ZUCTI

كلية الإبتكار التقني

COLLEGE OF TECHNOLOGICAL INNOVATION

NET-351 PROJECT PROGRESS

Solving Telnet security by Remote Access VPN

Shamma Rashed Alhameli
Noof Jasem Al Hammadi
Zayed University
Dr. Anwer Al-Dulaimi
November 19, 2023

Table of Contents

1. Introduction

Problem Identification

There has been a noticeable increase in the growth and demand for businesses and organizations in recent times. As a result, many organizations are opening new locations locally or across the globe. The pandemic's consequences caused a dramatic fundamental shift in the way businesses operate, with many choosing to allow remote work settings. This involves providing staff members remote access to databases and files so they can carry out their duties from different places. At the same time, several private businesses are taking steps to improve security by hiding the origins and destinations of their remote work activities.

Even with strong safety measures established for remote internet log-ins, enterprises are still vulnerable to sophisticated cyber threats like Man-in-the-Middle (MitM) attacks. These kinds of attacks represent a significant risk to enterprises that conduct remote operations because they involve an unauthorized party intercepting and perhaps changing communication between two parties. Therefore, even with careful safeguards, companies need to be on the lookout for new dangers and constantly strengthen their cybersecurity procedures to protect themselves in the digital world.

Project Business Objectives

1. Enhanced Protection:

- Data Encryption: By encrypting data as it travels between a remote device and the network, virtual private networks (VPNs) guarantee that confidential data is safe from prying eyes and illegal access.

- Safe Verification: Strong authentication techniques are frequently used by VPNs to further secure remote access.

2. Remote Access Security:

- Access Control: VPNs offer remote users a safe entry point, limiting direct access to internal systems and resources to those who possess the necessary credentials. This lowers the possibility of unwanted access.

- Private Connection: To prevent data from being intercepted via public networks, users connect to the organization's network via a private, encrypted tunnel.

3. Local Adaptability:

- International Accessibility: By enabling authorized users to access the company's network from almost anywhere in the world, remote management with VPN promotes flexible work arrangements and international collaboration.

Although using a VPN for remote management has many advantages, there are potential risks involved with remote access. To reduce these risks, it's important to put in place appropriate security measures, update configurations often, and train users on best practices.

Project Requirements

Our project was implemented on Packet Tracer. However, this project can be implemented in real-life enterprise networks as well. The following list is all the devices and wires used in the Packet Tracer simulation:

1. Routers:

   - Model: 1941

   - Quantity: 3

   - Routers are necessary to link several networks together. They are crucial in an organization's configuration for data routing between various departments or network segments.

2. Switch:

   - Model:2960

- Quantity: 1

- By connecting devices on the same network, switches are used to establish local area networks (LANs). They are essential for controlling and maximizing data flow inside a network and function at Layer 2 of the OSI architecture.

3. PCs:

- Model: Undefined

- Quantity: 2

- PCs are end-user devices that usually use the network to access resources and run software. They stand in for the gadgets that users use to communicate with the network.

4. Server:

- Model: Not specified

- Quantity:1

- Servers are specialized computers that offer resources or services to other networked devices. Email, web hosting, file storage, and other common server tasks are available.

5. DCE Serial Wires:

- Quantity: 2

- Routers and other serial devices are connected via Data Communications Equipment (DCE) serial wires. When it comes to creating serial communication linkages, they are essential.

6. Copper Cross-over Wire:

- Quantity: 1

- Crossover cables are employed when two similar devices need to be directly connected, like when two PCs or switches are connected. They allow devices of the same type to communicate with one other by flipping the transmit and receive pin assignments.

7. Straight-through copper wire:

   - Quantity: 3

   - Goal: Straight-through cables are frequently used to link various kinds of equipment together, including a PC and a switch or a router and a switch.

Scalability, security, and redundancy considerations should be taken into account when upgrading to an actual enterprise network. Depending on the demands of the company, more devices and technologies may need to be integrated.

2. Literature review:

What is Remote management?

Remote management is a thorough method for managing and controlling the IT systems, services, and group of a company from a distance. To ensure best performance, privacy, and consistency, IT organizations are often monitored, managed, and maintained using innovative technologies, and special service providers.

Remote management controls have been very famous because of their productivity, economy of cost, and flexibility in the expanding patterns of collaborative teams and working remotely [2]. Additionally, Telnet is one of the most used protocol for the remote access and management.

What is Telnet?

Telnet is a remote management protocol is an internet protocol between clients and servers that uses connections through TCP for transmitting information. In addition, Telnet enables written input as well as output for remotely managing the device. Moreover, the computer device serves as a computer and accepts controls across a TCP port between clients and servers, which is automatically created for this purpose [4].

Telnet implementation and security:

In a telnet, there is no ciphering or encryption for the packets being transmitted, which means all the packet and payload is in clear text, which makes it unsecure because all the data when it is transferred over the untrusted network it is exposed to network attacks that many intercept and read or replay to the message or packet begin sent [7].

According to the research [8] and implementation [10], the protocol that could be handled by network devices is Telnet, which is widely used for distant internet login on web browser while working remotely. It can open many internet applications and it can run on many types of operating systems. In addition, it uses channel 23 on the Transmission Control Protocol. Moreover, Devices such as switches and routers can be configured and managed distance remotely with Telnet. It gives a standard connection for communication input and output devices it features an interactive communication method and many language sets. As an example, we can control windows settings computer remotely while we are far away in distance.

Dalian Cyber Security's February 11, 2020, article titled "Early Warning: 510 thousand Servers, Routers, and IoT Devices Face Telnet Password Leak, IoT DDoS Threat Looms" highlights a significant security concern. The report reveals that around 100,000 internet users' information, including servers, switches, routers, and IoT devices, was leaked in early 2020 from a forum. The leaked data, totalling 14.5 megabytes in 16 txt files, exposes vulnerabilities. The essay suggests that hackers are likely using scripts to scan port 23 globally, exploiting weak passwords through blasting. The author conducted tests on leaked data, presenting screenshots indicating that common weak passwords are susceptible, raising concerns about potential IoT DDoS attacks [8].

One solution is to run the telnet protocol over the SSH “Secure-Shell” protocol which will add encryption for the packets and messages being transmitted. Another solution is our implantation of remote management using VPN.

What are common types of remote access protocols?

Protocols for remote access assist with controlling the link between a machine located miles away and a server that is far away. Standard methods for remote access consist of:

Point-to-Point Protocol (PPP): is a protocol that allows a line of computers to be connected directly to one another. PPP is extensively utilized in fast-speed and high-load internet networking.

Internet Protocol Security (IPsec): can be configured as remote management and it is a protected network, so the internal protocol security used data encryption and authentication to ensure that the network was connected to another one.

Point-to-Point Tunneling Protocol (PPTP): is a protocol where we apply the secure gateway through open networks. Because of several security holes, it is currently regarded as outdated.

Remote Access Services (RAS): is when individuals can establish an immediate broadband system or a secure VPN connection to the business system from another location [3].

What is VPN?

VPN stands for virtual private network. The VPN gives you the chance to connect through the network in a private connection while you are connected in a public network such as a mall, cafe, etc. VPNs hide your character on the web while you are online and secure your internet activity. This increases the difficulty level for anyone else to monitor how you use the web and steal information because of the security of the VPN [1].

What are the benefits of VPN?

VPN has many benefits, one of them is cryptography where a secret key is required to access the information. In the case of an attack with brute force, machines would need many years to decode the programming in the absence of one. a variety of unsecured networks, your browsing history is unknown because of the use of a VPN.

Another benefit of the VPN is the protection of the transmitted information when working remotely, you may require access to vital files within your company's network. To ensure the security of this data, it is imperative that it is transmitted through a secure channel. Typically, a VPN connection is essential for gaining access to the network. VPN services mitigate the risk of data leakage by connecting to private servers and employing encoding methods [1].

What are the protocols of VPN?

Some of the VPN protocols are Internet Protocol Security (IPsec) which is a VPN tunnelling protection that protects the information transfer by implementing session verification and packet encryption. The encryption communication is contained within the information packet and undergoes additional encryption layers. The internet protocol security uses VPN site-to-site configurations a lot because of its excellent adaptability and ability to merge with different protocols for additional protection.

Another protocol is SSL and TLS, which are secure versions of HTTP websites that are protected by encryption using a similar representation, which is called the Secure

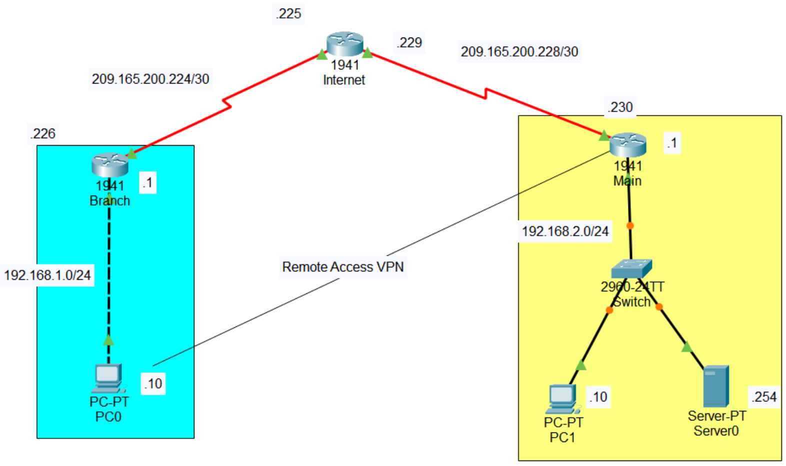
Sockets Level and Transmit Level Safety Protocols. So, customer access is restricted to particular apps and not to whole networks, with the internet navigator serving as a customer device. Furthermore, nearly all applications are often needed because SSL and TLS links are built into practically all web pages. VPNs for access from afar typically employ SSL and TLS [6].

How our project implementation solves telnet issue?

Overall, VPN allows encapsulation, encryption and Telnet allows remote management, they both perform multiple purposes. Whereas Telnet is primarily made for controlling machines from afar within an organization, VPNs are more often connected to providing confidentiality and security for basic internet activities. Telnet is not secure since it sends the information as clear text without encryption. However, our implementation is using both the remote access as well as security as encryption and encapsulation using VPN. Additionally, not all VPNs can encrypt the data some only encrypts the header other encrypts both data and header.

3. Network Design:

For our network design, although we implemented the project on a small main-branch organization, the remote management VPN can be implemented on a larger network.



We chose to have a main business branch which is highlighted in yellow, a second branch is a different geographical place highlighted in blue and a router representing the internet connecting the two branches.

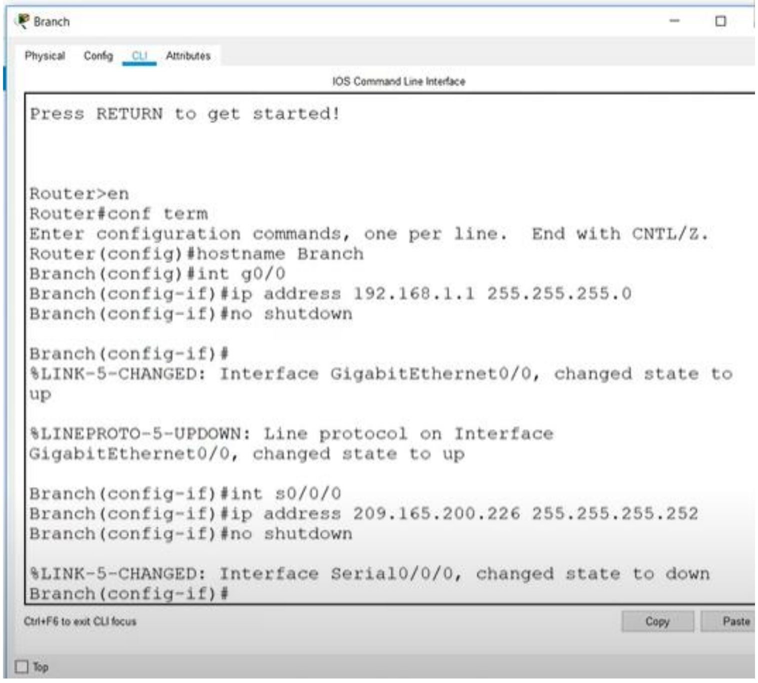
Device	IP address
Branch Router	G0/0:192.168.1.1 /24 S0/0/0:209.165.200.226 /30
Internet Router	S0/0/0:209.165.200.225 /30 S0/0/1:209.165.200.229 /30
Main router	G0/0:192.168.2.1 /24 S0/0/1:209.165.200.230 /30
Server	IP: 192.168.2.254/24 Default gateway: 192.168.2.1
PC-0	IP: 192.168.1.10/24 Default gateway: 192.168.1.1
PC-1	IP: 192.168.2.10/24 Default gateway: 192.168.2.1

4. Network Implementation:

Basic configuration:

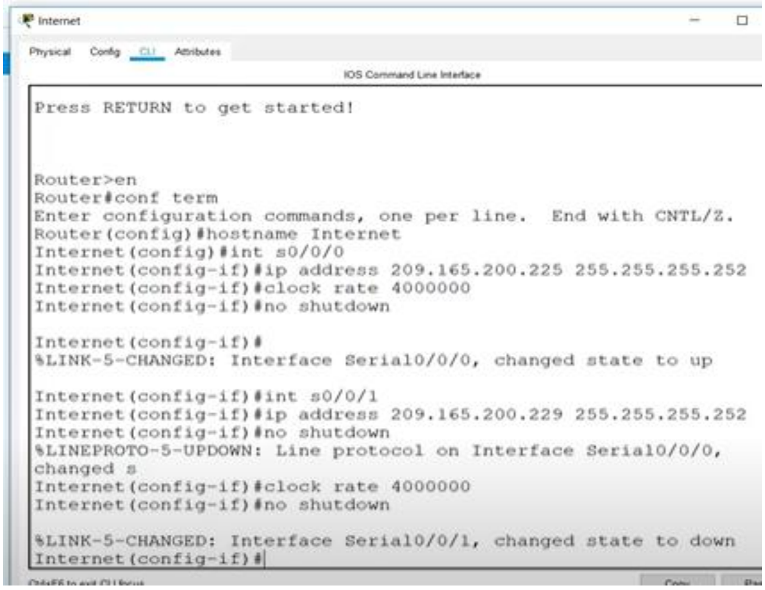
All the basic configuration is assigning the IP address and subnet for each interface.

1- We configured the Branch router.



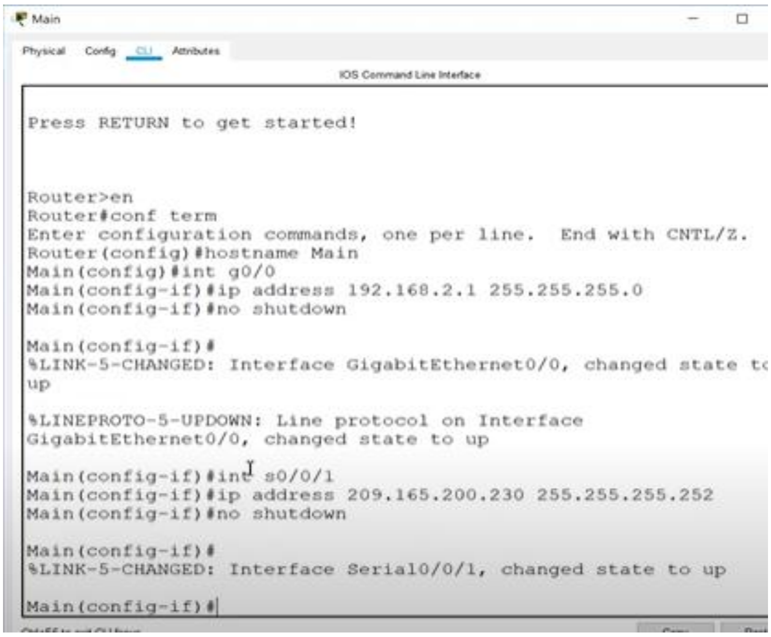
```
Press RETURN to get started!


Router>en
Router#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname Branch
Branch(config)#int g0/0
Branch(config-if)#ip address 192.168.1.1 255.255.255.0
Branch(config-if)#no shutdown

Branch(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to
up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0, changed state to up

Branch(config-if)#int s0/0/0
Branch(config-if)#ip address 209.165.200.226 255.255.255.252
Branch(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
Branch(config-if)#
```

2- we configured the Internet router.



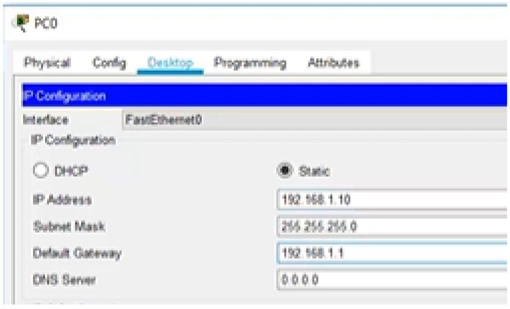
```
Press RETURN to get started!


Router>en
Router#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname Internet
Internet(config)#int s0/0/0
Internet(config-if)#ip address 209.165.200.225 255.255.255.252
Internet(config-if)#clock rate 4000000
Internet(config-if)#no shutdown

Internet(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

Internet(config-if)#int s0/0/1
Internet(config-if)#ip address 209.165.200.229 255.255.255.252
Internet(config-if)#no shutdown
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0,
changed s
Internet(config-if)#clock rate 4000000
Internet(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
Internet(config-if)#
```

3-We configured the Main router



```
Press RETURN to get started!


Router>en
Router#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname Main
Main(config)#int g0/0
Main(config-if)#ip address 192.168.2.1 255.255.255.0
Main(config-if)#no shutdown

Main(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to
up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0, changed state to up

Main(config-if)#int s0/0/1
Main(config-if)#ip address 209.165.200.230 255.255.255.252
Main(config-if)#no shutdown

Main(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

Main(config-if)#
```

4- We did the IP configurations on the PCs and server assigning their IP address, subnet, and the default gateway.



Interface: FastEthernet0

IP Configuration

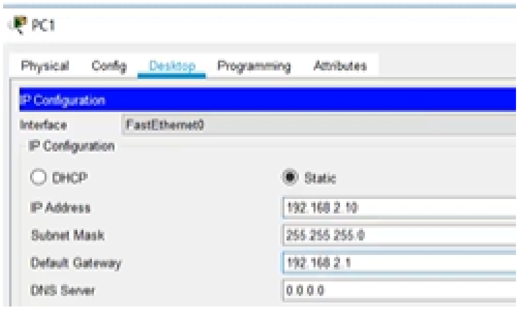
○ DHCP ● Static

IP Address: 192.168.1.10

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.1

DNS Server: 0.0.0.0



Interface: FastEthernet0

IP Configuration

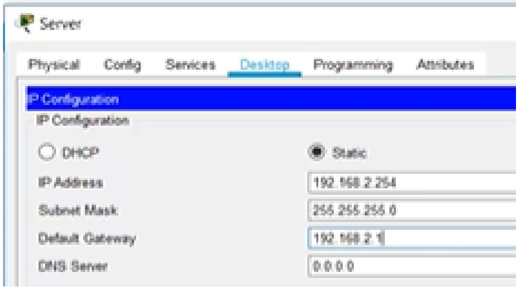
○ DHCP ● Static

IP Address: 192.168.2.10

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.2.1

DNS Server: 0.0.0.0



IP Configuration

○ DHCP ● Static

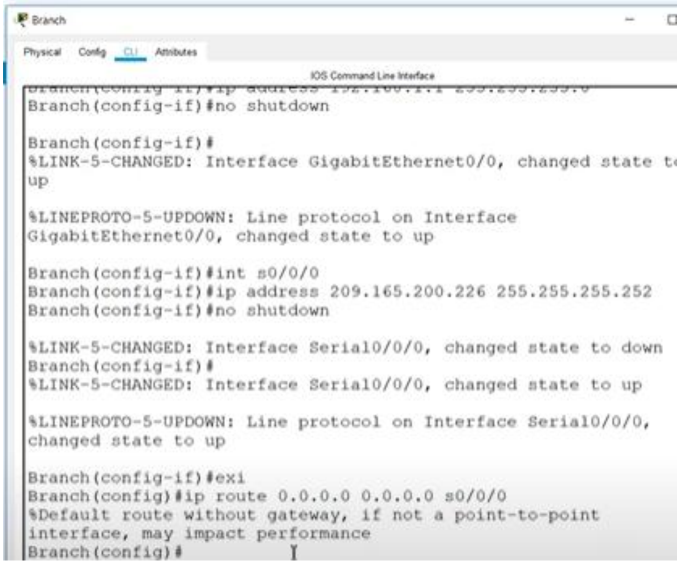
IP Address: 192.168.2.254

Subnet Mask: 255.255.255.0

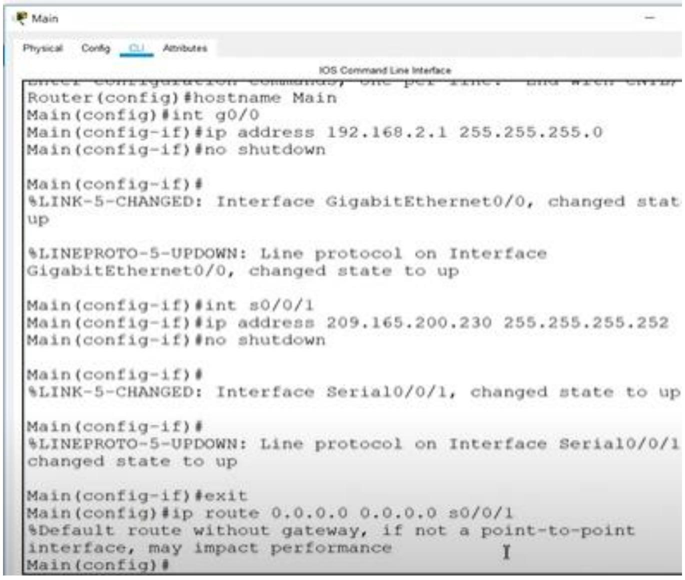
Default Gateway: 192.168.2.1

DNS Server: 0.0.0.0

5- Configuring the static router on the main and branch router:

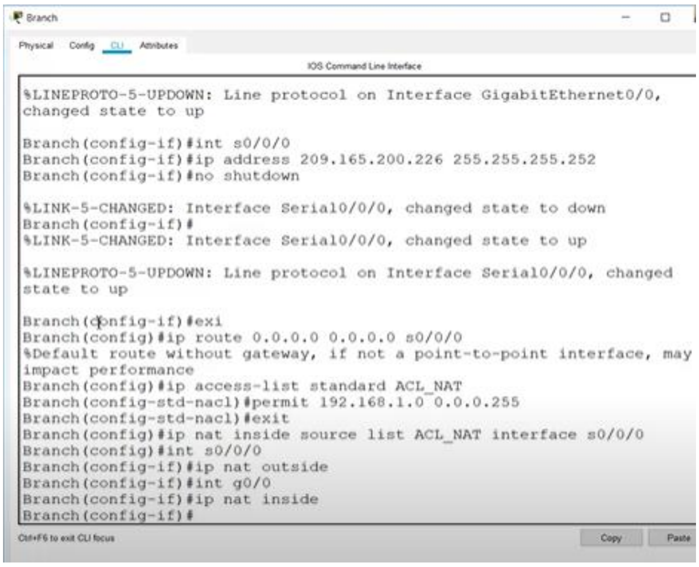


```
Branch(config-if)#no shutdown

Branch(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state t
up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0, changed state to up

Branch(config-if)#int s0/0/0
Branch(config-if)#ip address 209.165.200.226 255.255.255.252
Branch(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
Branch(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0,
changed state to up

Branch(config-if)#exi
Branch(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0
%Default route without gateway, if not a point-to-point
interface, may impact performance
Branch(config)#
```



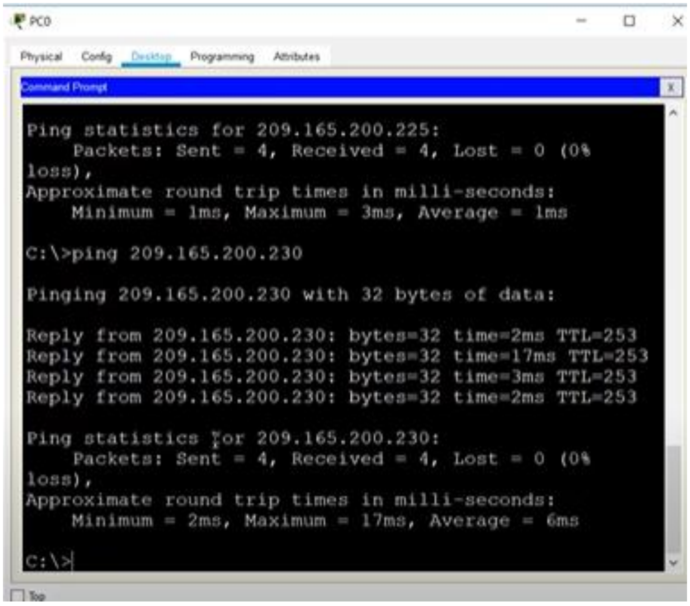
```
Router(config)#hostname Main
Main(config)#int g0/0
Main(config-if)#ip address 192.168.2.1 255.255.255.0
Main(config-if)#no shutdown

Main(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed stat
up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0, changed state to up

Main(config-if)#int s0/0/1
Main(config-if)#ip address 209.165.200.230 255.255.255.252
Main(config-if)#no shutdown

Main(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

Main(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1
changed state to up

Main(config-if)#exit
Main(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1
%Default route without gateway, if not a point-to-point
interface, may impact performance
Main(config)#
```

6-Configuring NAT on the Branch router:



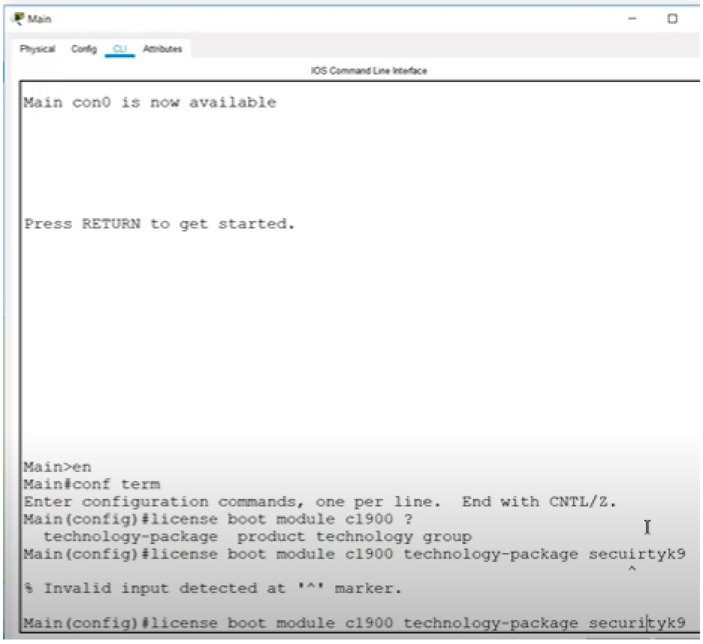
```
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
changed state to up

Branch(config-if)#int s0/0/0
Branch(config-if)#ip address 209.165.200.226 255.255.255.252
Branch(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
Branch(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed
state to up

Branch(config-if)#exi
Branch(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0
%Default route without gateway, if not a point-to-point interface, may
impact performance
Branch(config)#ip access-list standard ACL_NAT
Branch(config-std-nacl)#permit 192.168.1.0 0.0.0.255
Branch(config-std-nacl)#exit
Branch(config)#ip nat inside source list ACL_NAT interface s0/0/0
Branch(config)#int s0/0/0
Branch(config-if)#ip nat outside
Branch(config-if)#int g0/0
Branch(config-if)#ip nat inside
Branch(config-if)#
```

To make sure our NAT configuration works fine from PC-0 we pinged the branch and the main router:



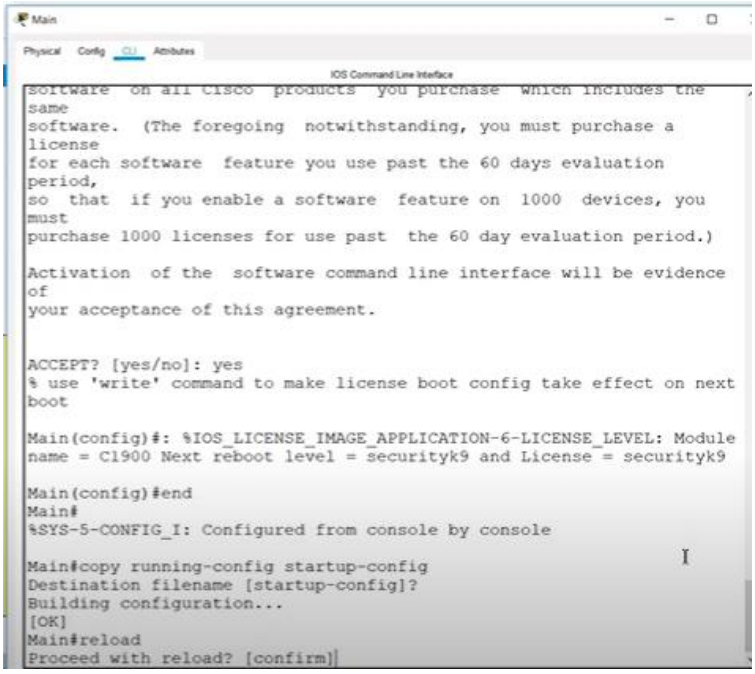
```
Ping statistics for 209.165.200.225:
    Packets: Sent = 4, Received = 4, Lost = 0 (0%
loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 3ms, Average = 1ms

C:\>ping 209.165.200.230

Pinging 209.165.200.230 with 32 bytes of data:

Reply from 209.165.200.230: bytes=32 time=2ms TTL=253
Reply from 209.165.200.230: bytes=32 time=17ms TTL=253
Reply from 209.165.200.230: bytes=32 time=3ms TTL=253
Reply from 209.165.200.230: bytes=32 time=2ms TTL=253

Ping statistics for 209.165.200.230:
    Packets: Sent = 4, Received = 4, Lost = 0 (0%
loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 17ms, Average = 6ms

C:\>
```

Creating the VPN on the Main router:



```
Main con0 is now available



Press RETURN to get started.









Main>en
Main#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
Main(config)#license boot module c1900 ?
  technology-package  product technology group
Main(config)#license boot module c1900 technology-package secuirtyk9
                                                                  ^
% Invalid input detected at '^' marker.

Main(config)#license boot module c1900 technology-package securityk9
```

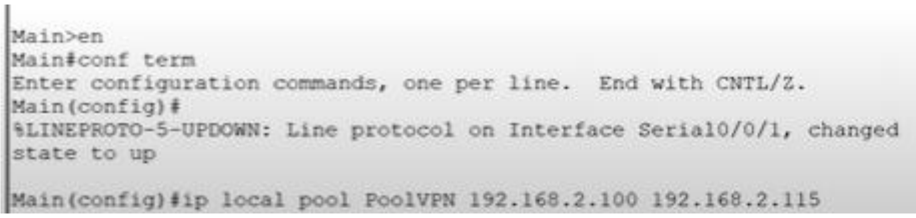
After adding the VPN on the router, we need to accept the agreement of the VPN, save the configuration to startup configuration then reload the router:



```
software  on all Cisco  products  you purchase  which includes the
same
software.  (The foregoing  notwithstanding, you must purchase a
license
for each software  feature you use past the 60 days evaluation
period,
so  that  if you enable a software  feature on  1000  devices, you
must
purchase 1000 licenses for use past  the 60 day evaluation period.)

Activation  of the  software command line interface will be evidence
of
your acceptance of this agreement.


ACCEPT? [yes/no]: yes
% use 'write' command to make license boot config take effect on next
boot

Main(config)#: %IOS_LICENSE_IMAGE_APPLICATION-6-LICENSE_LEVEL: Module
name = C1900 Next reboot level = securityk9 and License = securityk9

Main(config)#end
Main#
%SYS-5-CONFIG_I: Configured from console by console

Main#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Main#reload
Proceed with reload? [confirm]
```

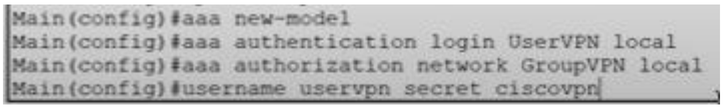
VPN configuration:

First, we added the ranges of IP addresses that connected to the VPN.



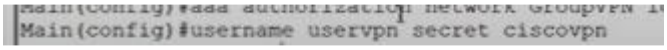
```
Main>en
Main#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
Main(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed
state to up

Main(config)#ip local pool PoolVPN 192.168.2.100 192.168.2.115
```

Second, we created a user authentication and authorization for the local database:



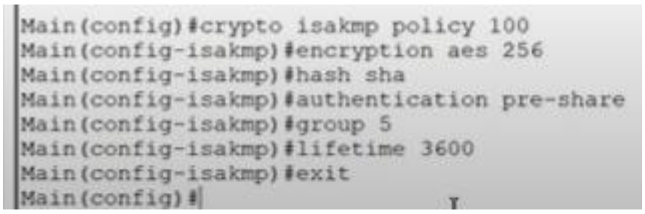
```
Main(config)#aaa new-model
Main(config)#aaa authentication login UserVPN local
Main(config)#aaa authorization network GroupVPN local
Main(config)#username uservpn secret ciscovpn
```

Third, we assigned the username as “uservpn” and the password as “ciscovpn” to be used later on in testing.



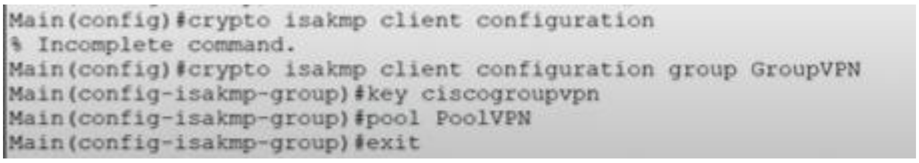
```
Main(config)#aaa authorization network GroupVPN lo
Main(config)#username uservpn secret ciscovpn
```

Fourth, we configured encryption on the VPN. We choose to use the AES encryption, SHA hash algorithm, and pre-shared key authentication.



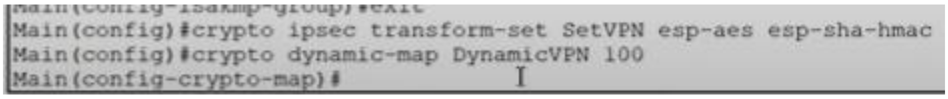
```
Main(config)#crypto isakmp policy 100
Main(config-isakmp)#encryption aes 256
Main(config-isakmp)#hash sha
Main(config-isakmp)#authentication pre-share
Main(config-isakmp)#group 5
Main(config-isakmp)#lifetime 3600
Main(config-isakmp)#exit
Main(config)#
```

Fifth, we created the client configuration using the isakmp. For the GroupVPN that was configured in the VPN in authentication.



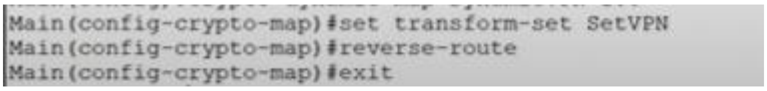
```
Main(config)#crypto isakmp client configuration
% Incomplete command.
Main(config)#crypto isakmp client configuration group GroupVPN
Main(config-isakmp-group)#key ciscogroupvpn
Main(config-isakmp-group)#pool PoolVPN
Main(config-isakmp-group)#exit
```

Sixth, we chose to make our VPN a Dynamic crypto map:



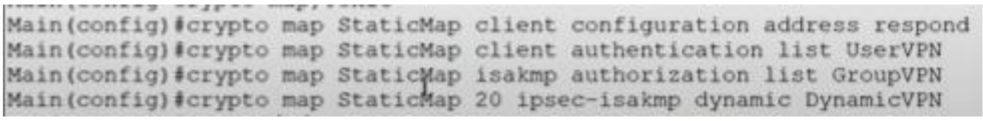
```
Main(config-isakmp-group)#exit
Main(config)#crypto ipsec transform-set SetVPN esp-aes esp-sha-hmac
Main(config)#crypto dynamic-map DynamicVPN 100
Main(config-crypto-map)#
```

Seventh, we applied the reverse route:



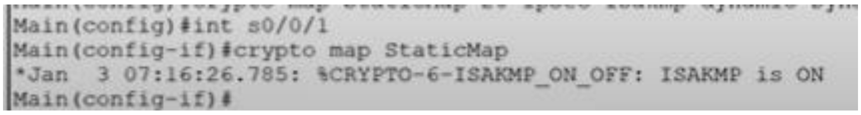
```
Main(config-crypto-map)#set transform-set SetVPN
Main(config-crypto-map)#reverse-route
Main(config-crypto-map)#exit
```

Eighth, we created a crypto static map. Then we added client authentication and authorization for the list “UserVPN” created above.



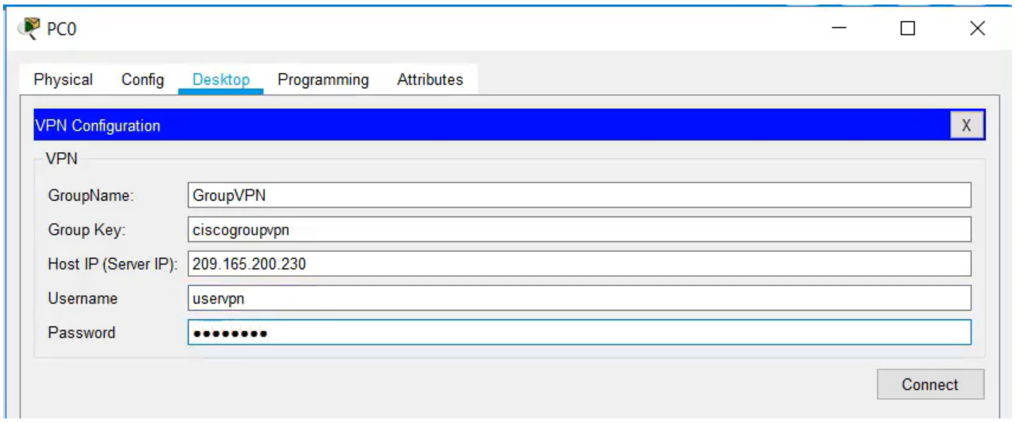
```
Main(config)#crypto map StaticMap client configuration address respond
Main(config)#crypto map StaticMap client authentication list UserVPN
Main(config)#crypto map StaticMap isakmp authorization list GroupVPN
Main(config)#crypto map StaticMap 20 ipsec-isakmp dynamic DynamicVPN
```

Ninth, we added the static map to the interface.



```
Main(config)#int s0/0/1
Main(config-if)#crypto map StaticMap
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Main(config-if)#
```

Connecting PC-0 to the VPN:



GroupName: GroupVPN

Group Key: ciscogroupvpn

Host IP (Server IP): 209.165.200.230

Username: uservpn

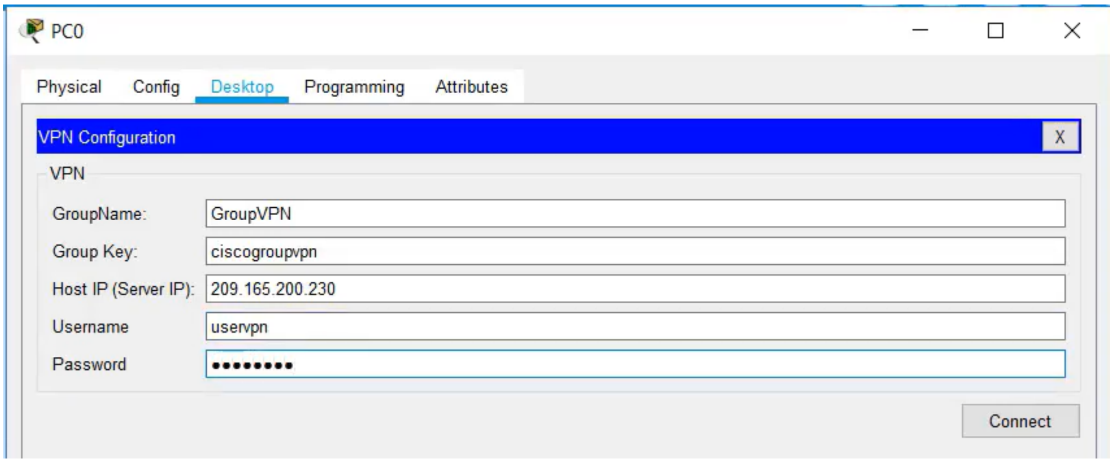
Password: ••••••••

All GroupName, Group Key, Host IP, Username, and Password were assigned in the main configuration in the VPN router above.

5. Testing:

We did the testing by verifying with the command ipconfig/ all on PC0 to get the IP address for the Ethernet interface and the tunnel interface. Then we pinged the PC0 with the PC1, which was its IP address, 192.168.2.10, and it was successful. After that, we pinged from PC0 to the server, and the IP address was 192.168.2.254, and it was successful. We also accessed the web browser using the server's IP address. Finally, we test with the tracert command and enter the IP address of PC1, which is

192.168.2.10, to see the hops. It displays two hops for us. The first hop was for the router, 209.165.200.254, and the second hop was for the destination, 192.168.2.10



GroupName: GroupVPN

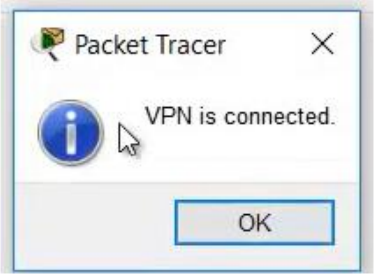
Group Key: ciscogroupvpn

Host IP (Server IP): 209.165.200.230

Username: uservpn

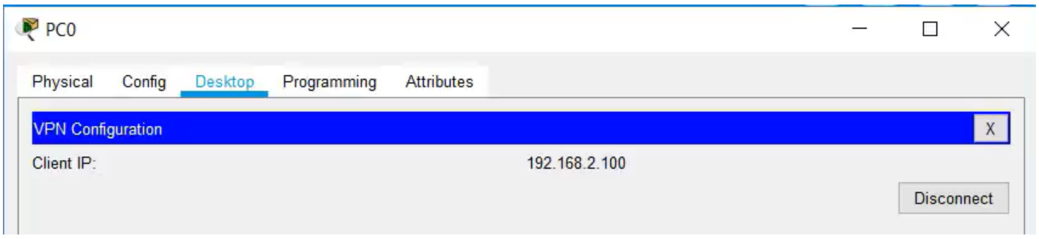
Password: ••••••••

Then click on connect to the VPN:

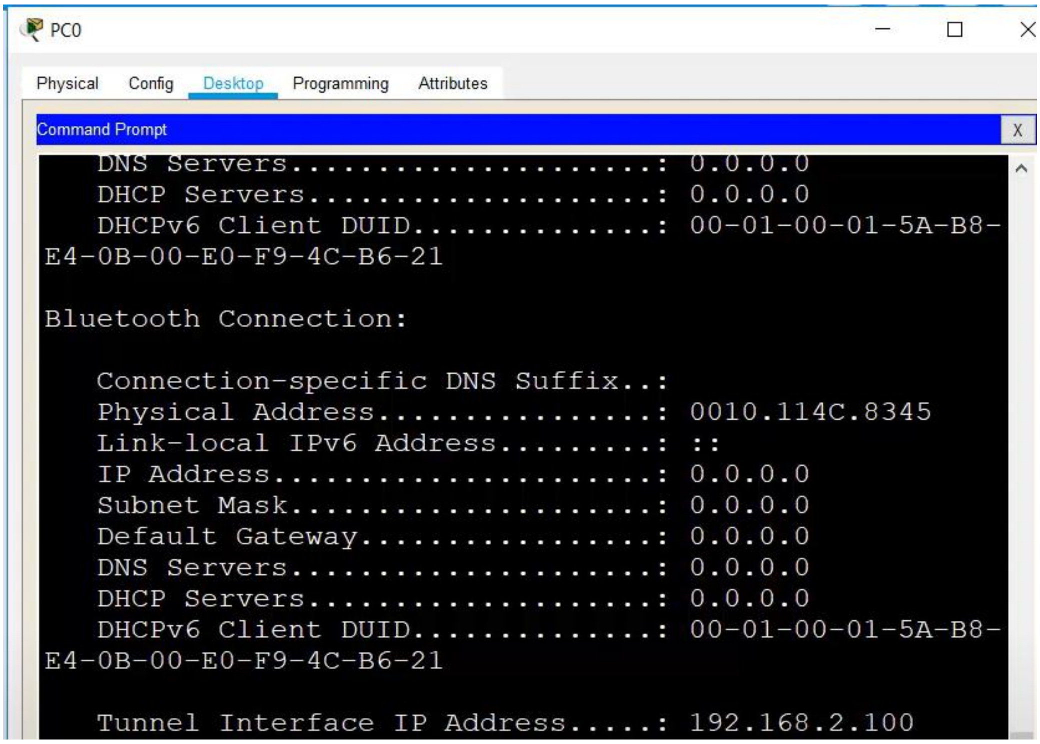


VPN is connected.

PC-0 connected to the VPN in the main router:

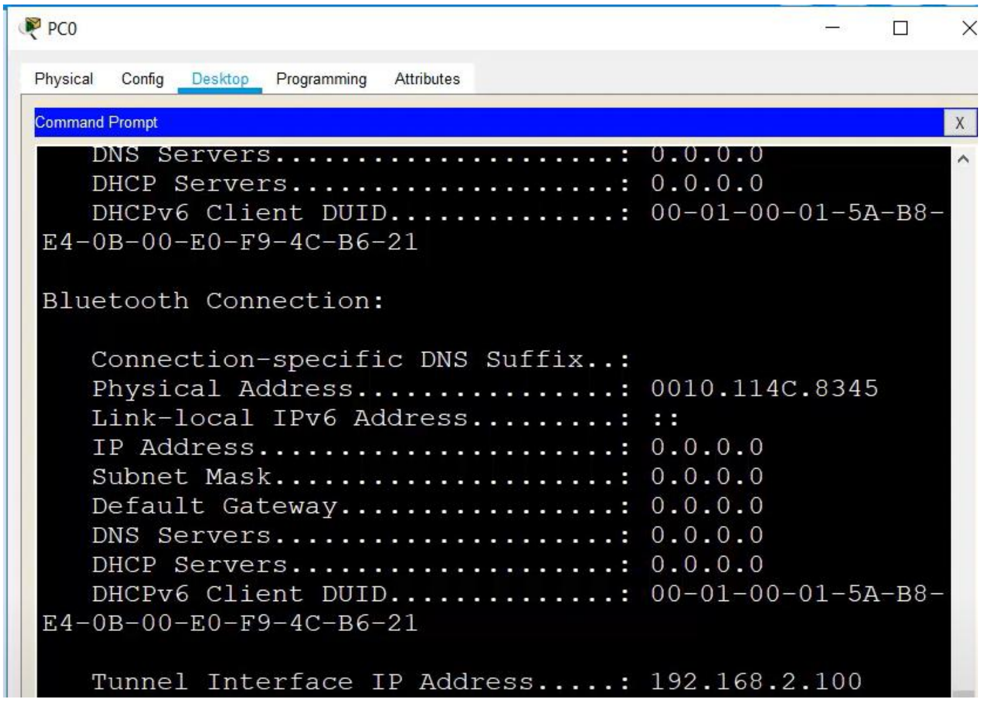


Client IP: 192.168.2.100



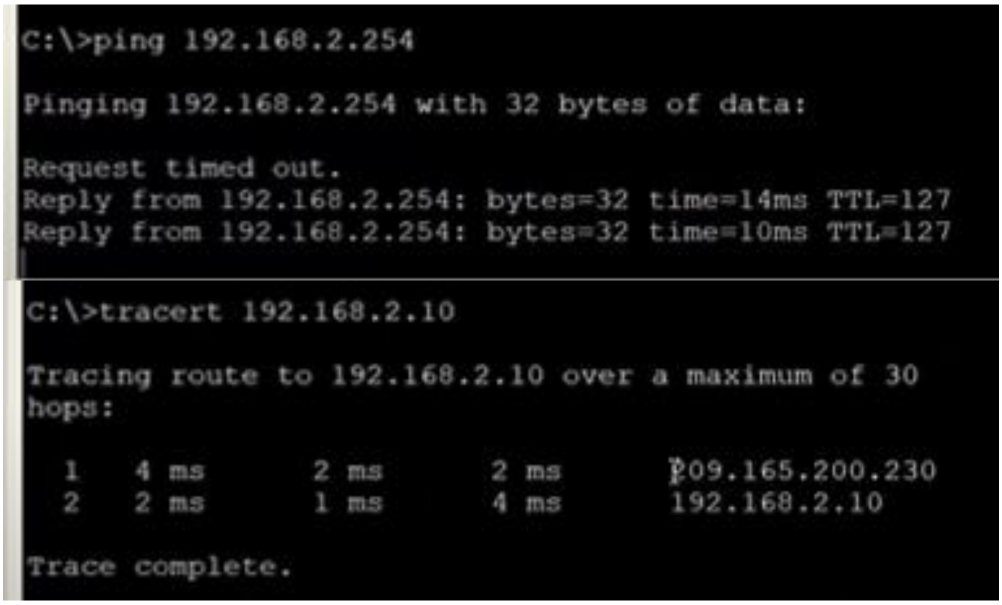
```
   DNS Servers.....................: 0.0.0.0
   DHCP Servers....................: 0.0.0.0
   DHCPv6 Client DUID..............: 00-01-00-01-5A-B8-
E4-0B-00-E0-F9-4C-B6-21

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Physical Address................: 0010.114C.8345
   Link-local IPv6 Address.........: ::
   IP Address......................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: 0.0.0.0
   DNS Servers.....................: 0.0.0.0
   DHCP Servers....................: 0.0.0.0
   DHCPv6 Client DUID..............: 00-01-00-01-5A-B8-
E4-0B-00-E0-F9-4C-B6-21

   Tunnel Interface IP Address.....: 192.168.2.100
```

To finally test the VPN connectivity to the Main router:



```
   DNS Servers.....................: 0.0.0.0
   DHCP Servers....................: 0.0.0.0
   DHCPv6 Client DUID..............: 00-01-00-01-5A-B8-
E4-0B-00-E0-F9-4C-B6-21

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Physical Address................: 0010.114C.8345
   Link-local IPv6 Address.........: ::
   IP Address......................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: 0.0.0.0
   DNS Servers.....................: 0.0.0.0
   DHCP Servers....................: 0.0.0.0
   DHCPv6 Client DUID..............: 00-01-00-01-5A-B8-
E4-0B-00-E0-F9-4C-B6-21

   Tunnel Interface IP Address.....: 192.168.2.100
```

Then we ping and tracert PC-0 to PC-1 and the pinging is successful:



```
C:\>ping 192.168.2.254

Pinging 192.168.2.254 with 32 bytes of data:

Request timed out.
Reply from 192.168.2.254: bytes=32 time=14ms TTL=127
Reply from 192.168.2.254: bytes=32 time=10ms TTL=127

C:\>tracert 192.168.2.10

Tracing route to 192.168.2.10 over a maximum of 30
hops:

  1   4 ms      2 ms      2 ms      209.165.200.230
  2   2 ms      1 ms      4 ms      192.168.2.10

Trace complete.
```

6. Challenges and Lessons Learned:

We haven't faced a lot of challenges in this project, we were only short on time since the basic configuration needed a lot of time to configure and we had to understand the commands entered. We have managed to VPN configuration only after searching and understanding the commands. The primary insight discovered while working on the remote management and VPN simulation project was the need of time management in distributed teams. Although there were no major technical difficulties during the project. Meetings, updates, and collaboration need careful preparation and adaptability To achieve productive collaboration in the face of schedule difficulties, it is crucial to schedule, and establish clear expectations regarding availability. Overall, this project demonstrated the importance of flexibility in remote work environments using security. We learned how to manage and configure a VPN for a network in the future and what our weaknesses are to improve in the future and to work on them.

7. Conclusions and Recommendations:

Taking into consideration actions to improve cybersecurity for remote access. Configuration of VPN and utilize Virtual Private Networks (VPNs) to secure remote connections and encrypt data. Authentication to improve user verification, implement strong authentication techniques like multi-factor authentication. Access Control Policies that strict access controls should be put in place within VPNs so that only authorized users with legitimate credentials can access internal resources. Tunnels using encryption which assures users connecting from a distance use private, encrypted tunnels to avoid data interception on public networks. Finally, Consistent Configuration Updates will keep security measures up to date and address potential vulnerabilities.

Companies with multiple branches can use this approach for remote management which will even help in case of a future natural disaster cases. From our perspective, remote access using VPN is a good approach that will increase the security and protection measures of companies helping them in reducing the risk in case of a cyber- threat or attack. For the sake of time, we implemented this project on a small main-branch network. However, this project can be implemented on multiple branches and bigger networks. This project is a small demonstration, and we can commercially use it for our senior project in case of any future collaboration with different companies.

To sum up, the recommended measures offer a thorough method to strengthen cybersecurity for remote access. Through the integration of technology solutions, and strict access restrictions, organizations can establish an efficient system that enables them to securely navigate the always-changing digital environment. In the area of remote operations, this proactive approach guarantees a strong defense against cyber-attacks along with regular updates and monitoring.

8. References

[1] Kaspersky, “What is a VPN and how does it work?,” *www.kaspersky.com*, Nov. 03, 2020. https://www.kaspersky.com/resource-center/definitions/what-is-a-vpn

[2] J. Murphy, “What is remote infrastructure management?,” *Networking*, Sep. 2023. https://www.techtarget.com/searchnetworking/definition/remote-infrastructure-management

[3] “What Is Remote Access? - IT Glossary | SolarWinds,” *www.solarwinds.com*. https://www.solarwinds.com/resources/it-glossary/remote-access

[4] “Telnet – the system-wide remote protocol,” *IONOS Digitalguide*. https://www.ionos.com/digitalguide/server/tools/telnet-the-system-wide-remote-protocol/

[5] M. U. of S. and Technology, “Secure Telnet Connection,” *Missouri S&T*. https://it.mst.edu/policies/secure-telnet/#:~:text=Telnet%20is%20inherently%20insecure.

[6] “Types of VPN protocols | NordLayer Learn,” *nordlayer.com*. https://nordlayer.com/learn/vpn/types-and-protocols/

[7] “What makes Telnet vulnerable,” *www.tutorialspoint.com*. https://www.tutorialspoint.com/what-makes-telnet-vulnerable#:~:text=Security%20Concerns%20with%20Telnet

[8] “Shibboleth Authentication Request,” login.zulib.idm.oclc.org. https://ieeexplore-ieee-org.zulib.idm.oclc.org/document/9151728

[9] C. Goyzueta, “Remote Access VPN - Packet Tracer,” *www.youtube.com*, Nov. 04, 2019. Available: https://youtu.be/8uWmFkrn6qE?si=B_vp5icM892bxwjn

[10] S. Tripathi, “Telnet on Router in Cisco Packet Tracer,” *YouTube*. Apr. 08, 2021. Available: https://www.youtube.com/watch?v=lpBblkiUUuU.