitively expensive. Due to the exorbitant price, it was only used by highly mobile professionals such as sales managers and important executive decision-makers who needed to be accessible at any time and from any location. Mobile telephone, on the other hand, has proven to be a valuable service that is becoming increasingly popular.

Wireless networks often provide a lot of flexibility, which translates to quick installation. Wireless networks link users to an existing network using a variety of base stations.

3. Working of Wireless Network:

A wireless local area network (WLAN) connects a collection of computers in the same way that a wired network does. Because “wireless” does not require costly cabling, the major benefit is that it is generally easier, faster, and less expensive to set up.

Building a network by dragging cables over an office's walls and ceilings, on the other hand, may be time-consuming and costly. Even if you currently have a wired network, a wireless network might be a cost-effective method to extend or expand it.

Radio Frequency (RF) technology, a frequency related with radio wave transmission within the electromagnetic spectrum, is used to power wireless networks. When an RF current is sent into an antenna, it creates an electromagnetic field that can travel over space.

A wireless network's core is a mechanism known as an access point (AP). The fundamental function of an access point is to transmit a wireless signal that computers can detect and tune into. Because wireless networks are frequently linked to wired networks, access points frequently serve as a portal to the resources of the wired network, such as an Internet connection.

To connect to an access point and join a wireless network, computers must be equipped with wireless network adapters. These are usually incorporated into the device, but if not, any computer or notebook can be turned wireless-capable by connecting an add-on adapter to an empty expansion slot, USB port, or, in the case of notebooks, a PC card slot.

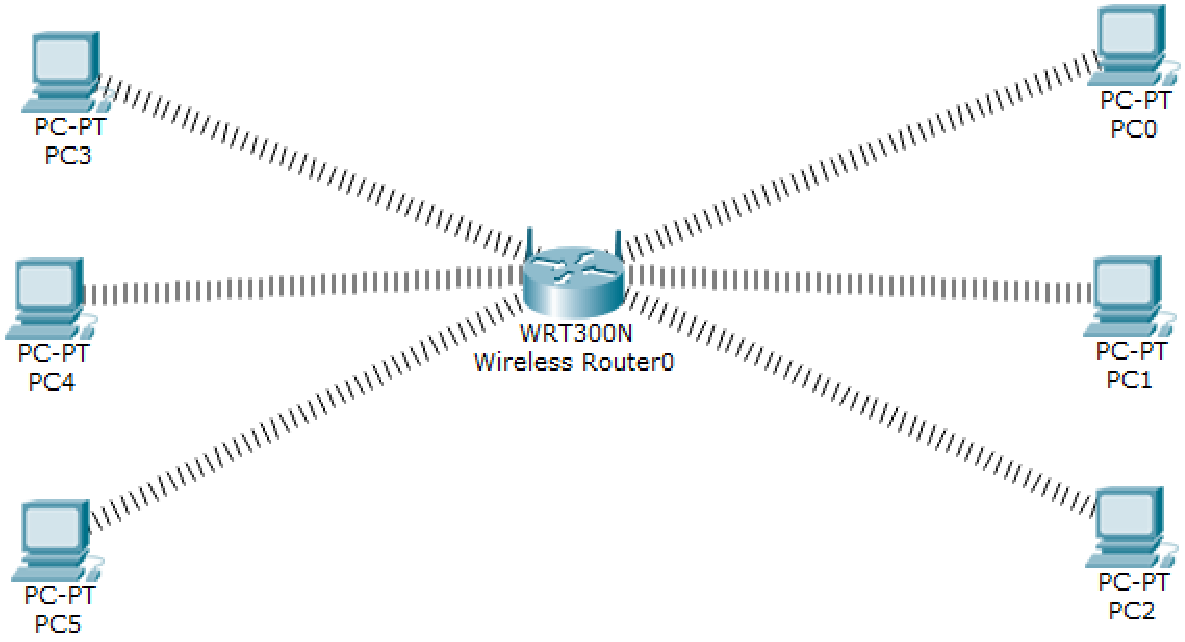


Fig-1: Wireless Network Topology

4. Configuration of Wireless Network:

The above topology mentioned in figure 1 we have six pc connected with Linksys Wireless routers.

1. DHCP is configured and enabled on Wireless router.
2. IP pool for DHCP is 192.168.0.100 to 192.168.0.150.
3. IP pool for DHCP is 192.168.0.100 to 192.168.0.150.
4. PC are configured to receive IP from DHCP Server.
5. No security is configured.
6. Default SSID is configured to Default.
7. Topology is working on infrastructure mode.

8. Default user name and password is admin.
9. IP of wireless is set to 192.168.0.1.

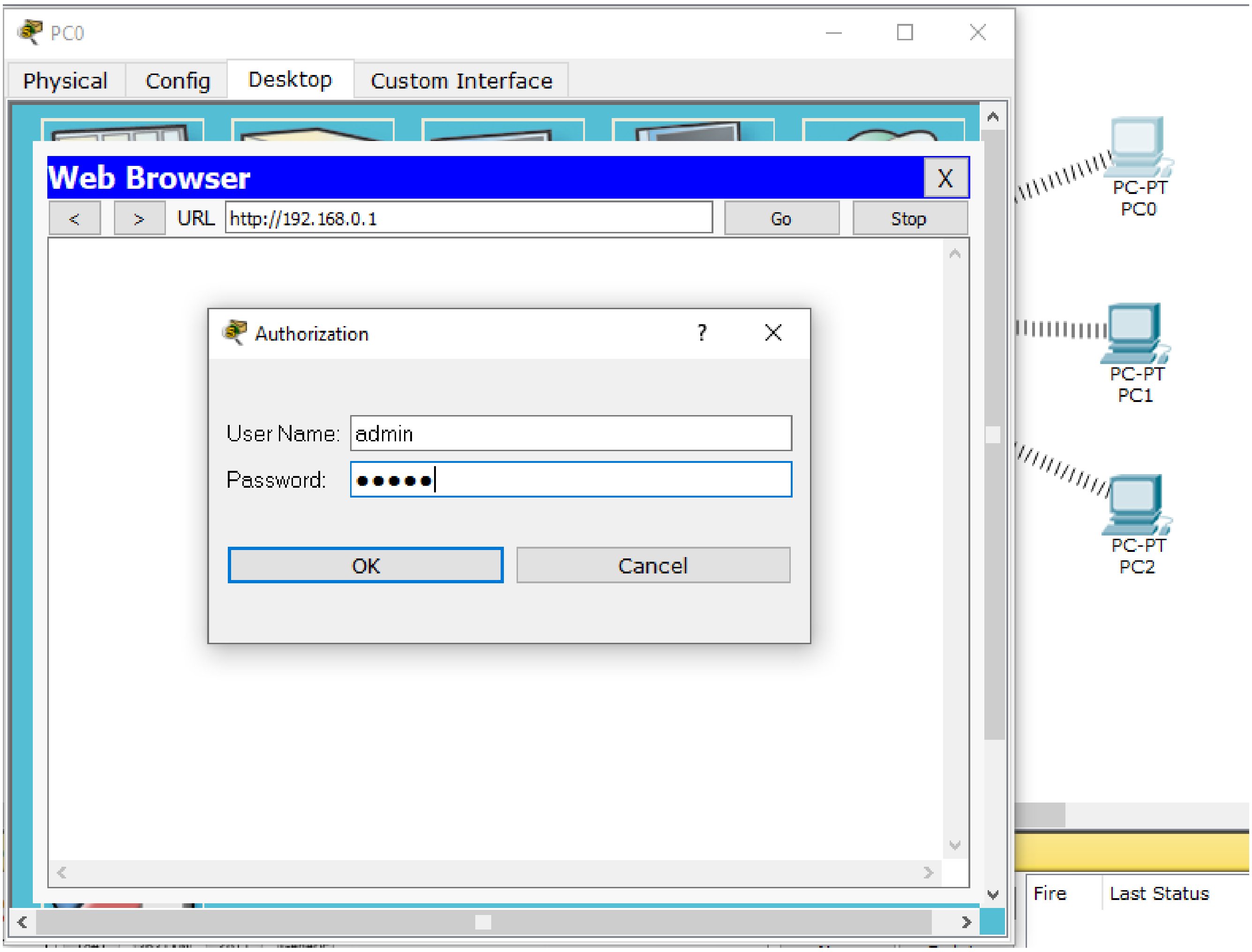
Now we perform some following tasks on the given above topology i.e., Figure 1:

- Configure Static IP on PC and Wireless Router
- Change SSID to Mother Network
- Change IP address of router and end devices
- Secure your network by configuring WAP key on Router
- Connect PC by using WAP key

To complete the above tasks, we will follow this step-by-step guide of how to configure wireless network

As given in question our network is running on 192.168.0.0 network and all PC's are DHCP clients and functioning properly. So, we will first connect to given Wireless router to turn off the DHCP Services.

Double click on PC and select Web Browser. As given in question IP of Wireless router is 192.168.0.1 so give it in Web browser and press enter, now it will ask for authentication which is also given in question. Default username is admin and password is also admin.



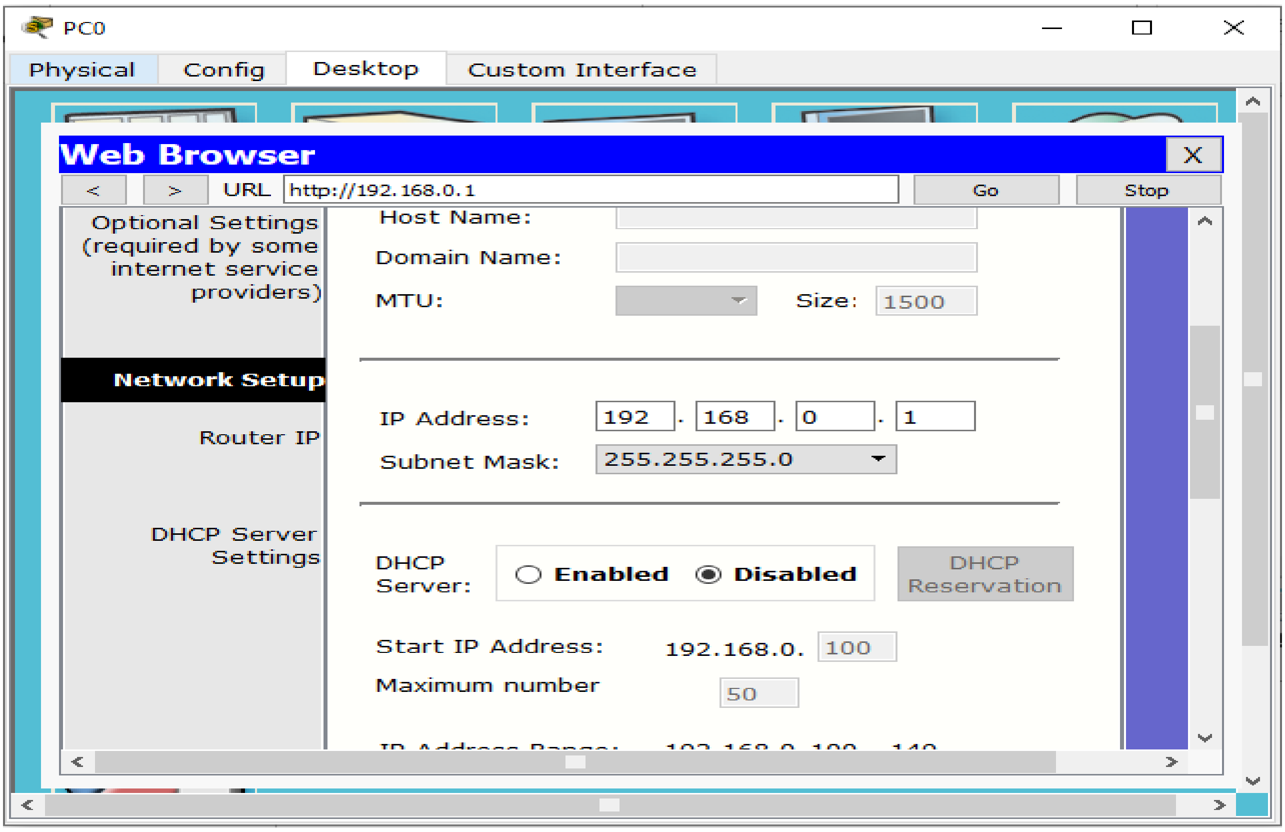
URL http://192.168.0.1

User Name: admin

Password: ●●●●●

Fig-2: Authentication using username & password

This will bring GUI mode of Wireless router. Scroll down screen to Network Step and Select Disable DHCP.



URL http://192.168.0.1

Optional Settings (required by some internet service providers)

Host Name:

Domain Name:

MTU: Size: 1500

Network Setup

Router IP

IP Address: 192 . 168 . 0 . 1

Subnet Mask: 255.255.255.0

DHCP Server Settings

DHCP Server: ○ Enabled ● Disabled

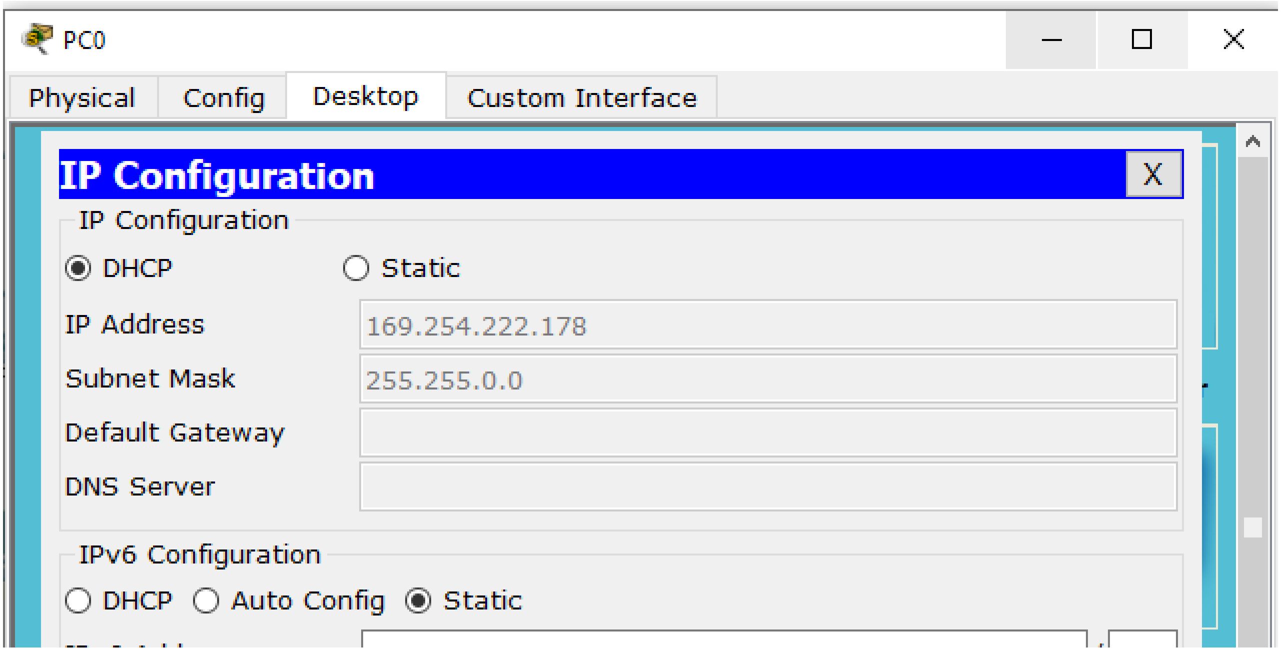
DHCP Reservation

Start IP Address: 192.168.0. 100

Maximum number 50

Fig-3: Select disabled option after authentication

Go in end of page and click on save setting this will save setting click on continue for further setting



IP Configuration

● DHCP ○ Static

IP Address 169.254.222.178

Subnet Mask 255.255.0.0

Default Gateway

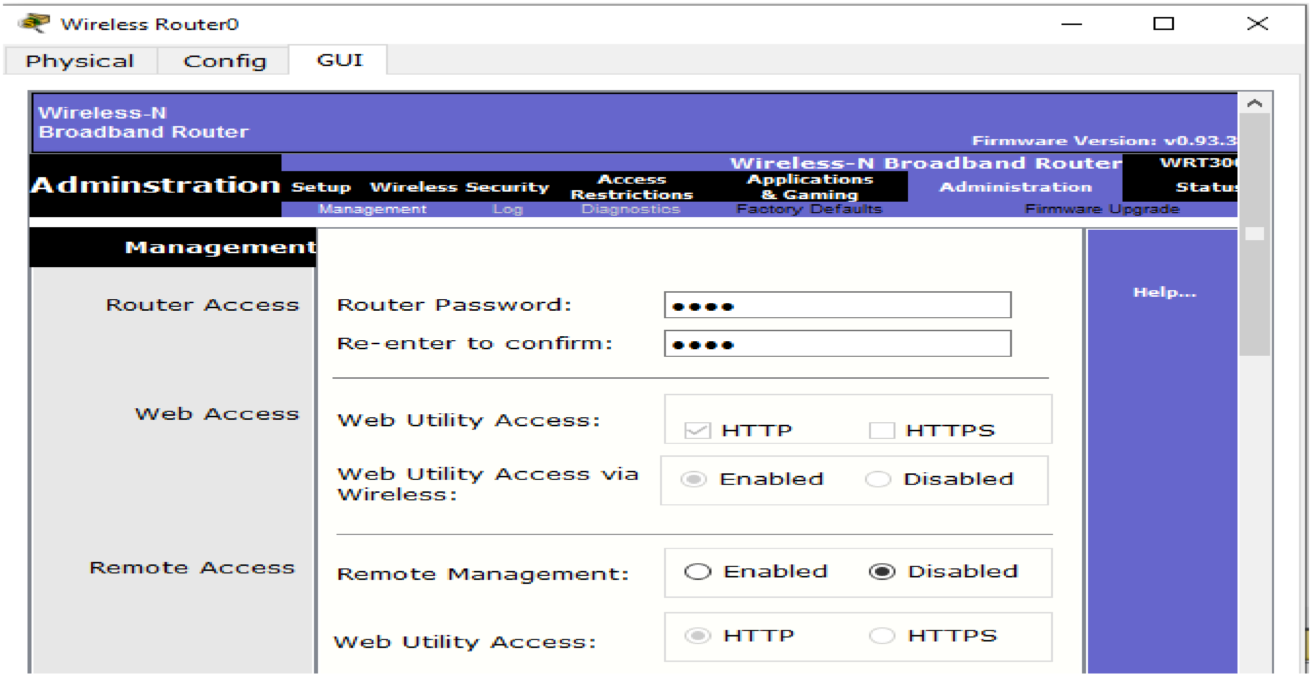
DNS Server

IPv6 Configuration

○ DHCP ○ Auto Config ● Static

Fig-4: After disabling DHCP, APIPA address is visible

Move to Router directly, select Administration from top Manu and change password to test and go in the end of page and Click on Save Setting.



Router Access

Router Password: ••••

Re-enter to confirm: ••••

Web Access

Web Utility Access: ☑ HTTP ☐ HTTPS

Web Utility Access via Wireless: ● Enabled ○ Disabled

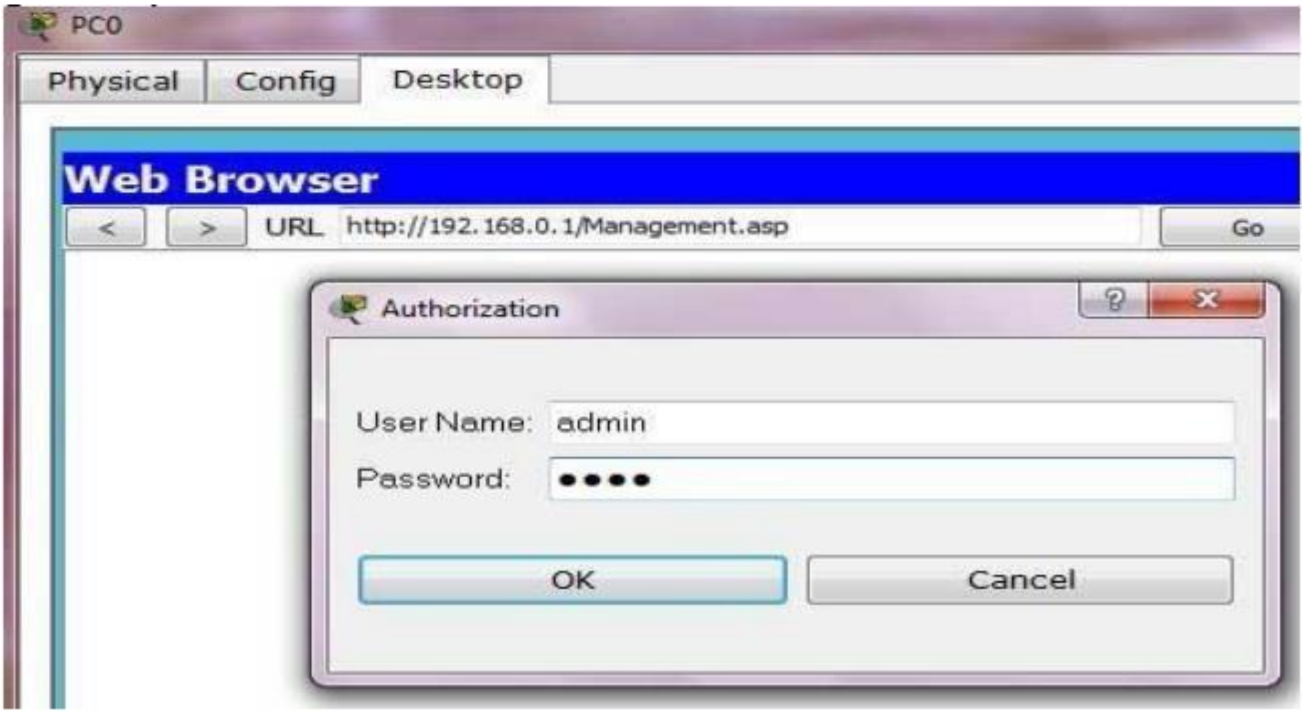
Remote Access

Remote Management: ○ Enabled ● Disabled

Web Utility Access: ● HTTP ○ HTTPS

Fig-5: Changing the default password

Click on continue for further setting. This time it will ask you to authenticate again give new password test this time



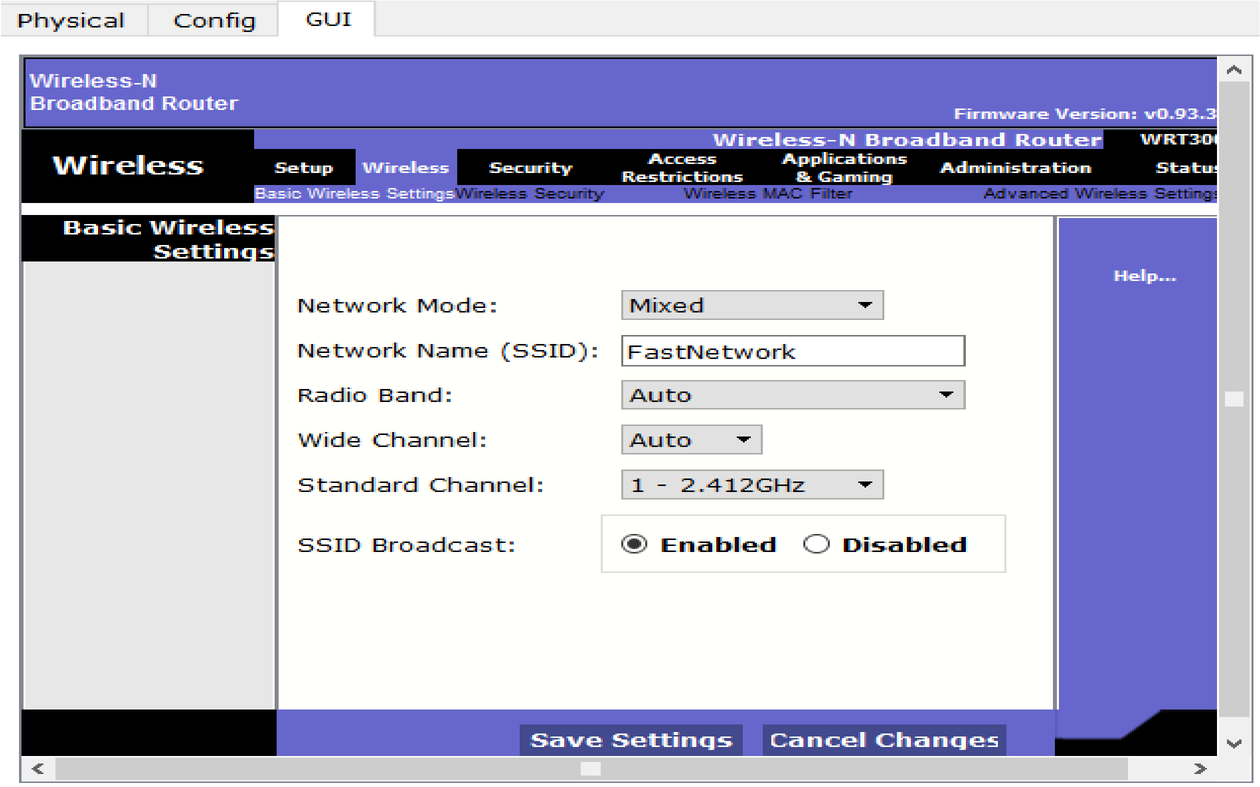
URL http://192.168.0.1/Management.asp

User Name: admin

Password: ••••

Fig-6: Authentication of the user with new password

Now click on wireless tab and set default SSID to FastNetwork.



Network Mode: Mixed

Network Name (SSID): FastNetwork

Radio Band: Auto

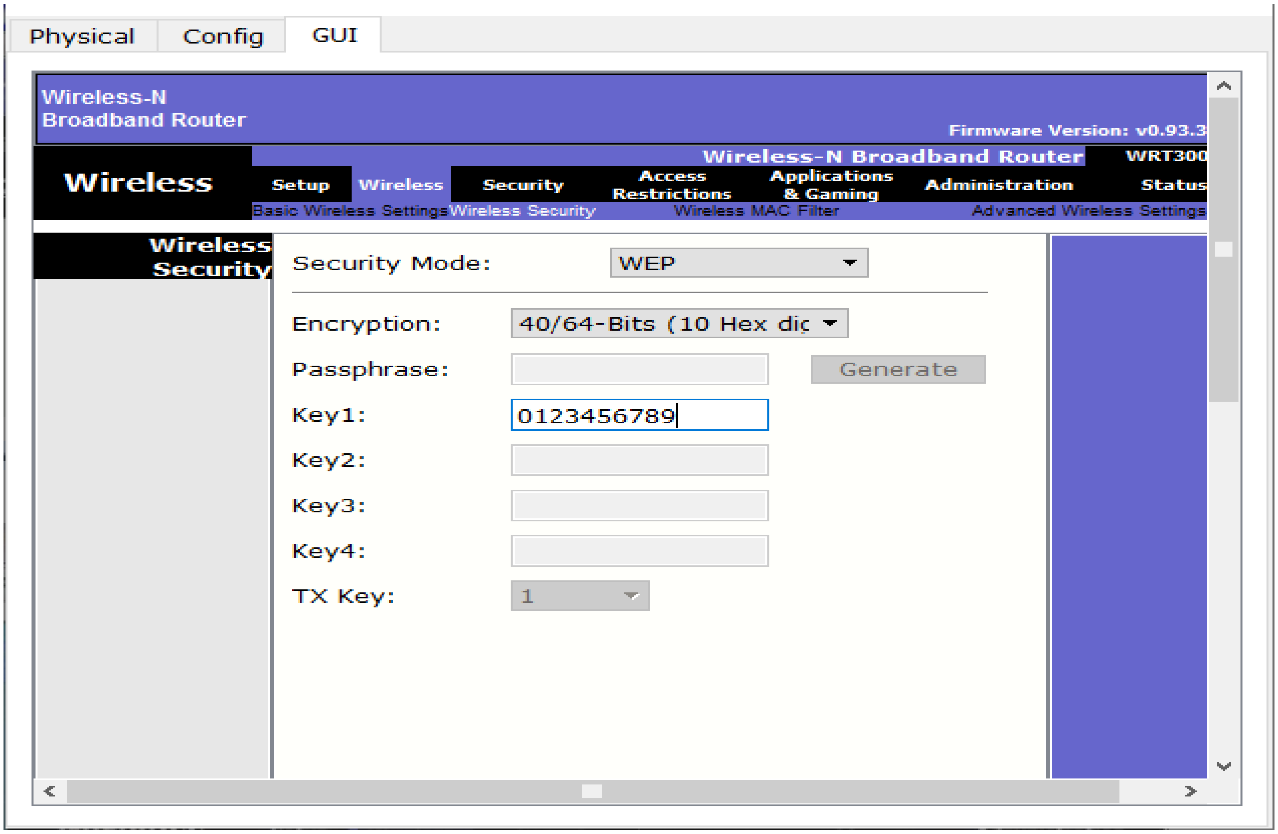
Wide Channel: Auto

Standard Channel: 1 - 2.412GHz

SSID Broadcast: ● Enabled ○ Disabled

Fig-7: Changing the SSID

Now Select wireless security and change Security Mode to WEP.



Security Mode: WEP

Encryption: 40/64-Bits (10 Hex dic

Passphrase:

Key1: 0123456789

Key2:

Key3:

Key4:

TX Key: 1

Fig-8: Setting WEP Key

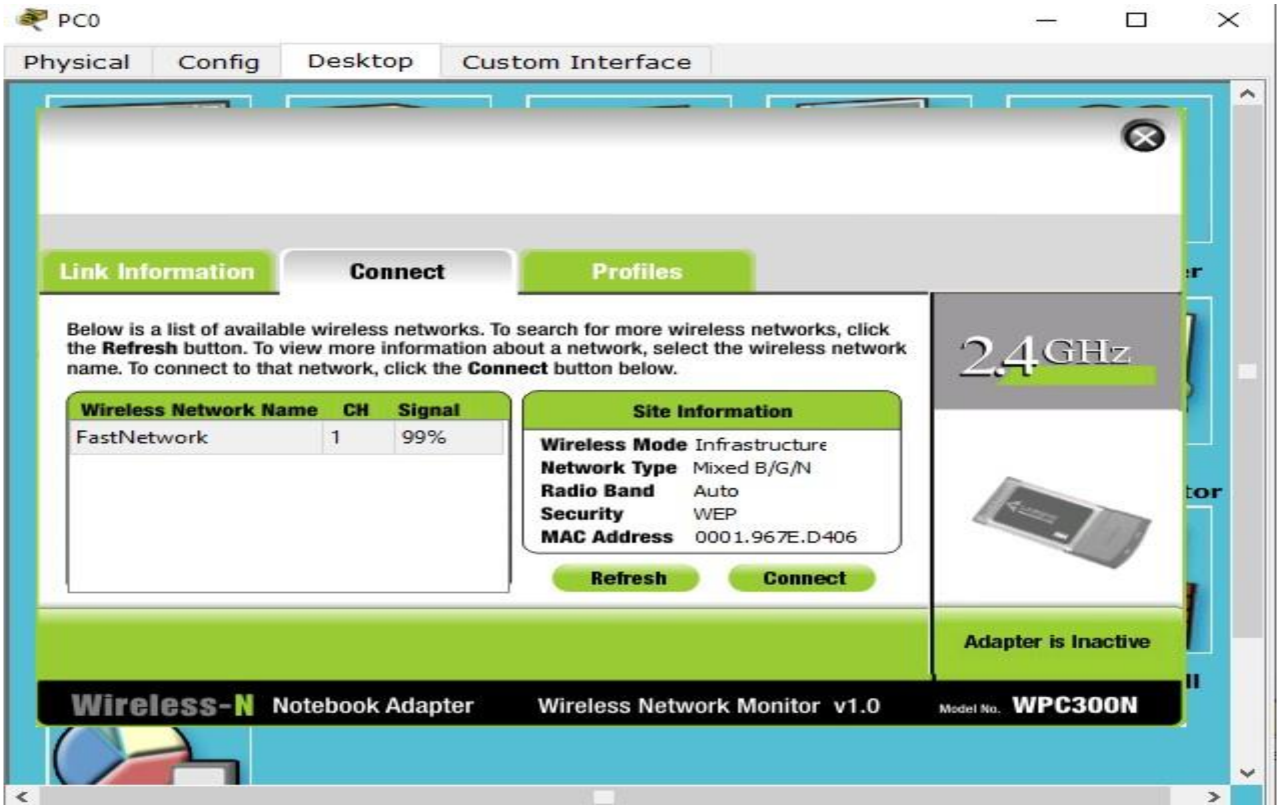
Again, go in the end of page and Click on Save Setting.

Now we have completed all given task on Wireless router. Now configure the static IP on all three PC's Double clicks on pc select Desktop tab click on IP configuration select Static IP and set IP as given below:

PC	IP	Subnet Mask	Default Gateway
PC0	192.168.0.2	255.255.255.0	192.168.0.1
PC1	192.168.0.3	255.255.255.0	192.168.0.1
PC2	192.168.0.4	255.255.255.0	192.168.0.1
PC3	192.168.0.5	255.255.255.0	192.168.0.1
PC4	192.168.0.6	255.255.255.0	192.168.0.1
PC5	192.168.0.7	255.255.255.0	192.168.0.1

Table-1: PC IP Addresses

Now it's time to connect PC's from Wireless router. To do so click PC select Desktop click on PC Wireless.



Below is a list of available wireless networks. To search for more wireless networks, click the **Refresh** button. To view more information about a network, select the wireless network name. To connect to that network, click the **Connect** button below.

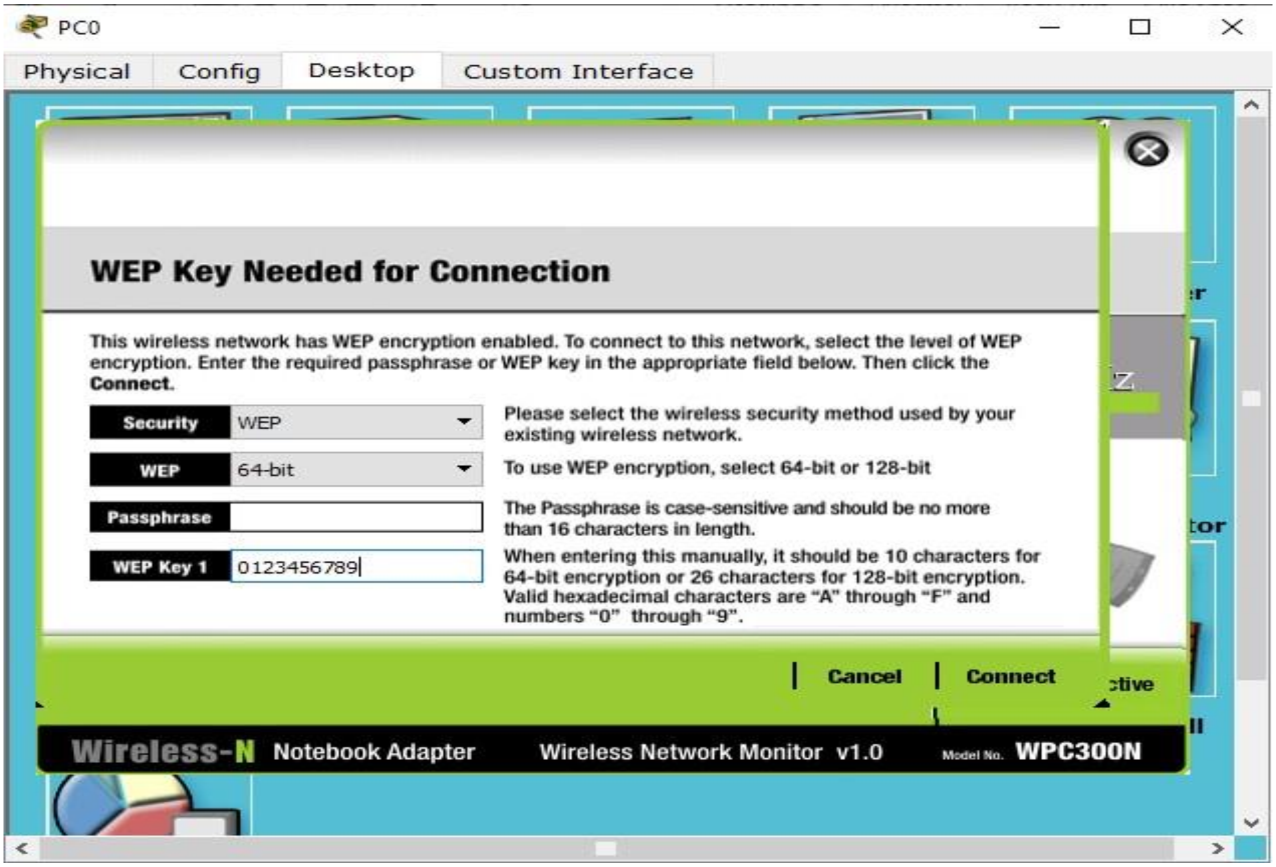
Wireless Network Name	CH	Signal
FastNetwork	1	99%

Site Information

Wireless Mode	Infrastructure
Network Type	Mixed B/G/N
Radio Band	Auto
Security	WEP
MAC Address	0001.967E.D406

Fig-9: Connecting to Network

Click on connect tab and click on Refresh button. It will ask for WEP key insert 0123456789 and click connect.



WEP Key Needed for Connection

This wireless network has WEP encryption enabled. To connect to this network, select the level of WEP encryption. Enter the required passphrase or WEP key in the appropriate field below. Then click the **Connect**.

Security: WEP — Please select the wireless security method used by your existing wireless network.

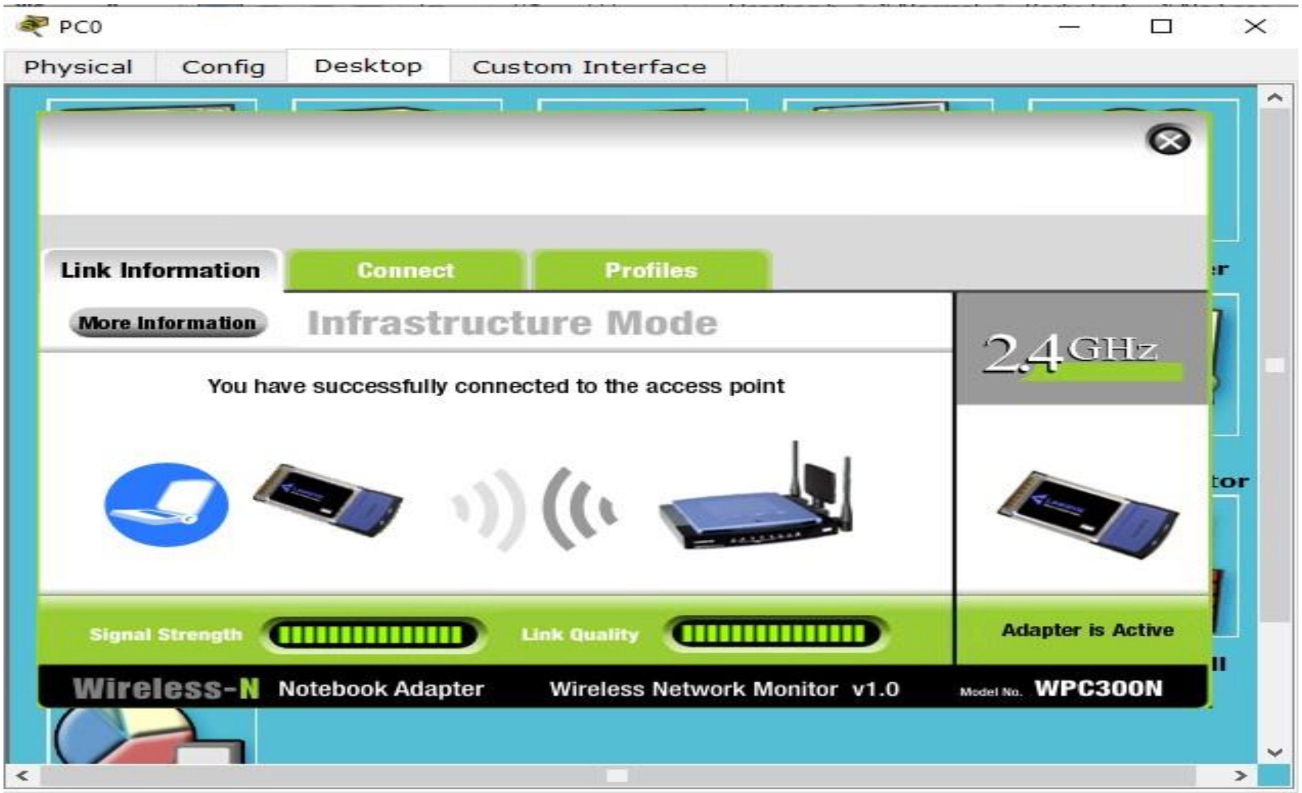
WEP: 64-bit — To use WEP encryption, select 64-bit or 128-bit

Passphrase: — The Passphrase is case-sensitive and should be no more than 16 characters in length.

WEP Key 1: 0123456789 — When entering this manually, it should be 10 characters for 64-bit encryption or 26 characters for 128-bit encryption. Valid hexadecimal characters are "A" through "F" and numbers "0" through "9".

Fig-10: Entering WEP Key

It will connect you with wireless router as shown in figure 11



Infrastructure Mode

You have successfully connected to the access point

Adapter is Active

Fig-11: Connected to the wireless network

NAT

5. Introduction to NAT & Its Types:

Network Address Translation (NAT) is a mechanism by which a device modifies a packet's TCP/IP address/port number and maps the IP address from one realm to another (usually from private IP address to public IP address and vice versa). This is accomplished by the NAT device allocating a temporary port number on the public side of the NAT when forwarding outbound packets from the internal host to the Internet, maintaining this mapping for a predetermined period of time, and forwarding inbound packets received from the Internet on this public port back to the internal host.

NAT devices are used to avoid the exhaustion of IPv4 address space by allowing multiple hosts to share a single public/Internet address. Also due to its mapping nature (i.e., a mapping can only be created by a transmission from an internal host), NAT device is preferred to be installed even when IPv4 address exhaustion is not a problem (for example when there is only one host at home), to provide some sort of security/shield for the internal hosts against threats from the Internet.

Despite the fact that NAT provides some shields for the internal network, one must distinguish NAT solution from firewall solution. NAT is not a firewall solution. A firewall is a security solution designed to enforce the security policy of an organization, while NAT is a connectivity solution to allow multiple hosts to use a single public IP address. Understandably both functionalities are difficult to separate at times, since many (typically consumer) products claims to do both with the same device and simply label the device a “NAT box”. But we do want to make this distinction rather clear, as PJNATH is a NAT traversal helper and not a firewall bypass solution (yet).

Following are the types of NAT.

Static NAT (Network Address Translation)- Static NAT (Network Address Translation) is one-to-one mapping of a private IP address to a public IP address. Static NAT (Network Address Translation) is useful when a network device inside a private network needs to be accessible from internet.

Dynamic NAT (Network Address Translation)- Dynamic NAT can be defined as mapping of a private IP address to a public IP address from a group of public IP addresses called as NAT pool. Dynamic NAT establishes a one-to-one mapping between a private IP address to a public IP address. Here the public IP address is taken from the pool of IP addresses configured on the end NAT router. The public to private mapping may vary based on the available public IP address in NAT pool.

PAT (Port Address Translation)- Port Address Translation (PAT) is another type of dynamic NAT which can map multiple private IP addresses to a single public IP address by using a technology known as Port Address Translation.

6. Configuration of NAT:

1. Static NAT Configuration:

Static NAT is used to do a one-to-one mapping between an inside address and an outside address. Static NAT also allows connections from an outside host to an inside host. Usually, static NAT is used for servers inside your network. For example, you may have a web server with the inside IP address 192.168.0.10 and you want it to be accessible when a remote host makes a request to 209.165.200.10. For this to work, you must do a static NAT mapping between those to IPs. In this example, we will use the Fast Ethernet 0/1 as the inside NAT interface, the interface connecting to our network, and the Serial 0/0/0 interface as the outside NAT interface, the one connecting to our service provider.

Working Step on Router:

```
Router(config)#ip nat inside source static 192.168.0.10 209.165.200.10
Router(config)#interface FastEthernet 0/1
Router(config-if)#ip nat inside
Router(config-if)#interface Serial 0/0/0
Router(config-if)#ip nat outside
```

2. Dynamic NAT Configuration:

Dynamic NAT is used when you have a “pool” of public IP addresses that you want to assign to your internal hosts dynamically. Don’t use dynamic NAT for servers or other devices that need to be accessible from the Internet. In this example, we will define our internal network as 192.168.0.0/24. We also have the pool of public IP addresses from 209.165.200.226 to 209.165.200.240 and our assigned netmask is 255.255.255.224. When you configure dynamic NAT, you have to define an ACL to permit only those addresses that are allowed to be translated.

Working Steps on Router:

```
Router(config)#ip nat pool NAT-POOL 209.165.200.226 209.165.200.240 netmask 255.255.255.224
Router(config)#access-list 1 permit 192.168.0.0 0.255.255.255
Router(config)#ip nat inside source list 1 pool NAT-POOL
Router(config)#interface FastEthernet 0/1
Router(config-if)#ip nat inside Router
(config-if)#interface Serial 0/0/0
Router(config-if)#ip nat outside
```

3. NAT Overload (PAT) Configuration:

NAT Overload, sometimes also called PAT, is probably the most used type of NAT. You can configure NAT overload in two ways, depending on how many public IP address you have available. The first case, and one of the most often seen cases, is that you have only one public IP address allocated by your ISP. In this case, you map all your inside hosts to the available IP address. The configuration is almost the same as for dynamic NAT, but this time you specify the outside interface instead of a NAT pool.

Working Steps on Router:

```
Router(config)#access list 1 permit 192.168.0.0 0.255.255.255
Router(config)#ip nat inside source list 1 interface serial 0/0/0 overload
Router(config)#interface FastEthernet 0/1
Router(config-if)#ip nat inside
Router(config-if)#interface Serial 0/0/0
Router(config-if)#ip nat outside
```

4. Example:

In this example we configure NAT overload (PAT) on the router which is located in Multan and static NAT is configured on Islamabad router. A simple topology is shown in figure 12.

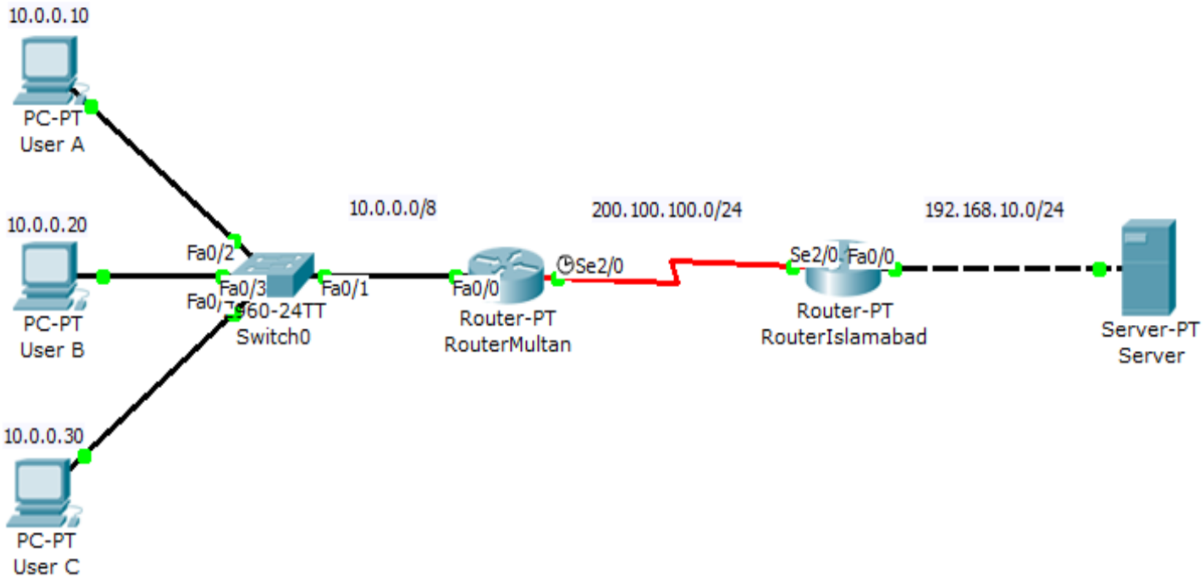


Fig-12: Network topology scenario for NAT

Assigning IP address to Multan router

```
Router>enable
Router# configure terminal
Router(config)#
Router(config)#hostname R1
R1(config)#interface FastEthernet0/0
R1(config-if)#ip address 10.0.0.1 255.0.0.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface Serial0/0/0
R1(config-if)#ip address 100.0.0.1 255.0.0.0
R1(config-if)#clock rate 64000
R1(config-if)#bandwidth 64
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#
```

Assigning IP address to Islamabad router

```
Router>enable
Router#configure terminal
Router(config)#hostname R2
R2(config)#interface FastEthernet0/0
R2(config-if)#ip address 192.168.1.1 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface Serial0/0/0
R2(config-if)#ip address 100.0.0.2 255.0.0.0
R2(config-if)#no shutdown
R2(config-if)#exit
```

Configuring NAT Overload (PAT) on router Multan

```
R1>enable
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#access-list 1 permit 10.0.0.10 0.0.0.0
R1(config)#access-list 1 permit 10.0.0.20 0.0.0.0
R1(config)#access-list 1 deny any
R1(config)#ip nat pool ccna 50.0.0.1 50.0.0.1 netmask 255.0.0.0
R1(config)#ip nat inside source list 1 pool ccna overload
R1(config)#interface FastEthernet 0/0
R1(config-if)#ip nat inside
R1(config-if)#exit
R1(config)#interface Serial 0/0/0
R1(config-if)#ip nat outside
R1(config-if)#exit
```

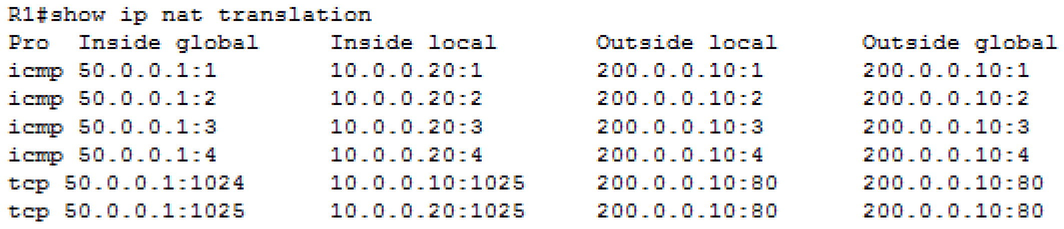
Configuring Static NAT on router Islamabad

```
R2>enable
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ip nat inside source static 192.168.1.10 200.0.0.10
R2(config)#interface Serial 0/0/0
R2(config-if)#ip nat outside
R2(config-if)#exit
R2(config)#interface FastEthernet 0/0
R2(config-if)#ip nat inside
R2(config-if)#exit
R2(config)#
```

Configuring static route on routers

```
R1(config)#ip route 200.0.0.0 255.255.255.0 100.0.0.2
R2(config)#ip route 50.0.0.0 255.0.0.0 100.0.0.1
```

Now ping server from a PC or open website through web browser using 200.0.0.10 IP address. To check the connectivity after configuring NAT. Use show “**ip nat translation command”** to verify NAT implementation on router.



```
R1#show ip nat translation
Pro  Inside global      Inside local       Outside local      Outside global
icmp 50.0.0.1:1         10.0.0.20:1        200.0.0.10:1       200.0.0.10:1
icmp 50.0.0.1:2         10.0.0.20:2        200.0.0.10:2       200.0.0.10:2
icmp 50.0.0.1:3         10.0.0.20:3        200.0.0.10:3       200.0.0.10:3
icmp 50.0.0.1:4         10.0.0.20:4        200.0.0.10:4       200.0.0.10:4
tcp 50.0.0.1:1024       10.0.0.10:1025     200.0.0.10:80      200.0.0.10:80
tcp 50.0.0.1:1025       10.0.0.20:1025     200.0.0.10:80      200.0.0.10:80
```

Fig-13: NAT information of Router 1 (Multan)

7. Wireshark of NAT:

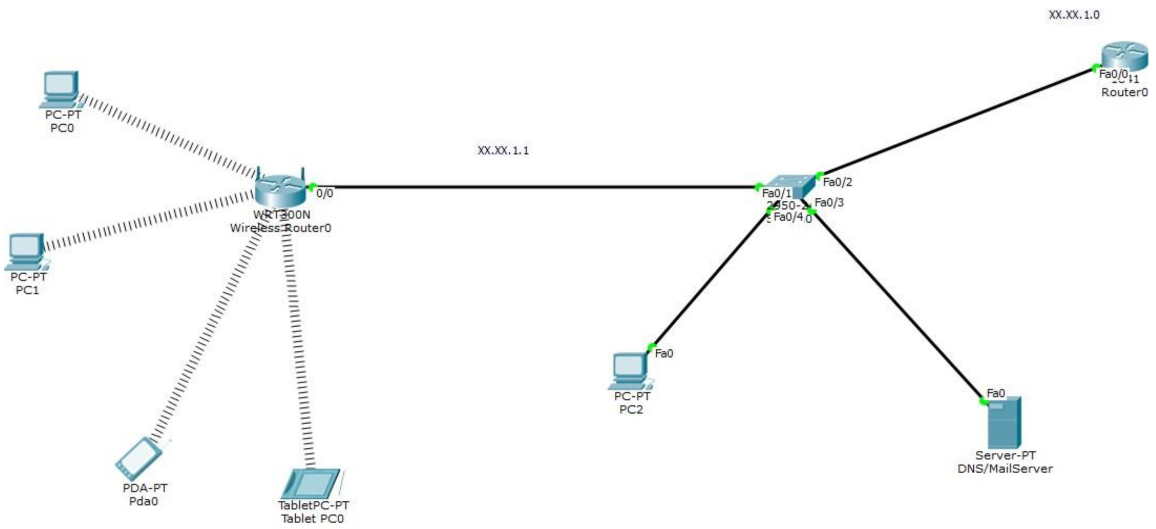
In this section, we'll capture packets from a simple web request from a client PC in a home network to a www.google.com server. Within the home network, the home network router provides a NAT service. Figure 12 shows our Wireshark trace-collection scenario. As in our other Wireshark labs, we collect a Wireshark trace on the client PC in our home network. This file is called NAT_home_side. Because weare also interested in the packets being sent by the NAT router into the ISP, we'll collect a second trace file at a PC (not shown) tapping into the link from the home router into the ISP network, as shown in Figure 12. (The hub device shown on the ISP side of the router is used to tap into the link between the NAT router and the first hop router in the ISP). Client-to-server packets captured by Wireshark at this point will have undergone NAT translation. The Wireshark trace file captured on the ISP side of the home router is called NAT_ISP_side.

Open the NAT_home_side file and answer the following questions. You might find it useful to use a Wireshark filter so that only frames containing HTTP messages are displayed from the trace file. Whenever possible, when answering a question below, you should hand in a printout of the packet(s) within the trace that you used to answer the question asked. Annotate the printout to explain your answer.To print a packet, use File->Print, choose Selected packet only, choose Packet summary line, and selectthe minimum amount of packet detail that you need to answer the given in the Exercise Section of NAT.

Download the zip file http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip and extract thefiles need for this lab.

8. Lab Exercise:

1. Wireless Network



Where XX.XX will be your roll number

Fig-14: Topology for 1st exercise

1. Do configure the network
2. Change the Network of Wireless Router to your StudentID+Name.
3. Set the key while connecting the wireless router with end devices.
4. Do perform secure communication on Switch0 and Router0 and check it through PC0.
5. Do send mails from Wireless Users to Lan Users by creating different domains.
6. Hit the web browser using CNAME.

7. Show HTTP and HTTPs packet movement by taking screenshots.

2. NAT (Cisco Packet Tracer)

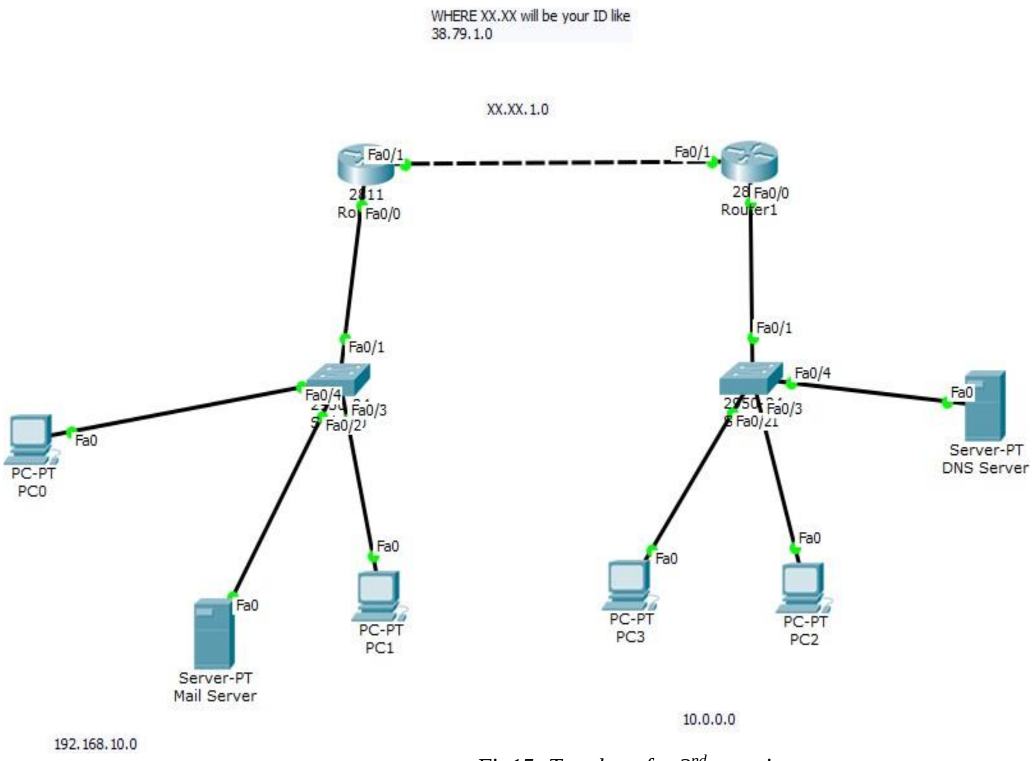


Fig15: Topology for 2nd exercise

1. Perform Static Nat on Router0 and Dynamic Nat on Router1
2. Do send mail from PC1 to PC2
3. Do hit the website from PC0

3. NAT (Wireshark)

1. What is the IP address of the client?
2. The client actually communicates with several different Google servers in order to implement "safe browsing." (See extra credit section at the end of this lab). The main Google server that willserve up the main Google web page has IP address 64.233.169.104. In order to display only thoseframes containing HTTP messages that are sent to/from this Google, server, enter the expression"http && ip.addr == 64.233.169.104" (without quotes) into the Filter: field in Wireshark .
3. Consider now the HTTP GET sent from the client to the Google server (whose IP address is IP address 64.233.169.104) at time 7.109267. What are the source and destination IP addresses andTCP source and destination ports on the IP datagram carrying this HTTP GET?
4. At what time4 is the corresponding 200 OK HTTP message received from the Google server? What are the source and destination IP addresses and TCP source and destination ports on the IPdatagram carrying this HTTP 200 OK message?
5. Recall that before a GET command can be sent to an HTTP server, TCP must first set up a connection using the three-way SYN/ACK handshake. At what time is the client-to-server TCP SYN segment sent that sets up the connection used by the GET sent at time 7.109267? What arethe source and destination IP addresses and source and destination ports for the TCP SYN segment? What are the source and destination IP addresses and source and destination ports of the ACK sent in response to the SYN. At what time is this ACK received at the client?