Network printer setup

(focus on DHCP, NAT, port forwarding, ACL, FTP server, HTTP server)

project owner: Ayesha Hafeez

course: computer networks.

Date: December 31, 2024

Contents

Winter 2024

Introduction

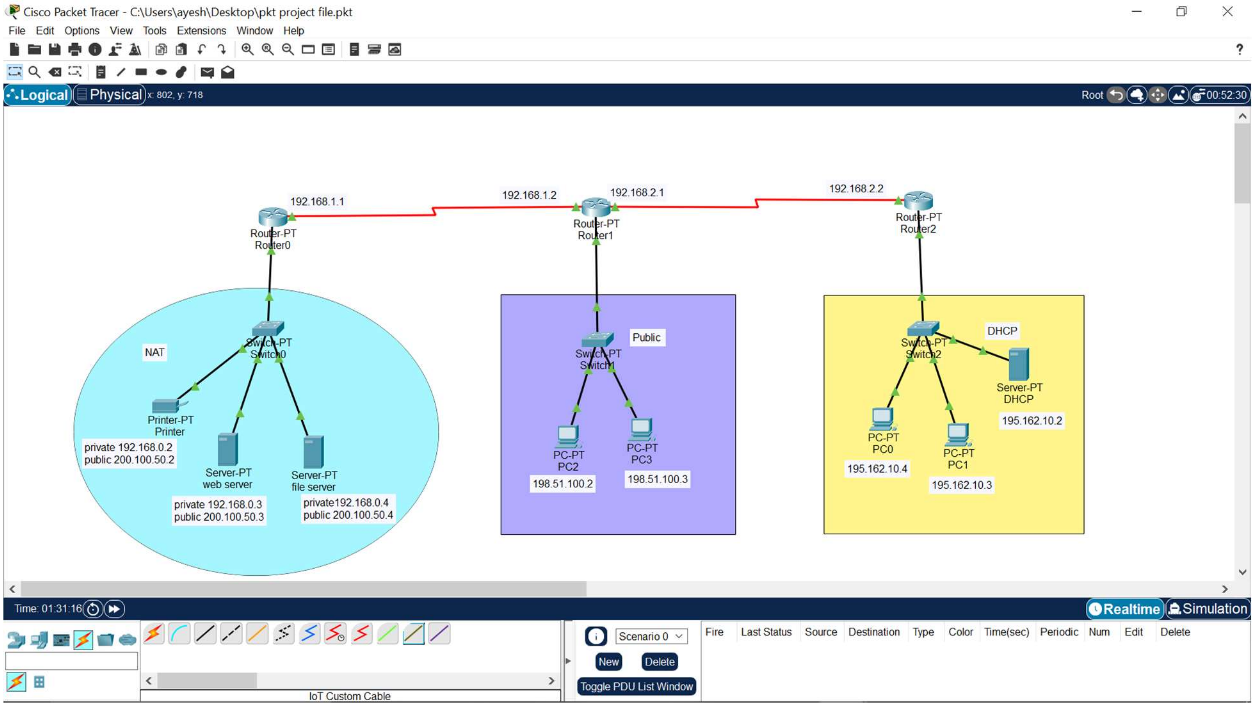
- **Objective:**

The objective of this project is to setup and configure a network printer across a simulated network in cisco packet tracer, incorporating networking concepts such as DHCP, port forwarding, NAT, ACL. The projects aims to demonstrate centralized printing by enabling multiple devices to access the printer, both within the private network and public network. It also provides managing IP configuration dynamically, securing access using ACLs.

- **Importance in real life**

NAT, ACL, and DHCP are crucial for modern networks. NAT allows private devices to access the internet securely and conserves IP addresses. ACL enhances security by controlling which devices or services can access the network. DHCP simplifies IP address assignment, ensuring devices connect quickly without manual configuration. Together, they make networks secure, efficient, and easy to manage.

Network design



Devices explanation and connections used:

This network consists of

3 routers   3 switches   4 pc's   3 servers   1 printer

- **Router:** 3 PT-routers are used (I used this router because it meets all the requirements of my network such as it has 4 FastEthernet, 2 serial interfaces).
- **Switches:** 3 PT-switches are used (6 FastEthernet interfaces).
- **Servers:** 3 servers are used, web server, file server, DHCP server.
- **Printer:** printer for sharing across all over the network.
- **PC's**: 2 public pc's, 2 pc's with dynamically assigned IP addresses.

- **Connections**: all the devices are connected with automatically chose connection type.

Structure:

- Router 0 is connected with switch0 and router1, switch0 is connected with printer, web server, file server (with automatically chose connection).
- Router1 is connected with switch1, router0, router2, switch1 is connected with 2 pc's (with automatically chose connection).
- Router2 is connected with switch2, router1, switch2 is connected with 2 pc's and DHCP server (with automatically chose connection).

IP addressing scheme:

1st network:

Printer: private IP address 192.168.0.2 gateway 192.168.0.1 public IP address 200.100.50.2

Web server: private IP address 192.168.0.3 gateway 192.168.0.1 public IP address 200.100.50.3

File server: private IP address 192.168.0.4 gateway 192.168.0.1 public IP address 200.100.50.4

Router0: FastEthernet0/0 192.168.0.1 serial2/0 192.168.1.1

static 195.162.10.0/24 via 192.168.1.2 198.51.100.0/24 via 192.168.1.2

2nd network:

Pc2: IP address 198.51.100.2 gateway 198.51.100.1

Pc3: IP address 198.51.100.3 gateway 198.51.100.1

Router1: FastEthernet0/0 198.51.100.1 serial2/0 192.168.1.2 serial3/0 192.168.2.1

Static 200.100.50.0/24 via 192.168.1.1 195.162.10.0/24 via 192.168.2.2

3rd network:

DHCP server: IP address **195.162.10.2** gateway **195.162.10.1**

Pc's: dynamically assigned pc's.

Router1: FastEthernet0/0 195.162.10.1 serial2/0 192.168.2.2

Static 200.100.50.0/24 via 192.168.2.1 198.51.100.0/24 via 192.168.2.1.

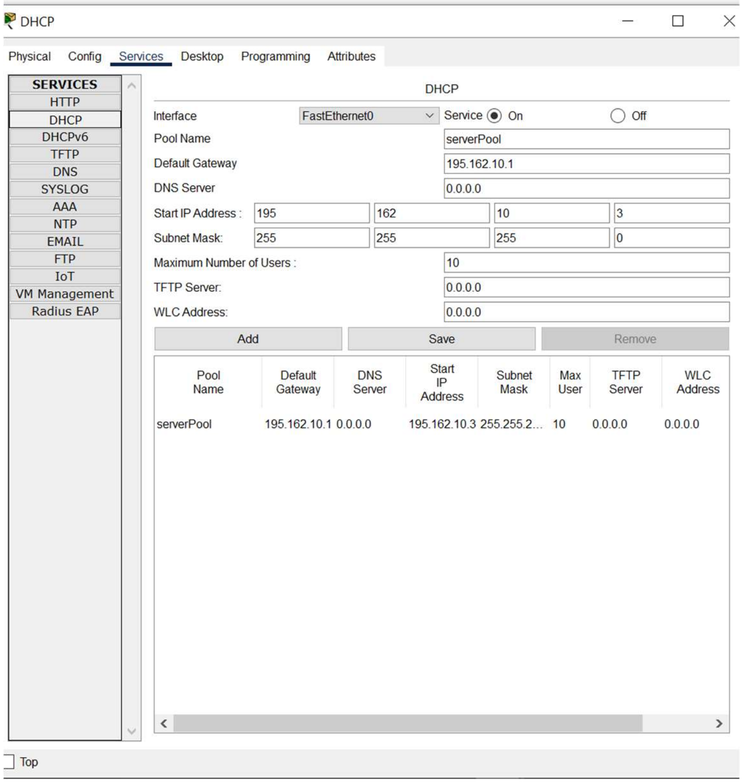
Functioning of the network

This network is design in such a way that NAT, port forwarding and ACL is configure on the router0. The printer, web and file server has private addresses and public addresses when they want to communicate with external networks they use public addresses and external devices hits these devices with public addresses external pc's cannot communicate by using their private addresses. The network connected with router1 is public and the network of router2 is configured in such a way that it is assigned with dynamically IPs. The pc 3 is restricted for using web service and file service by apply configuration on router 0 but it can access these servers but can't access the services on servers. And port forwarding forward the request for the services according to their port number.

DHCP Configuration

Dynamic Host Configuration Protocol is a network protocol used to automate the process of assigning IP addresses and other network configuration parameters to devices (such as computers, smartphones, and printers) on a network. Instead of manually configuring each device with an IP address, DHCP allows devices to connect to a network and receive all necessary network information, like IP address, subnet mask, default gateway, and DNS server addresses, automatically from a DHCP server.

This makes it easier to manage and maintain large networks, ensuring devices can communicate effectively without conflicts in their network settings. DHCP plays a crucial role in modern networks by simplifying the process of connecting devices and managing network resources efficiently.



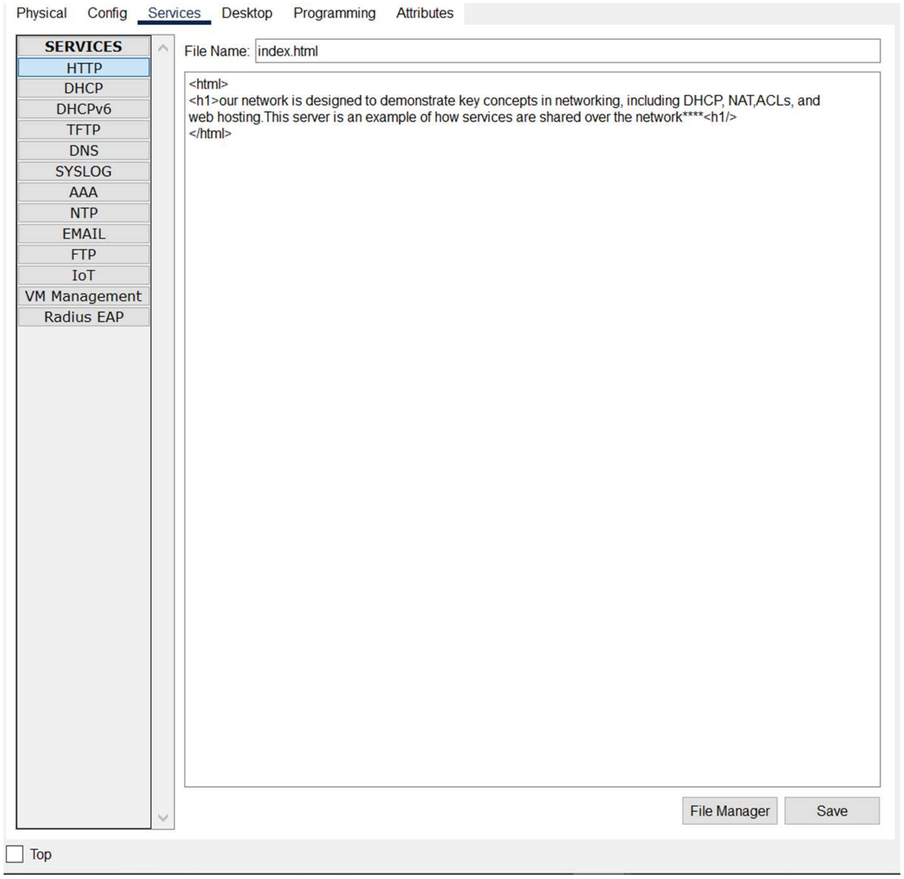
Interface: FastEthernet0
Service ● On ○ Off
Pool Name: serverPool
Default Gateway: 195.162.10.1
DNS Server: 0.0.0.0
Start IP Address : 195 162 10 3
Subnet Mask: 255 255 255 0
Maximum Number of Users : 10
TFTP Server: 0.0.0.0
WLC Address: 0.0.0.0

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool	195.162.10.1	0.0.0.0	195.162.10.3	255.255.2...	10	0.0.0.0	0.0.0.0

Do the Configuration of DHCP in this way and assign ip addresses dynamically to the pc's.

Web server setup

On the web server, click on services and then on HTTP and create the website and save it. You can access the website by any pc by move on desktop and then on web browser.



File Name: index.html

```
<html>
<h1>our network is designed to demonstrate key concepts in networking, including DHCP, NAT,ACLs, and
web hosting.This server is an example of how services are shared over the network****<h1/>
</html>
```

File server setup

On the file server, click on services and then on FTP and then fill the options.

In Cisco Packet Tracer, under the FTP (File Transfer Protocol) service settings on a server, these options define user permissions for accessing and managing files on the server:

Username and Password: Credentials required for authentication to access the FTP server.

Read: Allows users to view or download files from the server.

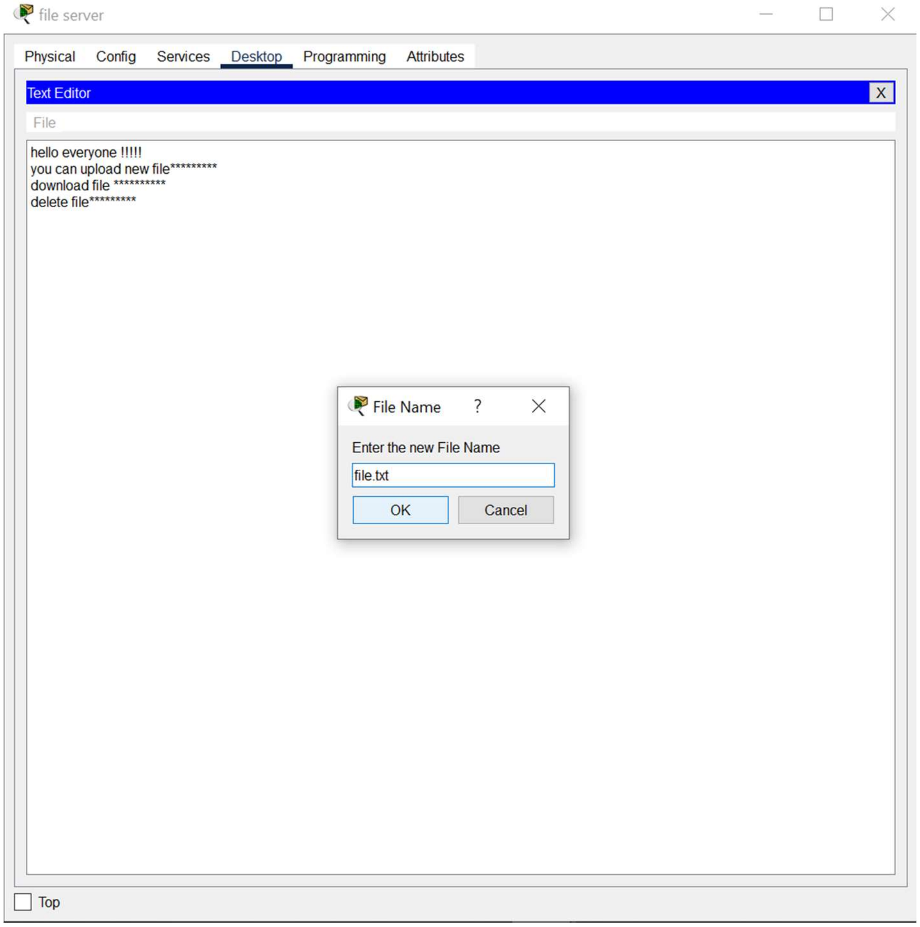
Write: Permits users to upload files to the server.

Delete: Enables users to remove files from the server.

Rename: Lets users rename existing files on the server.

List: Allows users to view the directory structure and file listings

Now move to text editor on desktop tab and create file and save the file name.

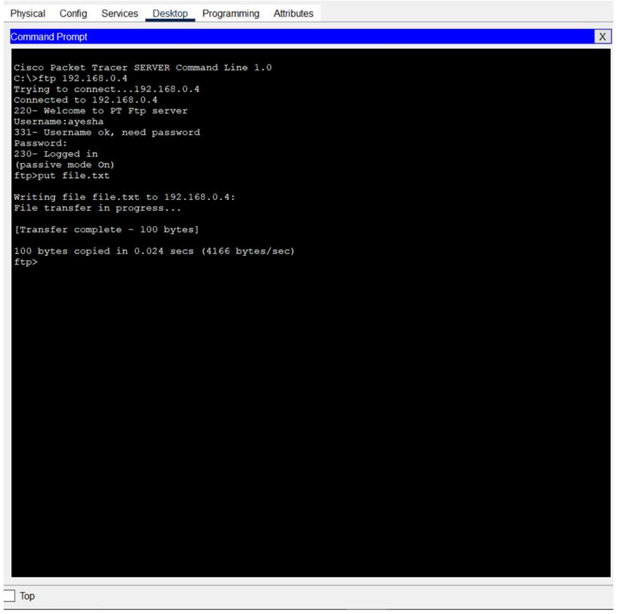


```
hello everyone !!!!!
you can upload new file*********
download file **********
delete file*********
```

Enter the new File Name

file.txt

Now move to command prompt and upload the file in this way

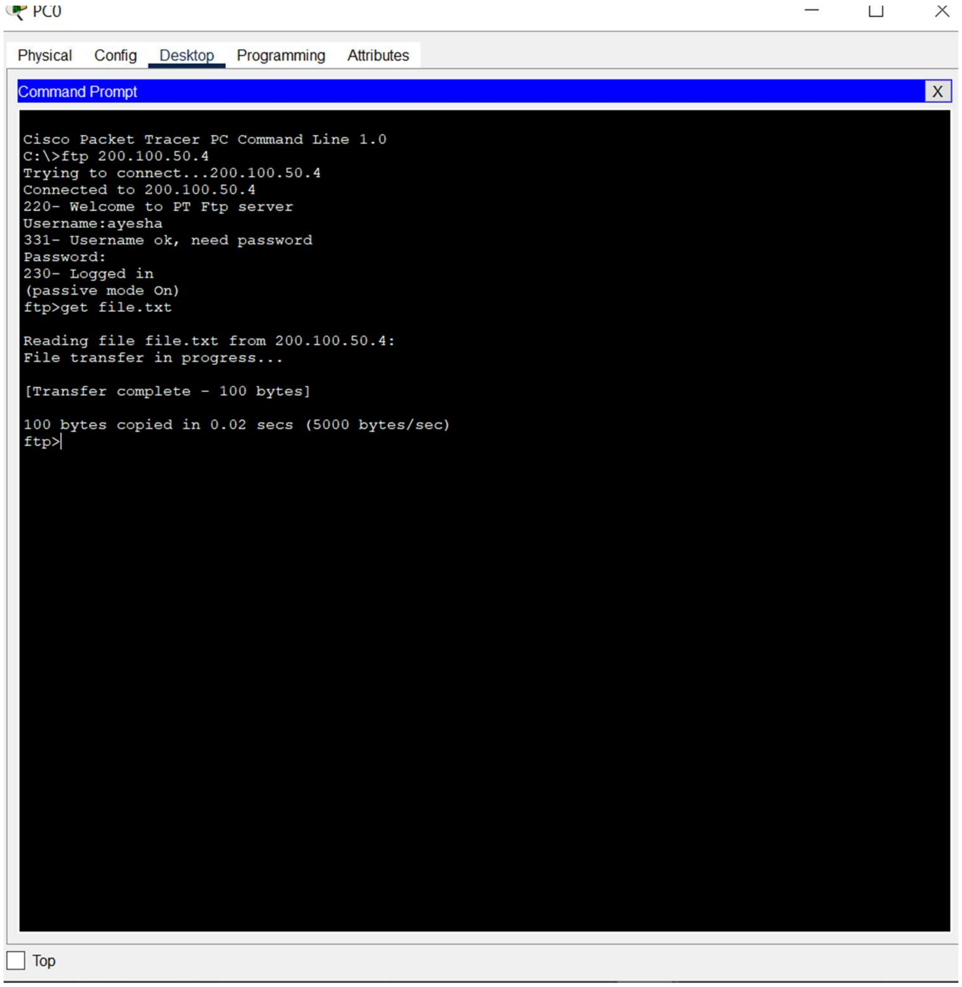


```
Cisco Packet Tracer SERVER Command Line 1.0
C:\>ftp 192.168.0.4
Trying to connect...192.168.0.4
Connected to 192.168.0.4
220- Welcome to PT Ftp server
Username:ayesha
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>put file.txt

Writing file file.txt to 192.168.0.4:
File transfer in progress...

[Transfer complete - 100 bytes]

100 bytes copied in 0.024 secs (4166 bytes/sec)
ftp>
```

Username for this: ayesha

Pasword: hafeez

You can upload, get, delete, rename, see the list on any pc you want in such a way (in this we get the uploaded file which we upload through server).



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ftp 200.100.50.4
Trying to connect...200.100.50.4
Connected to 200.100.50.4
220- Welcome to PT Ftp server
Username:ayesha
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>get file.txt

Reading file file.txt from 200.100.50.4:
File transfer in progress...

[Transfer complete - 100 bytes]

100 bytes copied in 0.02 secs (5000 bytes/sec)
ftp>
```

You can delete, rename and see list by any pc by using these commands

Delete a File: delete <filename>

Rename a File: rename <old_filename> <new_filename>

List Files: dir

Download the file to the PC using the get command.

updated file back to the server using the put command.

You can do all this because you give the permissions to the pc's that know the user name and password

NAT configuration

Network Address Translation (NAT) is a process in which one or more local IP addresses are translated into one or more Global IP addresses and vice versa to provide Internet access to the local hosts. Generally, the border router is configured for NAT i.e. the router which has one interface in the local (inside) network and one interface in the global (outside) network. When a packet traverse outside the local (inside) network, then NAT converts that local (private) IP address to a global (public) IP address. When a packet enters the local network, the global (public) IP address is converted to a local (private) IP address.

Network Address Translation (NAT) Types

There are 3 ways to configure NAT:

- *Static NAT*
- *Dynamic NAT*
- *Port Address Translation (PAT)*

IN this network the static NAT is used

Static NAT

In this, a single unregistered (Private) IP address is mapped with a legally registered (Public) IP address i.e one-to-one mapping between local and global addresses. This is generally used for Web hosting. These are not used in organizations as there are many devices that will need Internet access and to provide Internet access, a public IP address is needed.

Suppose, if there are 3000 devices that need access to the Internet, the organization has to buy 3000 public addresses that will be very costly.

The question raised is that

The main objective is Nat to conserve IPV4 addresses by allowing multiple devices in a private network to share a single public IP but in this **type there is one-to-one**

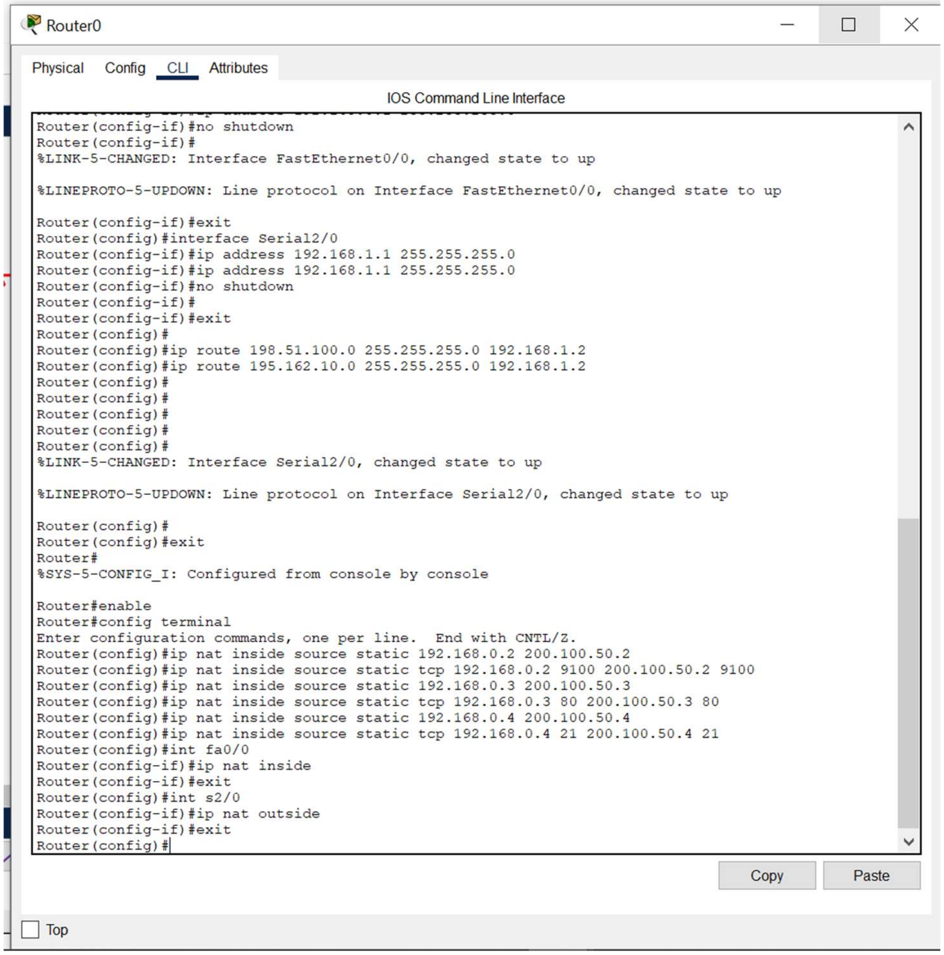
mapping than what is the benefit of using this type and why we use it?

This type of NAT is mostly used for servers where we want to provide security by preventing direct access, ensuring controlled and secure communication.

Configuration:

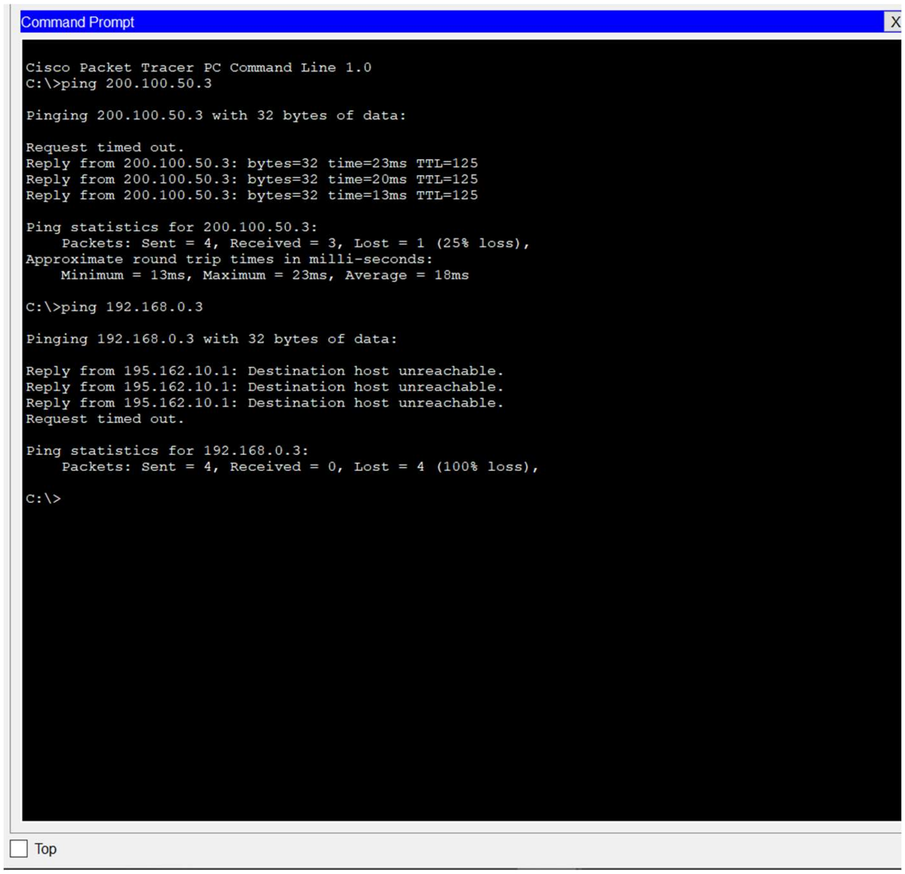
Configuration for NAT on router for printer and 2 servers is:

- **For printer**: ip nat inside source static 192.168.0.2 200.100.50.2
- **For web server:** ip nat inside source static 192.168.0.3 200.100.50.3
- **For file server:** ip nat inside source static 192.168.0.4 200.100.50.4
- int fa0/0
- ip nat inside
- exit
- int s2/0
- ip nat outside
- exit

- 

```
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

Router(config-if)#exit
Router(config)#interface Serial2/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#
Router(config-if)#exit
Router(config)#
Router(config)#ip route 198.51.100.0 255.255.255.0 192.168.1.2
Router(config)#ip route 195.162.10.0 255.255.255.0 192.168.1.2
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
%LINK-5-CHANGED: Interface Serial2/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up

Router(config)#
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#enable
Router#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip nat inside source static 192.168.0.2 200.100.50.2
Router(config)#ip nat inside source static tcp 192.168.0.2 9100 200.100.50.2 9100
Router(config)#ip nat inside source static 192.168.0.3 200.100.50.3
Router(config)#ip nat inside source static tcp 192.168.0.3 80 200.100.50.3 80
Router(config)#ip nat inside source static 192.168.0.4 200.100.50.4
Router(config)#ip nat inside source static tcp 192.168.0.4 21 200.100.50.4 21
Router(config)#int fa0/0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#int s2/0
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#
```

It is clear that when you want to access the pc by their public address it is accessed but when you use the private address it give the reply destination host unreachable. So nat is success full.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 200.100.50.3

Pinging 200.100.50.3 with 32 bytes of data:

Request timed out.
Reply from 200.100.50.3: bytes=32 time=23ms TTL=125
Reply from 200.100.50.3: bytes=32 time=20ms TTL=125
Reply from 200.100.50.3: bytes=32 time=13ms TTL=125

Ping statistics for 200.100.50.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 13ms, Maximum = 23ms, Average = 18ms

C:\>ping 192.168.0.3

Pinging 192.168.0.3 with 32 bytes of data:

Reply from 195.162.10.1: Destination host unreachable.
Reply from 195.162.10.1: Destination host unreachable.
Reply from 195.162.10.1: Destination host unreachable.
Request timed out.

Ping statistics for 192.168.0.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Port forwarding

In computer networking, **port forwarding** or **port mapping** is an application of network address translation (NAT) that redirects a communication request from one address and port number combination to another while the packets are traversing a network gateway, such as a router or firewall. This technique is most commonly used to make services on a host residing on a protected or masqueraded (internal) network available to hosts on the opposite side of the gateway (external network), by remapping the destination IP address and port number of the communication to an internal host.

Port forwarding facilitates the connection by remote computers, for example, Internet hosts, to a specific computer or service within a local area network (LAN).

Port forwarding is used to direct incoming network traffic on a specific port to a particular device or service within a private network.

When configuring port forwarding, the network administrator sets aside one port number on the gateway for the exclusive use of communicating with a service in the private network, located on a specific host. External hosts must know this port number and the address of the gateway to communicate with the network-internal service. Often, the port numbers of well-known Internet services, such as port number 80 for web services (HTTP), are used in port forwarding, so that common Internet services may be implemented on hosts within private networks.

Typical applications include the following:

- Running a public **HTTP** server within a private LAN
- Permitting **secure shell** access to a host on the private LAN from the Internet
- Permitting **FTP** access to a host on a private LAN from the Internet
- Running a publicly available game server within a private LAN

Port numbers used in this network

80	HTTP	web traffic
20/21	FTP	file transfer

9100	printer	used for direct printing to network printers

In this network the router is configure for port forwarding, when the request is coming for service the port forwarding control the traffic coming from external devices and see the port number of the service and directly send it to that service. However, Packet tracer does not visually show the internal workings of how the router processes or manages this traffic.

3389	RDP	remote desktop access

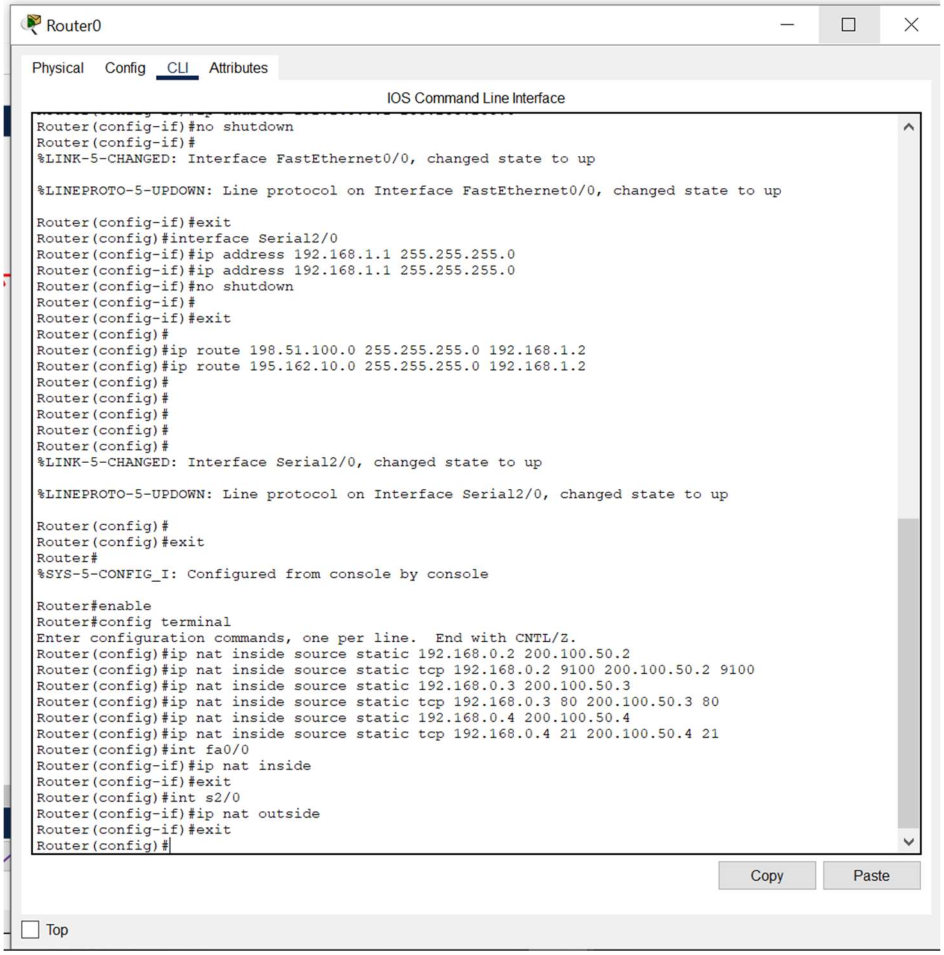
By using this port you can access your desktop from anywhere as setting in front of desktop. But RDP is not directly supported in cisco.

Configuration of port forwarding:

For printer: ip nat inside source static tcp 192.168.0.2 9100 200.100.50.2 9100

For web server: ip nat inside source static tcp 192.168.0.3 80 200.100.50.3 80

For file server: ip nat inside source static tcp 192.168.0.4 21 200.100.50.4 21



```
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

Router(config-if)#exit
Router(config)#interface Serial2/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#
Router(config-if)#exit
Router(config)#
Router(config)#ip route 198.51.100.0 255.255.255.0 192.168.1.2
Router(config)#ip route 195.162.10.0 255.255.255.0 192.168.1.2
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
%LINK-5-CHANGED: Interface Serial2/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up

Router(config)#
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#enable
Router#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip nat inside source static 192.168.0.2 200.100.50.2
Router(config)#ip nat inside source static tcp 192.168.0.2 9100 200.100.50.2 9100
Router(config)#ip nat inside source static 192.168.0.3 200.100.50.3
Router(config)#ip nat inside source static tcp 192.168.0.3 80 200.100.50.3 80
Router(config)#ip nat inside source static 192.168.0.4 200.100.50.4
Router(config)#ip nat inside source static tcp 192.168.0.4 21 200.100.50.4 21
Router(config)#int fa0/0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#int s2/0
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#
```

ACL configuration

Access control list (ACL) is a set of rules defined for controlling network traffic and reducing network attacks. ACLs are used to filter traffic based on the set of rules defined for the incoming or outgoing of the network.

ACL features –

1. The set of rules defined are matched serial wise i.e matching starts with the first line, then 2nd, then 3rd, and so on.

2. The packets are matched only until it matches the rule. Once a rule is matched then no further comparison takes place and that rule will be performed.
3. There is an implicit denial at the end of every ACL, i.e., if no condition or rule matches then the packet will be discarded.

Types of ACL

There are two main different types of Access-list namely:

Standard Access-list

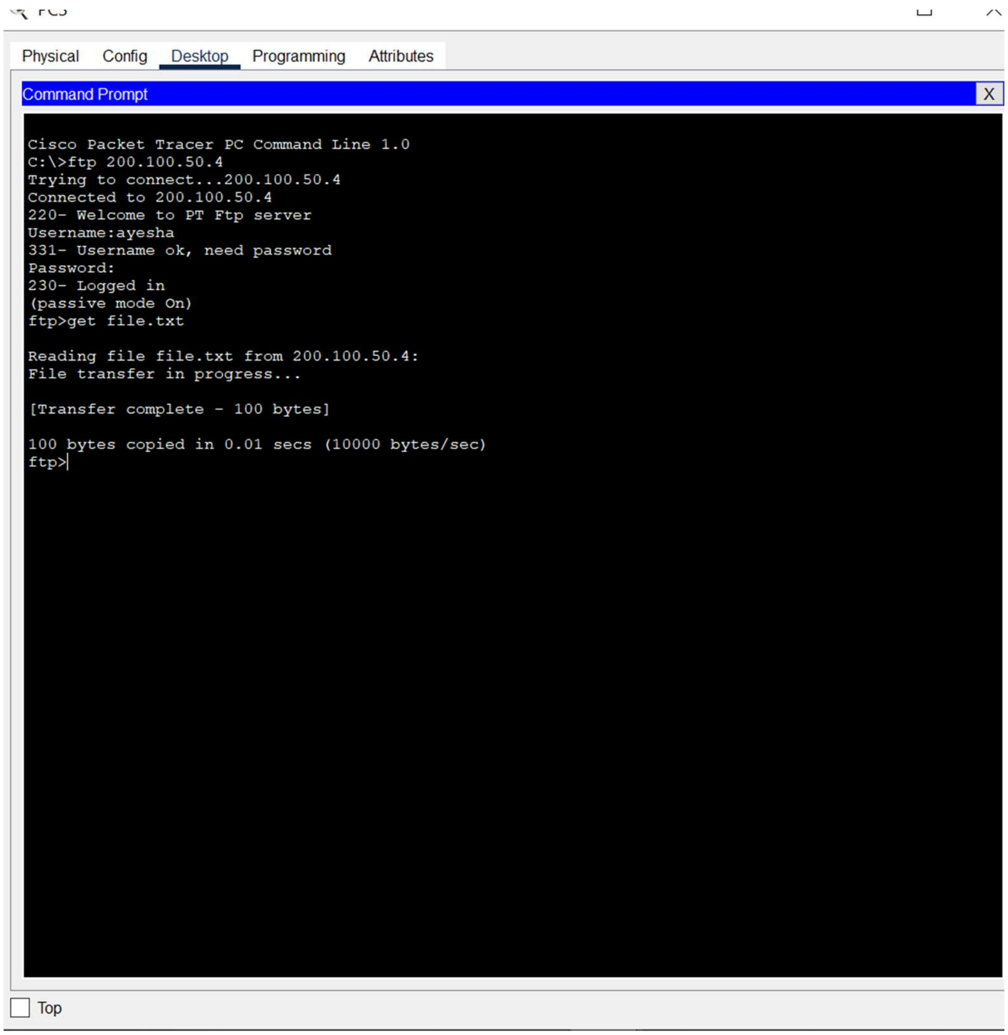
These are the Access-list that are made using the source IP address only. These ACLs permit or deny the entire protocol suite. They don't distinguish between the IP traffic such as TCP, UDP, HTTPS, etc. By using numbers 1-99 or 1300-1999, the router will understand it as a standard ACL and the specified address as the source IP address.

Extended Access-list

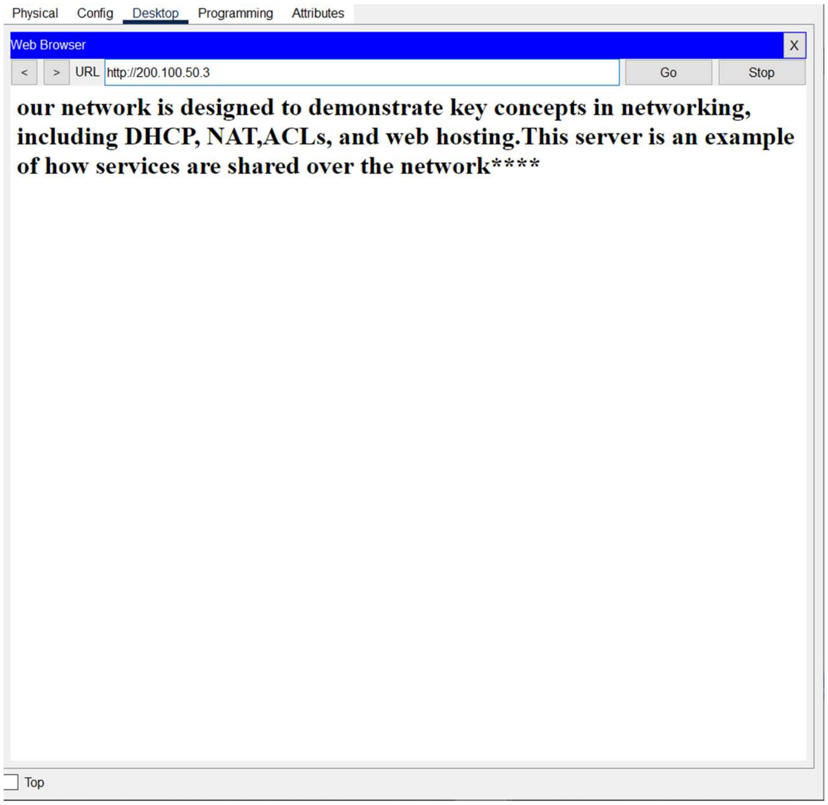
These are the ACL that uses source IP, Destination IP, source port, and Destination port. These types of ACL, we can also mention which IP traffic should be allowed or denied. These use range 100-199 and 2000-2699.

Before applying restrictions:

You can access the services of web server and file server through pc3.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ftp 200.100.50.4
Trying to connect...200.100.50.4
Connected to 200.100.50.4
220- Welcome to PT Ftp server
Username:ayesha
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>get file.txt

Reading file file.txt from 200.100.50.4:
File transfer in progress...

[Transfer complete - 100 bytes]

100 bytes copied in 0.01 secs (10000 bytes/sec)
ftp>
```



http://200.100.50.3

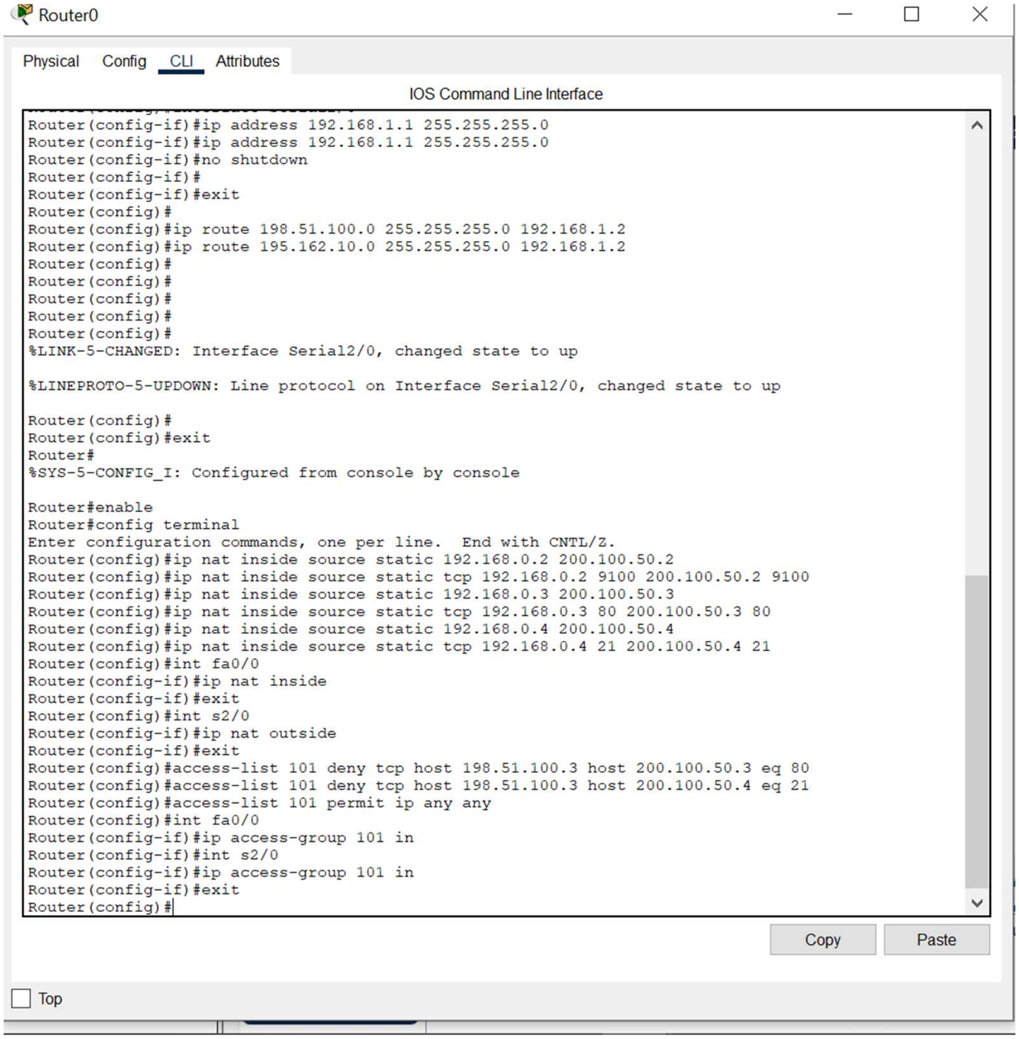
our network is designed to demonstrate key concepts in networking, including DHCP, NAT,ACLs, and web hosting.This server is an example of how services are shared over the network****

In this network extended access list is used because we want to restrict pc 3 to access the service of web server and service of file server. The pc3 can access the servers but cannot access the services as we configure the router to deny its request for services. All other pc's can access the services and printer.

Configuration of ACL on router:

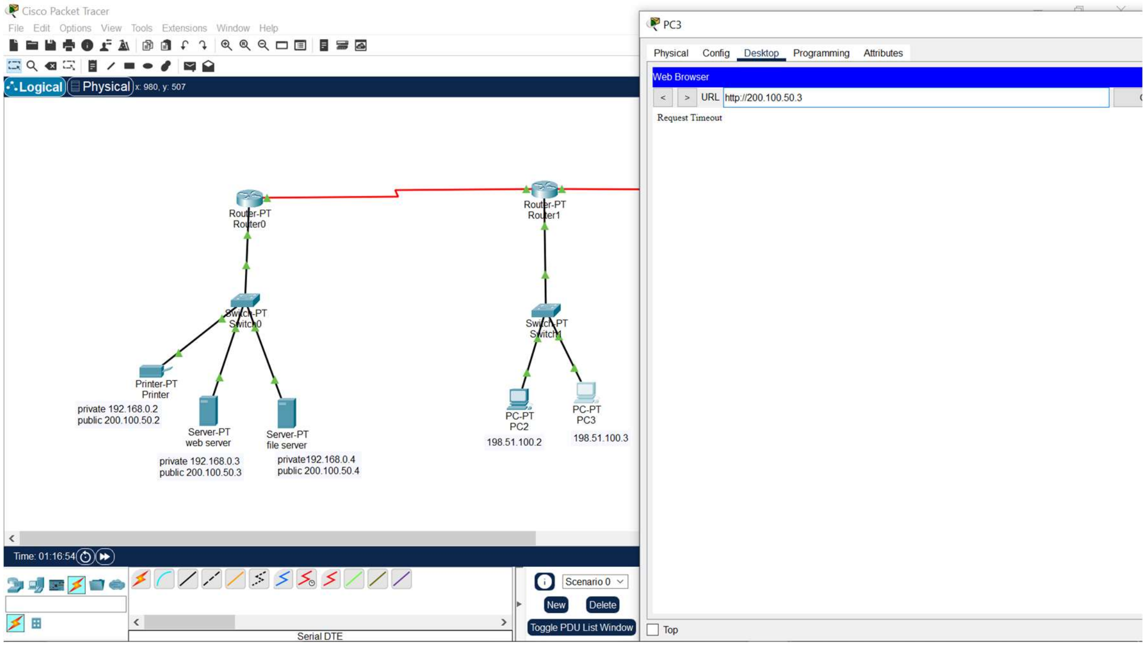
- access-list 101 deny tcp host 198.51.100.3 host 200.100.50.3 eq 80
- access-list 101 deny tcp host 198.51.100.3 host 200.100.50.4 eq 21
- access-list 101 permit ip any any

- int fa0/0
- ip access-group 101 in
- int s2/0
- ip access-group 101 in
- exit

- 

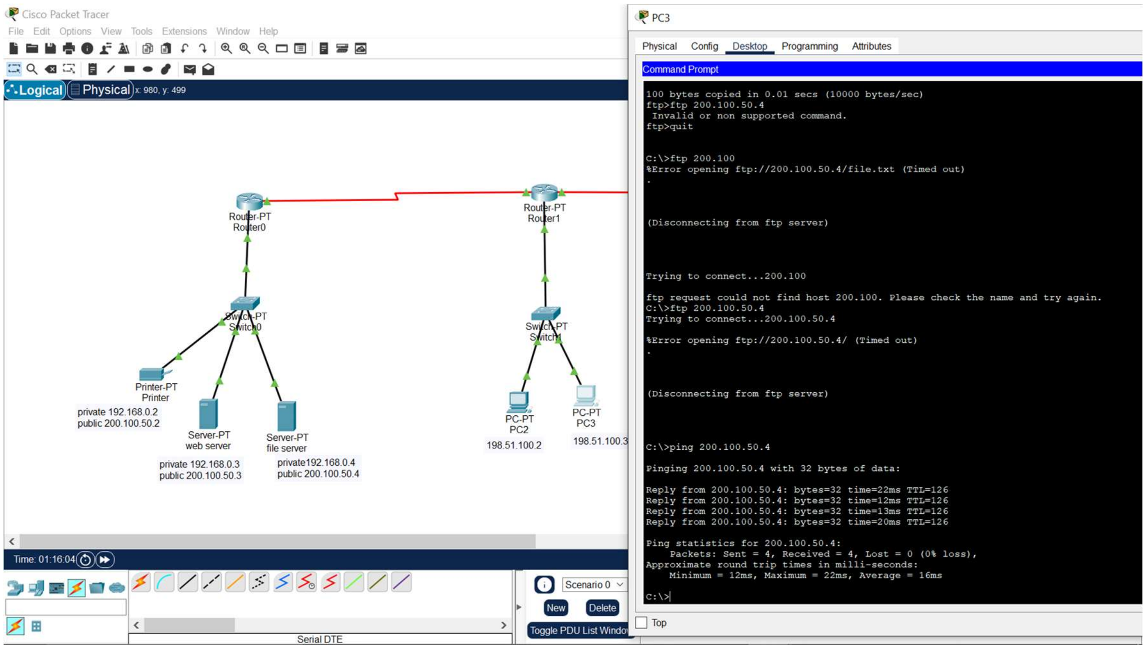
```
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#
Router(config-if)#exit
Router(config)#
Router(config)#ip route 198.51.100.0 255.255.255.0 192.168.1.2
Router(config)#ip route 195.162.10.0 255.255.255.0 192.168.1.2
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
%LINK-5-CHANGED: Interface Serial2/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up

Router(config)#
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#enable
Router#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip nat inside source static 192.168.0.2 200.100.50.2
Router(config)#ip nat inside source static tcp 192.168.0.2 9100 200.100.50.2 9100
Router(config)#ip nat inside source static 192.168.0.3 200.100.50.3
Router(config)#ip nat inside source static tcp 192.168.0.3 80 200.100.50.3 80
Router(config)#ip nat inside source static 192.168.0.4 200.100.50.4
Router(config)#ip nat inside source static tcp 192.168.0.4 21 200.100.50.4 21
Router(config)#int fa0/0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#int s2/0
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#access-list 101 deny tcp host 198.51.100.3 host 200.100.50.3 eq 80
Router(config)#access-list 101 deny tcp host 198.51.100.3 host 200.100.50.4 eq 21
Router(config)#access-list 101 permit ip any any
Router(config)#int fa0/0
Router(config-if)#ip access-group 101 in
Router(config-if)#int s2/0
Router(config-if)#ip access-group 101 in
Router(config-if)#exit
Router(config)#
```

After applying ACL:



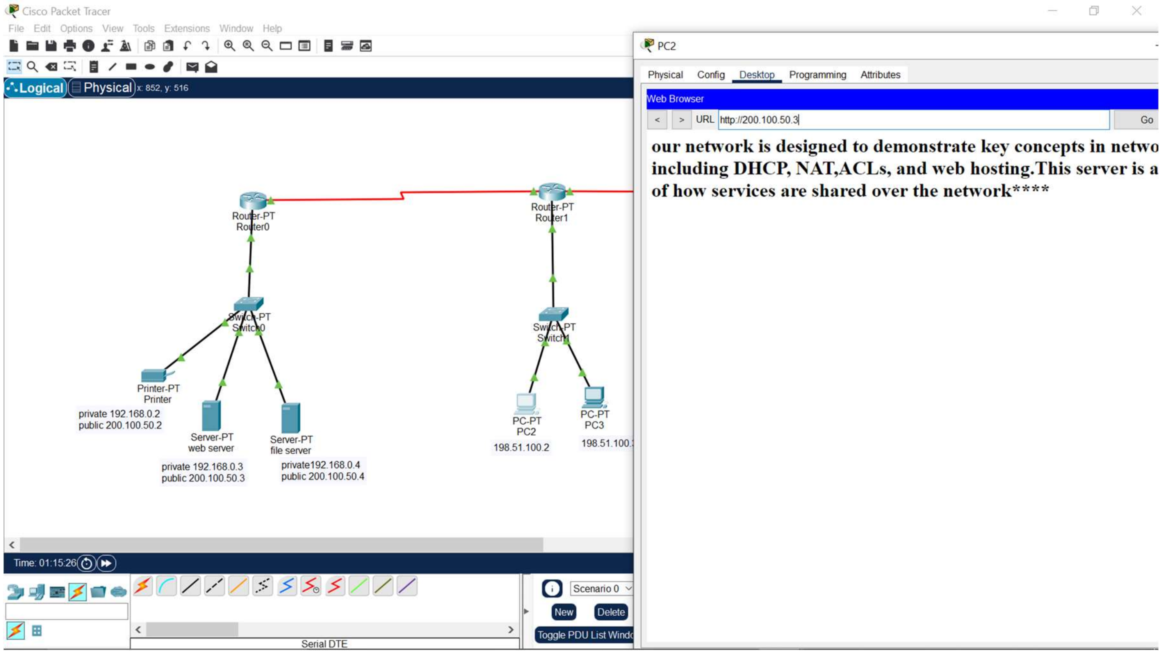
URL http://200.100.50.3

Request Timeout



```
100 bytes copied in 0.01 secs (10000 bytes/sec)
ftp>ftp 200.100.50.4
 Invalid or non supported command.
ftp>quit


C:\>ftp 200.100
%Error opening ftp://200.100.50.4/file.txt (Timed out)
.



(Disconnecting from ftp server)




Trying to connect...200.100

ftp request could not find host 200.100. Please check the name and try again.
C:\>ftp 200.100.50.4
Trying to connect...200.100.50.4

%Error opening ftp://200.100.50.4/ (Timed out)
.



(Disconnecting from ftp server)




C:\>ping 200.100.50.4

Pinging 200.100.50.4 with 32 bytes of data:

Reply from 200.100.50.4: bytes=32 time=22ms TTL=126
Reply from 200.100.50.4: bytes=32 time=12ms TTL=126
Reply from 200.100.50.4: bytes=32 time=13ms TTL=126
Reply from 200.100.50.4: bytes=32 time=20ms TTL=126

Ping statistics for 200.100.50.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 12ms, Maximum = 22ms, Average = 16ms

C:\>
```

This shows that you can access the servers but cannot access the services.



URL http://200.100.50.3

our network is designed to demonstrate key concepts in netwo
including DHCP, NAT,ACLs, and web hosting.This server is a
of how services are shared over the network****

But you can access the services from any other pc as there is no restriction for other pc's

Challenges and solutions

1. If we want to restrict some other services but I already write the allow statement and as in CLI we cannot delete the commands and if we write these command again without deleting there is no change in such case as ACLs are processed top to bottom, so

you need to move your deny statements above the permit statements.

Solution: use this command

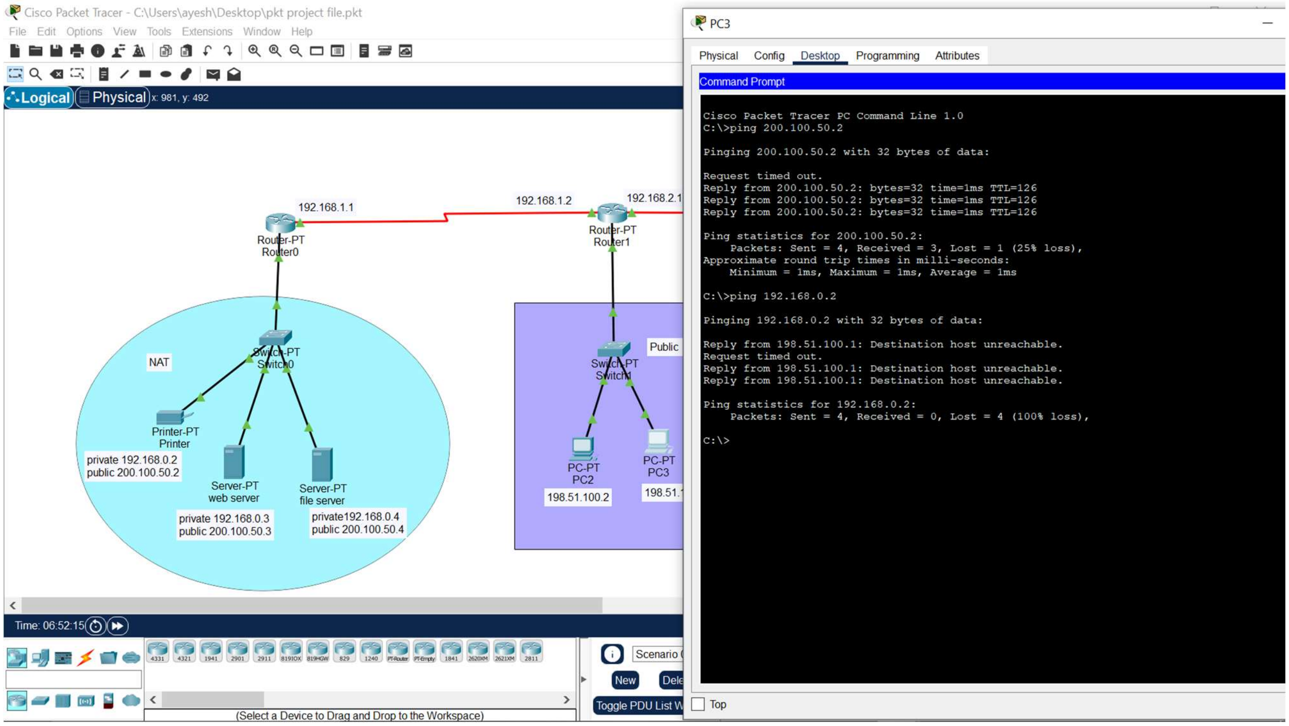
No access-list <ACL_number>

And configure the complete ACL again.

2. **When we use ftp command in command prompt how to return to the normal command prompt interface.**

   Solution: use command **quit**
3. Selection about NAT which type is suitable here
4. Converting the network from class A to class C in class C less IPs waste but this can also overlap if not done carefully.

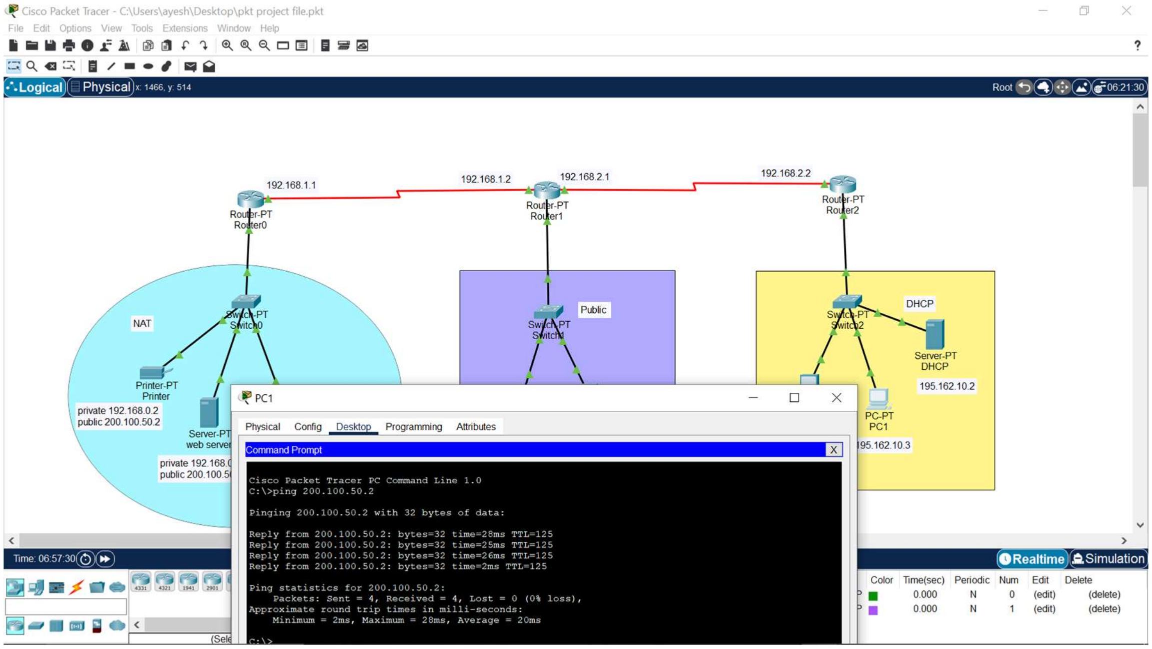
Screen shoots for printer



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 200.100.50.2

Pinging 200.100.50.2 with 32 bytes of data:

Request timed out.
Reply from 200.100.50.2: bytes=32 time=1ms TTL=126
Reply from 200.100.50.2: bytes=32 time=1ms TTL=126
Reply from 200.100.50.2: bytes=32 time=1ms TTL=126

Ping statistics for 200.100.50.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\>ping 192.168.0.2

Pinging 192.168.0.2 with 32 bytes of data:

Reply from 198.51.100.1: Destination host unreachable.
Request timed out.
Reply from 198.51.100.1: Destination host unreachable.
Reply from 198.51.100.1: Destination host unreachable.

Ping statistics for 192.168.0.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

The pc which is restricted for services of servers can access the printer as there is no restriction for pc to access the printer. And printer cannot be accessed by their private address but can be accessed by public.

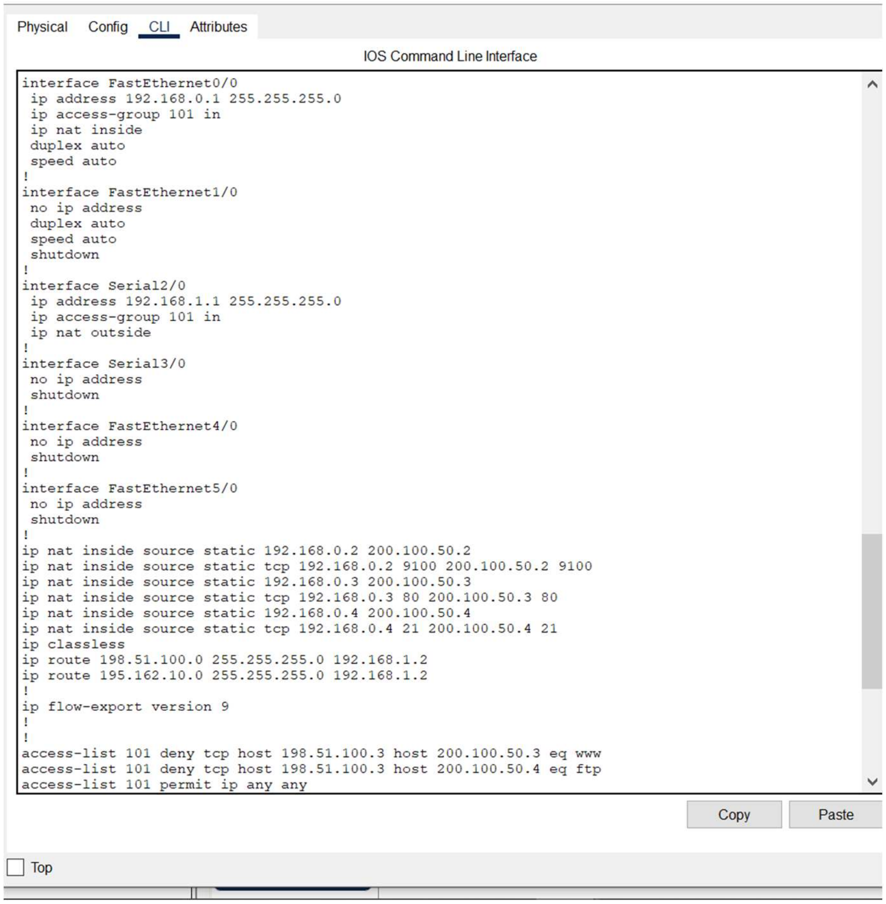
The printer is accessed by the pc's, with IP addresses assigned dynamically:



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 200.100.50.2

Pinging 200.100.50.2 with 32 bytes of data:

Reply from 200.100.50.2: bytes=32 time=28ms TTL=125
Reply from 200.100.50.2: bytes=32 time=25ms TTL=125
Reply from 200.100.50.2: bytes=32 time=26ms TTL=125
Reply from 200.100.50.2: bytes=32 time=2ms TTL=125

Ping statistics for 200.100.50.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 28ms, Average = 20ms

C:\>
```

Color	Time(sec)	Periodic	Num	Edit	Delete
🟩	0.000	N	0	(edit)	(delete)
🟪	0.000	N	1	(edit)	(delete)

Complete configuration



```
interface FastEthernet0/0
 ip address 192.168.0.1 255.255.255.0
 ip access-group 101 in
 ip nat inside
 duplex auto
 speed auto
!
interface FastEthernet1/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial2/0
 ip address 192.168.1.1 255.255.255.0
 ip access-group 101 in
 ip nat outside
!
interface Serial3/0
 no ip address
 shutdown
!
interface FastEthernet4/0
 no ip address
 shutdown
!
interface FastEthernet5/0
 no ip address
 shutdown
!
ip nat inside source static 192.168.0.2 200.100.50.2
ip nat inside source static tcp 192.168.0.2 9100 200.100.50.2 9100
ip nat inside source static 192.168.0.3 200.100.50.3
ip nat inside source static tcp 192.168.0.3 80 200.100.50.3 80
ip nat inside source static 192.168.0.4 200.100.50.4
ip nat inside source static tcp 192.168.0.4 21 200.100.50.4 21
ip classless
ip route 198.51.100.0 255.255.255.0 192.168.1.2
ip route 195.162.10.0 255.255.255.0 192.168.1.2
!
ip flow-export version 9
!
!
access-list 101 deny tcp host 198.51.100.3 host 200.100.50.3 eq www
access-list 101 deny tcp host 198.51.100.3 host 200.100.50.4 eq ftp
access-list 101 permit ip any any
```

To see the configuration you perform on router click ctrl+z and write show running-config.

References

https://www.geeksforgeeks.org/steps-of-configuring-nat-for-ip-address-conservation/

https://youtu.be/5bUp6AI0aeM?si=YmB_JXvpDSiuLo7I

https://youtube.com/watch?v=NIaP2Bkzs6k&si=9Ds_kSPOpLrk26BK

https://youtu.be/NBReniXzlz0?si=dzN6V6VRS1yBcFne

https://youtu.be/Mk5WUsHOK0Y?si=iX6m94QG7IA6Dbnv