HACETTEPE UNIVERSITY
DEPARTMENT OF COMPUTER ENGINEERING
BBM453 COMPUTER NETWORK LABORATORY

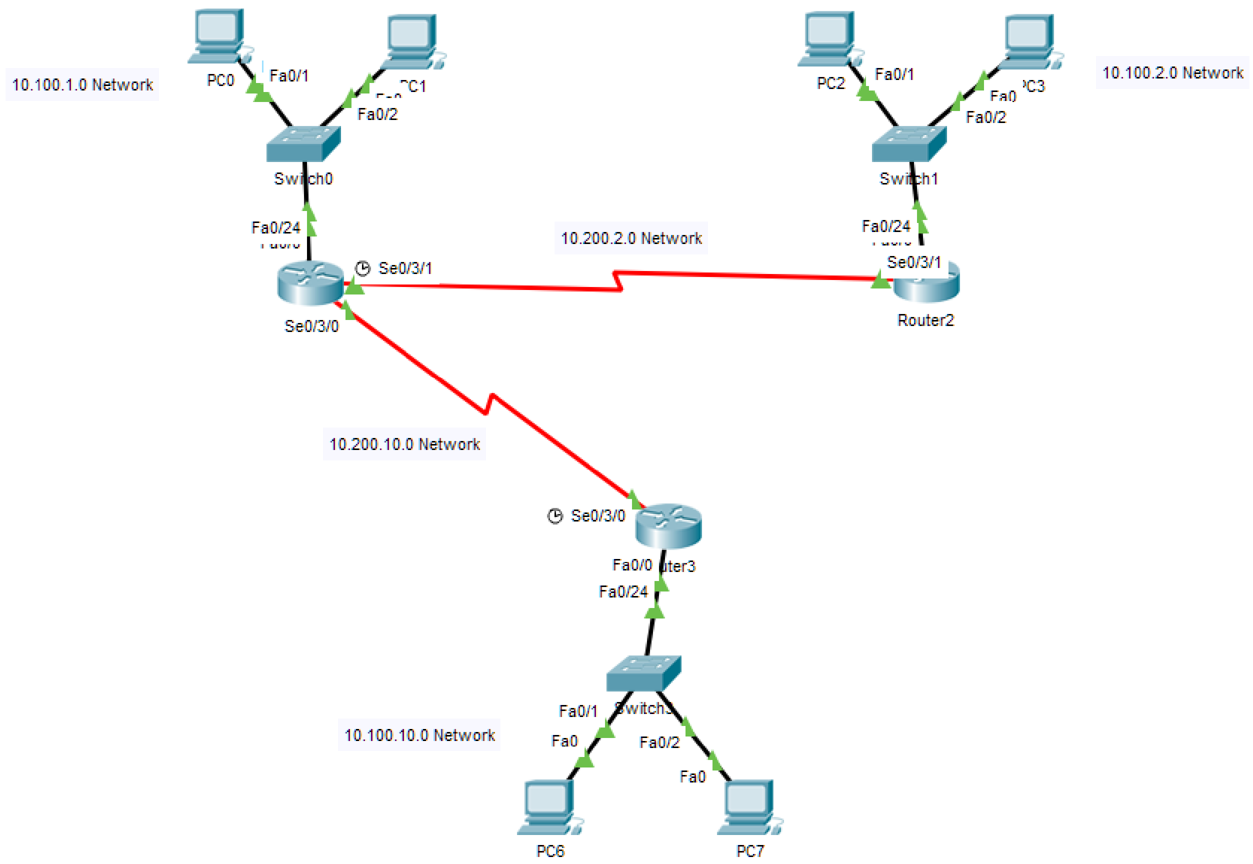
REPORT OF EXPERIMENT
12 - NAT

AUTHORS OF EXPERIMENT

21627868	Burak Yılmaz	Group 1
21627557	Gökhan Özeloğlu	Group 1
21627581	Mehmet Sezer	Group 2
21727226	İlkan Akın Erenler	Group 2
21627452	Güney Kırık	Group 10
21727135	İrem Dereli	Group 10

1. Your aim is to configure NAT on your router and translate your PC's IP address in your group to a single IP from your subnet. After translation process, you will be able to test your address translation with pinging to new IP addresses and using show commands. Another way to test your configuration is to connect remotely to another group's router and running show user command to see logged in users on that router.

Here is our topology:



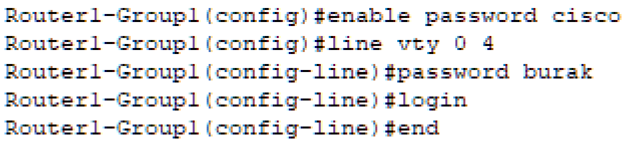
2. You are going to use telnet for remote connection. To be able to use telnet, you have to configure necessary password steps for security restrictions. For example try to telnet (from your PC) to another group's Router (IP address of Serial interface), and understand why you are not able to connect to the Router.

Since no telnet connection permission configuration is set on each router, this process will fail even if we make a telnet request to these routers.

3. You have to enable password and telnet password for remote connection.

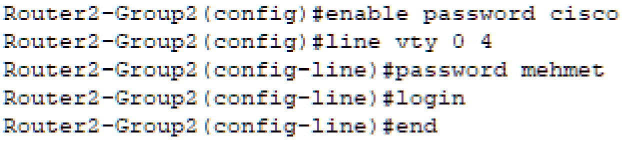
As you can see, we set enabled passwords and telnet passwords here. Thus, to activate routers, the "cisco" password, and the following passwords for each router must be entered when the telnet connection is established.

Router 1 Telnet



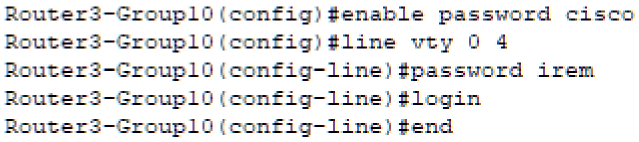
```
Router1-Group1(config)#enable password cisco
Router1-Group1(config)#line vty 0 4
Router1-Group1(config-line)#password burak
Router1-Group1(config-line)#login
Router1-Group1(config-line)#end
```

Router 2 Telnet



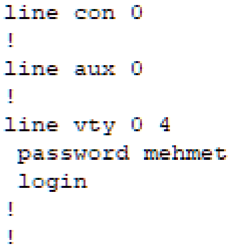
```
Router2-Group2(config)#enable password cisco
Router2-Group2(config)#line vty 0 4
Router2-Group2(config-line)#password mehmet
Router2-Group2(config-line)#login
Router2-Group2(config-line)#end
```

Router 3 Telnet



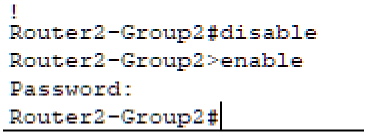
```
Router3-Group10(config)#enable password cisco
Router3-Group10(config)#line vty 0 4
Router3-Group10(config-line)#password irem
Router3-Group10(config-line)#login
Router3-Group10(config-line)#end
```

4. Display your configuration changes on running-config and try logout from Router using disable command and then enable again.



```
line con 0
!
line aux 0
!
line vty 0 4
 password mehmet
 login
!
!
```

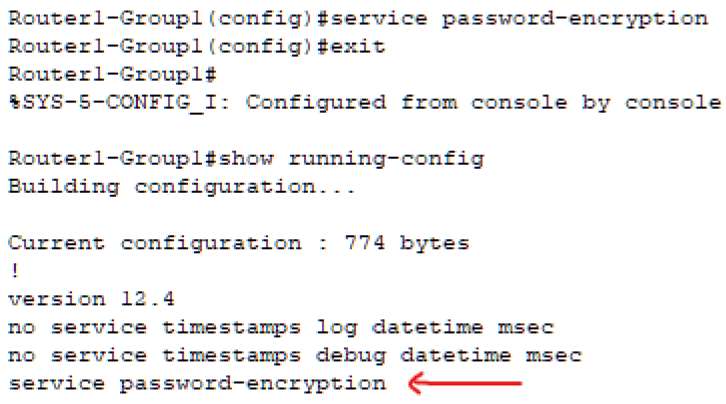
Here you can see our configuration changes on running-config. The telnet password is set as "mehmet".



```
!
Router2-Group2#disable
Router2-Group2>enable
Password:
Router2-Group2#
```

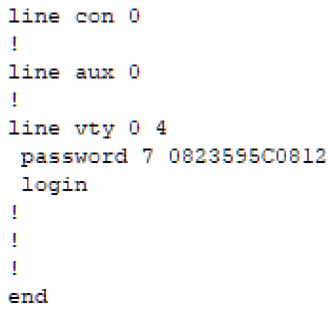
Here we logout with a disable command and are enabled again using the password.

5. You should observe that all text passwords can be easily seen in a config file. That is also a security bug. You should use an encryption service for encrypting password texts.



```
Router1-Group1(config)#service password-encryption
Router1-Group1(config)#exit
Router1-Group1#
%SYS-5-CONFIG_I: Configured from console by console

Router1-Group1#show running-config
Building configuration...

Current configuration : 774 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
```

Here we can see the config file content and in the line shown we see that the password-encryption service is used.

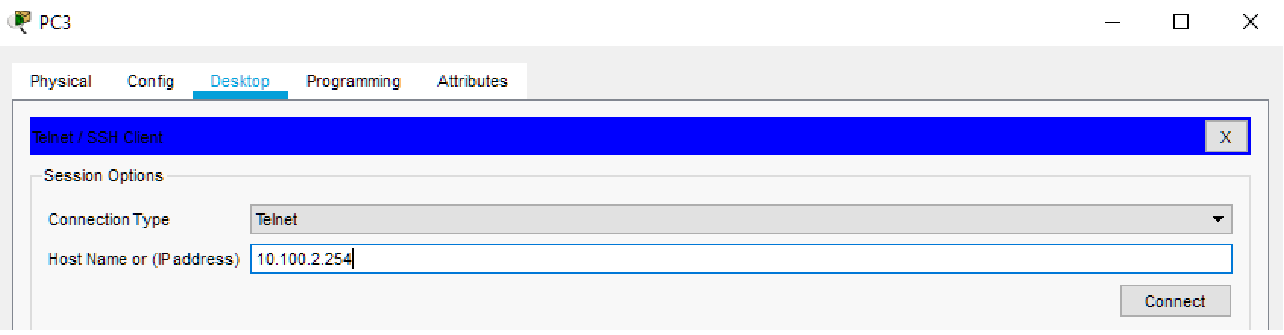


```
line con 0
!
line aux 0
!
line vty 0 4
 password 7 0823595C0812
 login
!
!
!
end
```

In this way, Someone entering the "show running-config" command will not be able to see the password set for telnet in plain text.

6. Now you are ready to telnet (from your PC) to another remote Routers. Enter their telnet and enable passwords and login to their router. Use show user command to display logged-in connections on the router in this session. Observe your IP address. The * shows your connection. NOTE: If you jump from that Router to another one, that is called reverse telnet. You can use the exit command for terminating the telnet session.

As you can see here, we telnet from PC3 to Router2.

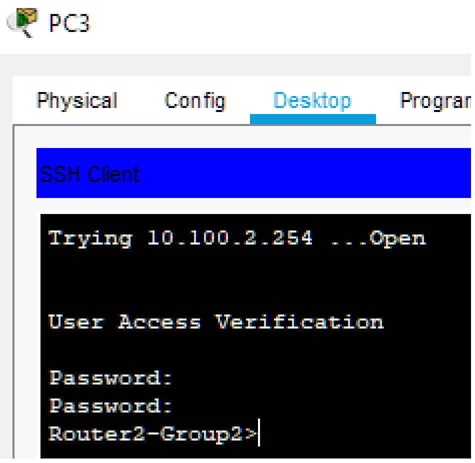


Telnet / SSH Client

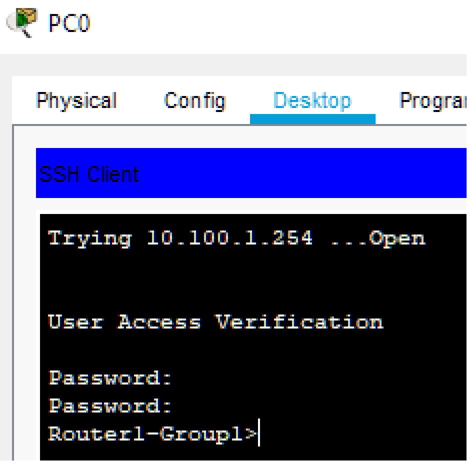
Session Options

Connection Type: Telnet

Host Name or (IP address): 10.100.2.254



```
Trying 10.100.2.254 ...Open


User Access Verification

Password:
Password:
Router2-Group2>
```

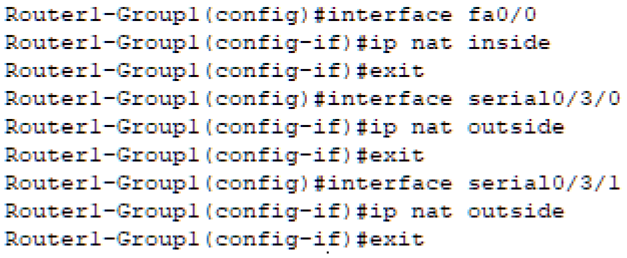


```
Trying 10.100.1.254 ...Open


User Access Verification

Password:
Password:
Router1-Group1>
```

We were able to successfully telnet to Router2-Group2 device from both PC3 and PC0. We observed that when we entered the "mehmet" password we set for this device, we could access the device's interface.

7. If a router supports address translation (if it has an address translation software), then the connection interfaces to which the address translation is to be applied, must be specified and defined as inside or outside. This is done using the ip nat [inside | outside] command while in the sub-configuration mode.

While defining Network Address Translation (NAT) for each router, we used the "ip nat inside" command because the FastEthernet connection interfaces of the routers specify the local network to which the computers are connected, and the "ip nat outside" command for the Serial connection interfaces.

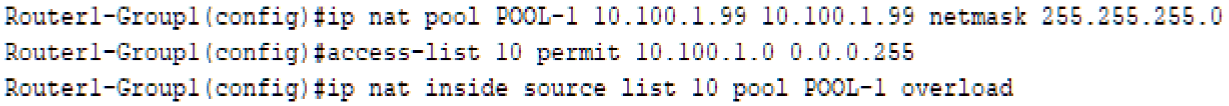


```
Router1-Group1(config)#interface fa0/0
Router1-Group1(config-if)#ip nat inside
Router1-Group1(config-if)#exit
Router1-Group1(config)#interface serial0/3/0
Router1-Group1(config-if)#ip nat outside
Router1-Group1(config-if)#exit
Router1-Group1(config)#interface serial0/3/1
Router1-Group1(config-if)#ip nat outside
Router1-Group1(config-if)#exit
```

8. You are going to configure dynamic overloading NAT. Commands are the same as dynamic NAT configuration with overload command at the end. You should translate your client IP to another IP from your subnet (for example: 10.100.X.99) using dynamic overloading NAT commands.

When overloading is configured, the device maintains enough information from higher-level protocols (for example, TCP or UDP port numbers). This action translates the global address back to the correct local address. When multiple local addresses map to one global address, the TCP or UDP port numbers of each inside host distinguish between local addresses.

We entered the IP addresses of 10.100.x.99 specified in the PDF in the "beginningIP" and "endingIP" parameters in the first command we used here. We have defined our "poolName" command as "POOL-1" in a way that is separate for Router1-Group1 and compatible with the group number 1. In our "access-list" command, we entered our "listNo" parameter as "10" for Router1-Group1. For our "net / subnet IP" command, we gave the network IP address of the computers in the local networks covered by the Router1-Group1.

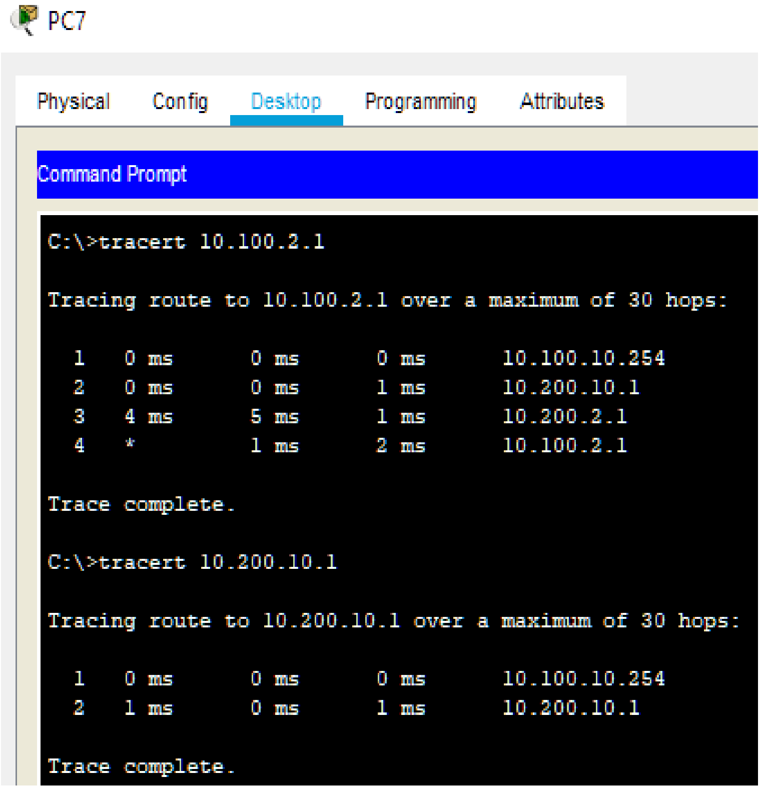


```
Router1-Group1(config)#ip nat pool POOL-1 10.100.1.99 10.100.1.99 netmask 255.255.255.0
Router1-Group1(config)#access-list 10 permit 10.100.1.0 0.0.0.255
Router1-Group1(config)#ip nat inside source list 10 pool POOL-1 overload
```

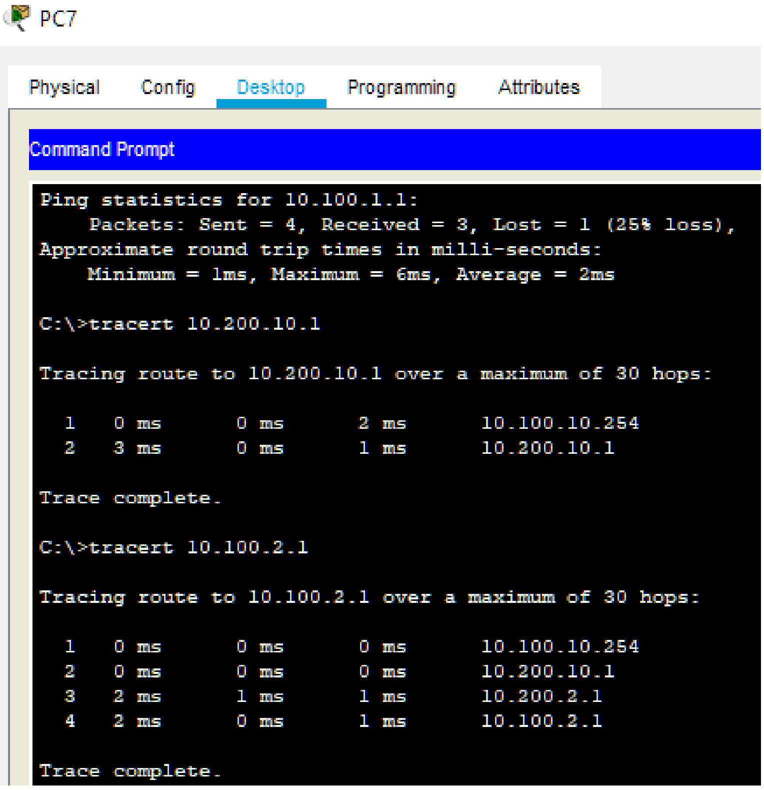
9. After NAT configuration, try to ping other groups client IP addresses and translated IP addresses. Discuss the results.

There are the screenshots of NAT applied to the topology:

1. **Tracerouting from PC7 to PC2 and Router1-Group1.**



```
C:\>tracert 10.100.2.1

Tracing route to 10.100.2.1 over a maximum of 30 hops:

  1   0 ms      0 ms      0 ms      10.100.10.254
  2   0 ms      0 ms      1 ms      10.200.10.1
  3   4 ms      5 ms      1 ms      10.200.2.1
  4   *         1 ms      2 ms      10.100.2.1

Trace complete.

C:\>tracert 10.200.10.1

Tracing route to 10.200.10.1 over a maximum of 30 hops:

  1   0 ms      0 ms      0 ms      10.100.10.254
  2   1 ms      0 ms      1 ms      10.200.10.1

Trace complete.
```



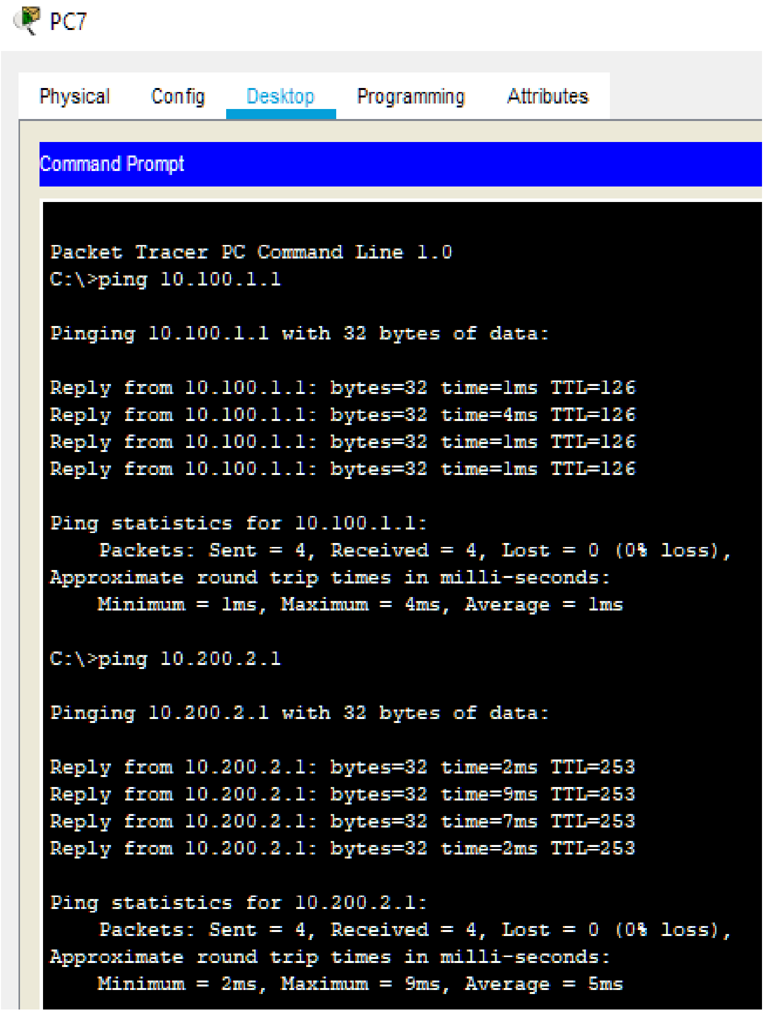
```
Ping statistics for 10.100.1.1:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 6ms, Average = 2ms

C:\>tracert 10.200.10.1

Tracing route to 10.200.10.1 over a maximum of 30 hops:

  1   0 ms      0 ms      2 ms      10.100.10.254
  2   3 ms      0 ms      1 ms      10.200.10.1

Trace complete.

C:\>tracert 10.100.2.1

Tracing route to 10.100.2.1 over a maximum of 30 hops:

  1   0 ms      0 ms      0 ms      10.100.10.254
  2   0 ms      0 ms      0 ms      10.200.10.1
  3   2 ms      1 ms      1 ms      10.200.2.1
  4   2 ms      0 ms      1 ms      10.100.2.1

Trace complete.
```

BEFORE NAT

AFTER NAT

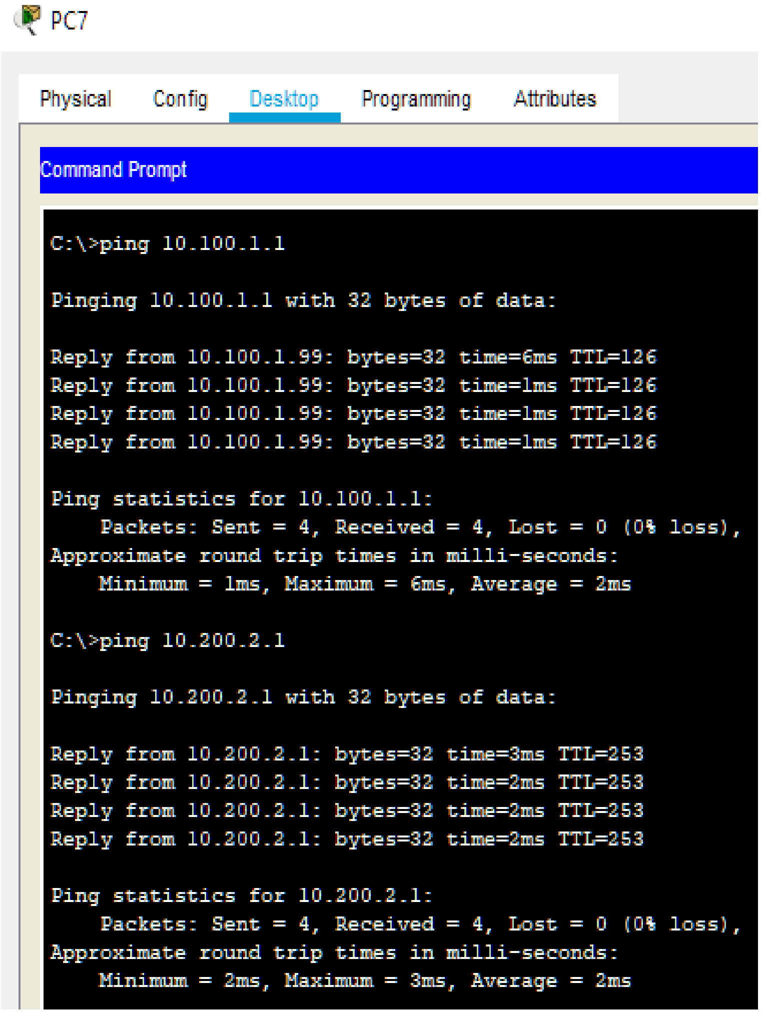
Since we only apply NAT operation to Router1-Group1 device, this process only affects pings that will be thrown to the local network covered by the device. Since PC2 belongs to Router2-Group2 device, we did not expect any changes in the traceroute process. Since Router1-Group1 device is the center of the NAT operation, there was no change in the traceroute process on this device.

2. Pinging from PC7 to PC0 and Router2-Group2.



```
Packet Tracer PC Command Line 1.0
C:\>ping 10.100.1.1

Pinging 10.100.1.1 with 32 bytes of data:

Reply from 10.100.1.1: bytes=32 time=1ms TTL=126
Reply from 10.100.1.1: bytes=32 time=4ms TTL=126
Reply from 10.100.1.1: bytes=32 time=1ms TTL=126
Reply from 10.100.1.1: bytes=32 time=1ms TTL=126

Ping statistics for 10.100.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 4ms, Average = 1ms

C:\>ping 10.200.2.1

Pinging 10.200.2.1 with 32 bytes of data:

Reply from 10.200.2.1: bytes=32 time=2ms TTL=253
Reply from 10.200.2.1: bytes=32 time=9ms TTL=253
Reply from 10.200.2.1: bytes=32 time=7ms TTL=253
Reply from 10.200.2.1: bytes=32 time=2ms TTL=253

Ping statistics for 10.200.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 9ms, Average = 5ms
```

BEFORE NAT



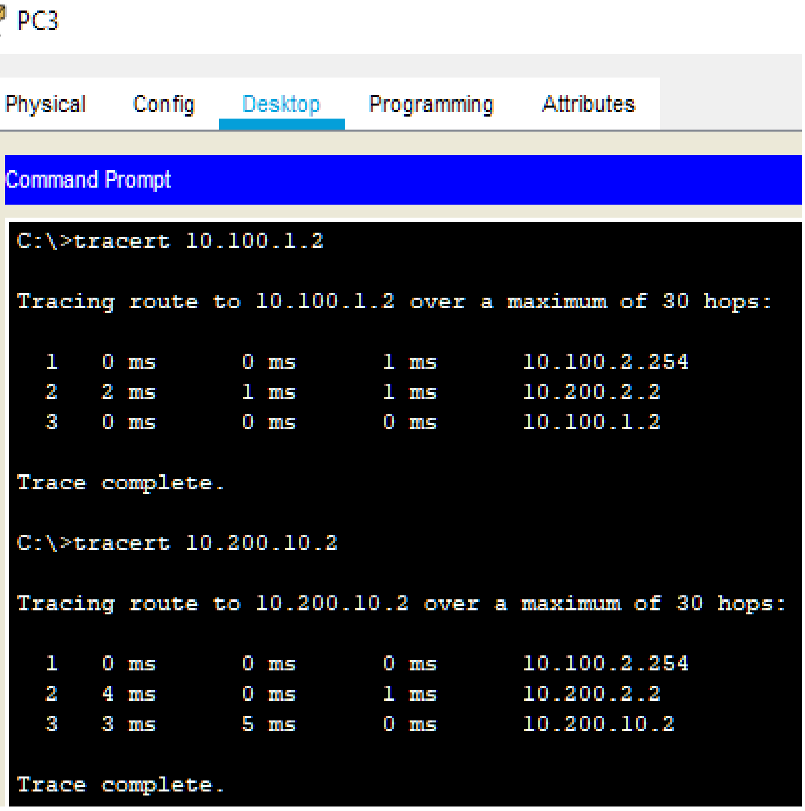
```
C:\>ping 10.100.1.1

Pinging 10.100.1.1 with 32 bytes of data:

Reply from 10.100.1.99: bytes=32 time=6ms TTL=126
Reply from 10.100.1.99: bytes=32 time=1ms TTL=126
Reply from 10.100.1.99: bytes=32 time=1ms TTL=126
Reply from 10.100.1.99: bytes=32 time=1ms TTL=126

Ping statistics for 10.100.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 6ms, Average = 2ms

C:\>ping 10.200.2.1

Pinging 10.200.2.1 with 32 bytes of data:

Reply from 10.200.2.1: bytes=32 time=3ms TTL=253
Reply from 10.200.2.1: bytes=32 time=2ms TTL=253
Reply from 10.200.2.1: bytes=32 time=2ms TTL=253
Reply from 10.200.2.1: bytes=32 time=2ms TTL=253

Ping statistics for 10.200.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 3ms, Average = 2ms
```

AFTER NAT

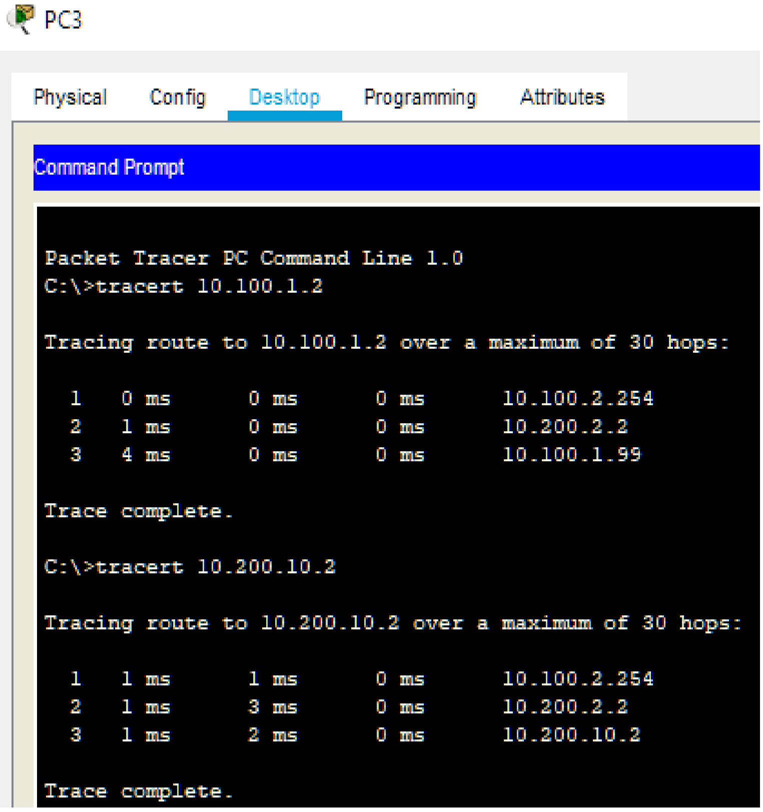
In this scenario, we did not expect a change in the ping process because we did not apply NAT to Router2-Group2 device and there was no change. However, if we look at the PC0 device, we notice a change in the IP address during the ping process, since PC0 is connected to the network created by Router1-Group1 device. While the reply returned before the NAT application is returned from the IP address 10.100.1.1, the response after the NAT application is returned from the IP address 10.100.1.99, which is the NAT address of Router1-Group1.

From here, we can understand that although PC0 has an IP address of 10.100.1.1, it is connected to the Router1-Group1 device, so the exit IP address from the local network is different. This case summarizes why the NAT operation is done.

3. Traceroute from PC3 to PC1 and Router3-Group10



```
C:\>tracert 10.100.1.2

Tracing route to 10.100.1.2 over a maximum of 30 hops:

  1   0 ms      0 ms      1 ms      10.100.2.254
  2   2 ms      1 ms      1 ms      10.200.2.2
  3   0 ms      0 ms      0 ms      10.100.1.2

Trace complete.

C:\>tracert 10.200.10.2

Tracing route to 10.200.10.2 over a maximum of 30 hops:

  1   0 ms      0 ms      0 ms      10.100.2.254
  2   4 ms      0 ms      1 ms      10.200.2.2
  3   3 ms      5 ms      0 ms      10.200.10.2

Trace complete.
```



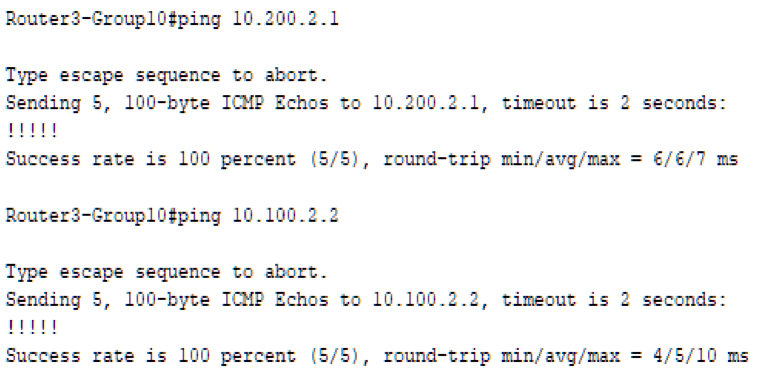
```
Packet Tracer PC Command Line 1.0
C:\>tracert 10.100.1.2

Tracing route to 10.100.1.2 over a maximum of 30 hops:

  1   0 ms     0 ms     0 ms     10.100.2.254
  2   1 ms     0 ms     0 ms     10.200.2.2
  3   4 ms     0 ms     0 ms     10.100.1.99

Trace complete.

C:\>tracert 10.200.10.2

Tracing route to 10.200.10.2 over a maximum of 30 hops:

  1   1 ms     1 ms     0 ms     10.100.2.254
  2   1 ms     3 ms     0 ms     10.200.2.2
  3   1 ms     2 ms     0 ms     10.200.10.2

Trace complete.
```

BEFORE NAT **AFTER NAT**

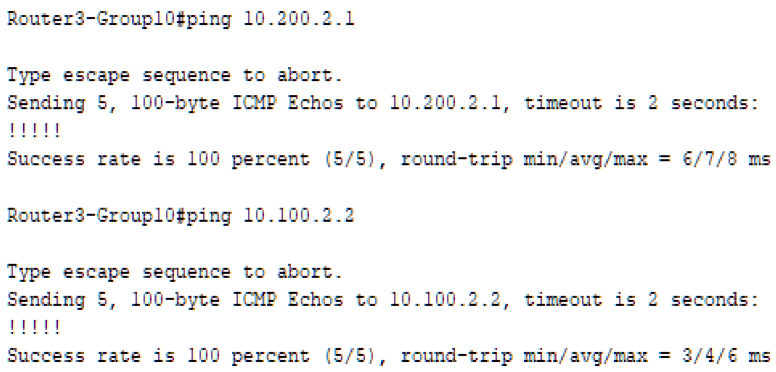
In our third scenario, we perform the traceroute process from PC3 to PC1 and Router3-Group10 devices. In the traceroute process made to PC1, the 3.hop before NAT is applied and the 3.hop part after NAT is different on both sides. While we see the IP address of PC1 (10.100.1.2) before NAT is applied, we see the NAT IP address (10.100.1.99) that we gave to Router1-Group1 after NAT is applied.

There is no change in the traceroute process made to the Router3-Group10 device.

4. Pinging from Router3-Group10 to Router2-Group2 and PC3.



```
Router3-Group10#ping 10.200.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.200.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 6/6/7 ms

Router3-Group10#ping 10.100.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.100.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/5/10 ms
```



```
Router3-Group10#ping 10.200.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.200.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 6/7/8 ms

Router3-Group10#ping 10.100.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.100.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/4/6 ms
```

BEFORE NAT **AFTER NAT**

In our last test, we tried to ping Router2-Group2 and PC3 devices from Router3-Group10 device. However, both of our observations ended with similar results, as no NAT process was applied to any of these devices.

To sum everything up, if we compare before and after the NAT application, after the NAT configuration and Access-list definitions we made on the Router1-Group1, **we saw the following:**

1) PC-to-PC Communication: While everything remained as it is in the communication between computers in general, the following point came to our attention after the NAT operation: We saw that the reply IP addresses changed after the pings sent to the computers belonging to the Router1-Group1 device on which we applied the NAT operation. The computers returned with their own IP addresses before the NAT was applied, and after the NAT operation, it started to reply from the IP address 10.100.1.99. On the other hand, no changes were observed on computers that do not have NAT operation.

2) Router-to-Router Communication: In the form of communication between routers, no changes were observed before and after NAT was applied. Because NAT process is a process that affects the network inside the routers. Therefore, "Router to Router" style ping operations continue as before.

3) Router-to-PC Communication: Since the reply IP address does not appear in the ping process performed over routers, we cannot make a comment. However, in the traceroute process made to computers belonging to Router1-Group1 device, we notice changes in IP addresses. While the computers' own IP addresses were visible before the NAT was applied, we see the 10.100.1.99 IP address we determined after the NAT was applied.

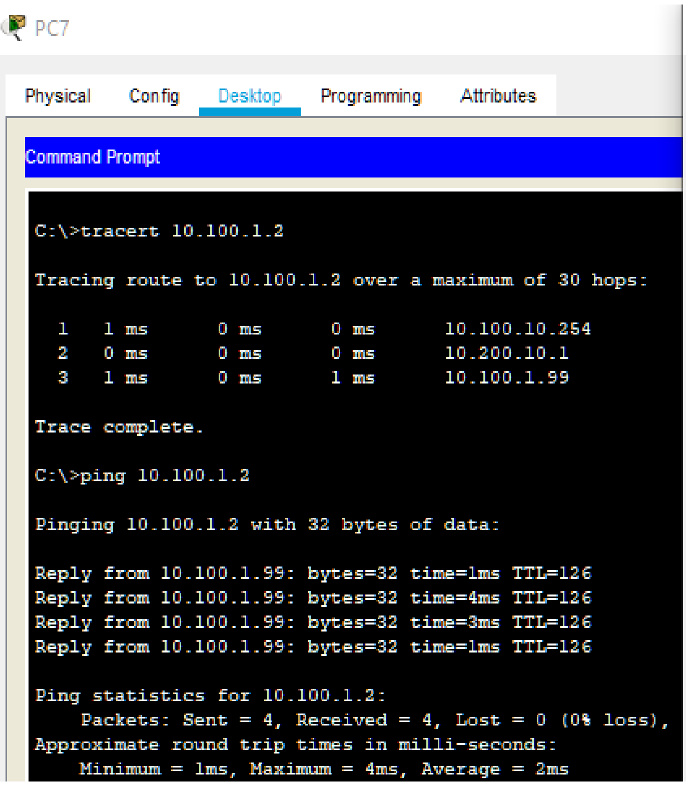
10. Use show ip nat translation command to show translated IP addresses and port numbers. Discuss each column on the table (inside/outside, local/global). If you didn't see any output, you should successfully ping remote clients and also your PC should be pinged from outside.

Inside local address: An IP address that is assigned to a host on the inside network. The address that the Network Information Center (NIC) or service provider assigns is probably not a legitimate IP address.

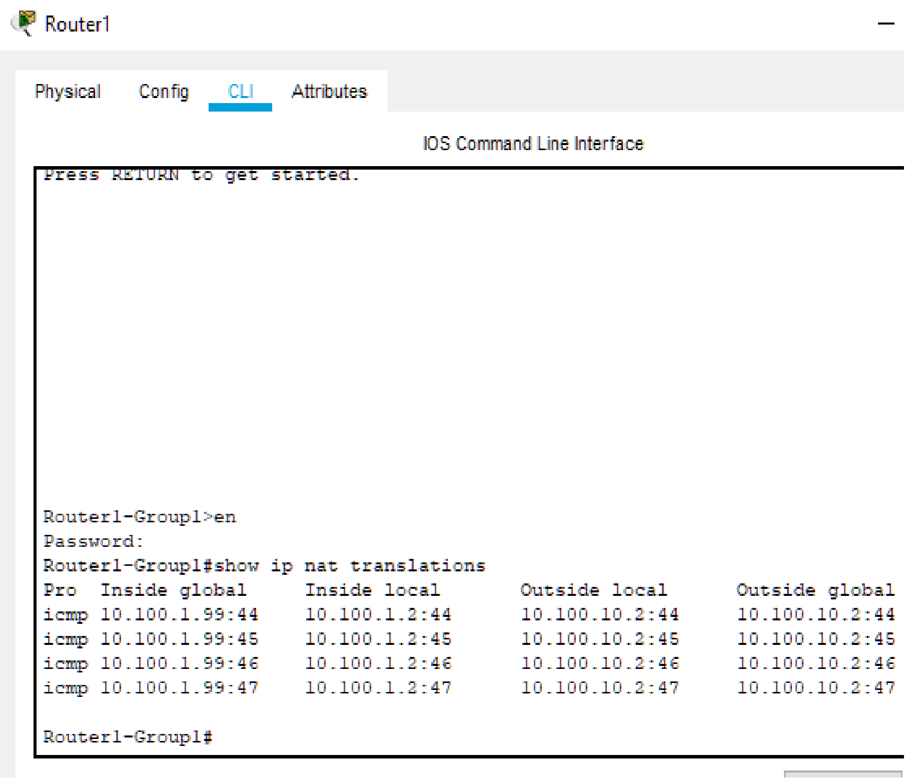
Inside global address: A legitimate IP address assigned by the NIC or service provider that represents one or more inside local IP addresses to the outside world.

Outside local address: The IP address of an outside host as it appears to the inside network. Not necessarily a legitimate address, it is allocated from the address space that is routable on the inside.

Outside global address: The IP address that is assigned to a host on the outside network by the owner of the host. The address is allocated from a globally routable address or network space.



```
C:\>tracert 10.100.1.2

Tracing route to 10.100.1.2 over a maximum of 30 hops:

  1   1 ms      0 ms      0 ms      10.100.10.254
  2   0 ms      0 ms      0 ms      10.200.10.1
  3   1 ms      0 ms      1 ms      10.100.1.99

Trace complete.

C:\>ping 10.100.1.2

Pinging 10.100.1.2 with 32 bytes of data:

Reply from 10.100.1.99: bytes=32 time=1ms TTL=126
Reply from 10.100.1.99: bytes=32 time=4ms TTL=126
Reply from 10.100.1.99: bytes=32 time=3ms TTL=126
Reply from 10.100.1.99: bytes=32 time=1ms TTL=126

Ping statistics for 10.100.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 4ms, Average = 2ms
```

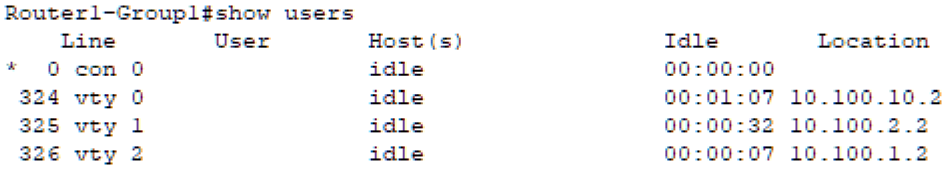


```
Press RETURN to get started.







Router1-Group1>en
Password:
Router1-Group1#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 10.100.1.99:44    10.100.1.2:44      10.100.10.2:44     10.100.10.2:44
icmp 10.100.1.99:45    10.100.1.2:45      10.100.10.2:45     10.100.10.2:45
icmp 10.100.1.99:46    10.100.1.2:46      10.100.10.2:46     10.100.10.2:46
icmp 10.100.1.99:47    10.100.1.2:47      10.100.10.2:47     10.100.10.2:47

Router1-Group1#
```

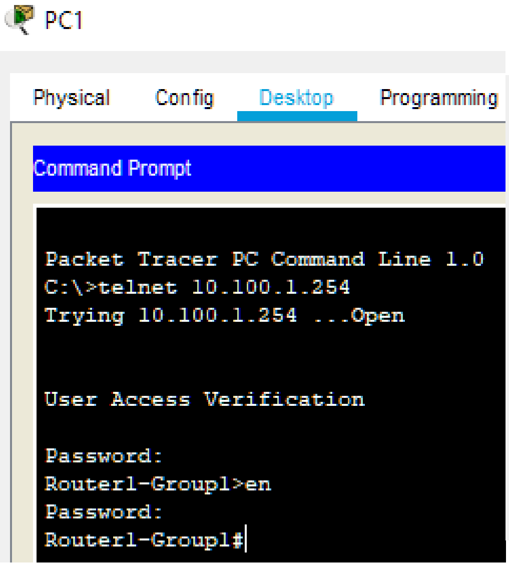
As we have observed before, even though we ping the IP address 10.100.1.2 from PC7 to PC1, our IP address is 10.100.1.99. This explains the NAT process.

11. Finally, connect to other remote Routers using telnet, and display connected users and observe your IP address.

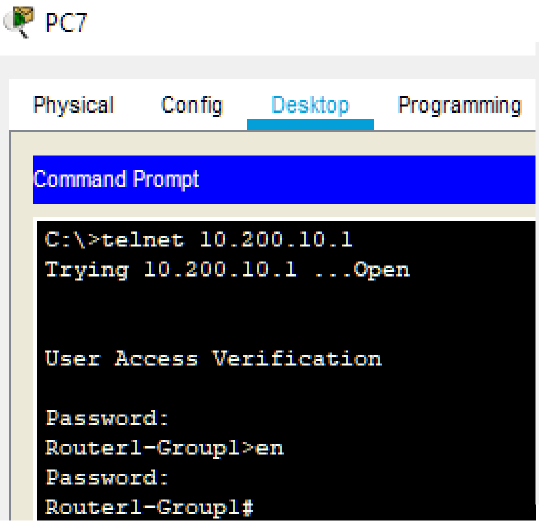
We made a telnet connection to Router1-Group1 device from computers belonging to all different networks. Then we ran the "show users" command. Connections 324, 325, and 326 represent remote telnet connections via computers.



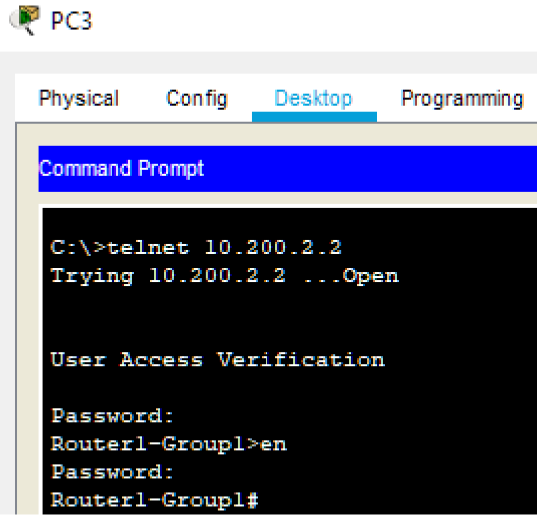
```
Router1-Group1#show users
    Line       User       Host(s)              Idle       Location
*   0 con 0               idle                 00:00:00
 324 vty 0                idle                 00:01:07 10.100.10.2
 325 vty 1                idle                 00:00:32 10.100.2.2
 326 vty 2                idle                 00:00:07 10.100.1.2
```



```
Packet Tracer PC Command Line 1.0
C:\>telnet 10.100.1.254
Trying 10.100.1.254 ...Open


User Access Verification

Password:
Router1-Group1>en
Password:
Router1-Group1#
```



```
C:\>telnet 10.200.10.1
Trying 10.200.10.1 ...Open


User Access Verification

Password:
Router1-Group1>en
Password:
Router1-Group1#
```



```
C:\>telnet 10.200.2.2
Trying 10.200.2.2 ...Open


User Access Verification

Password:
Router1-Group1>en
Password:
Router1-Group1#
```