

CS2120 COMPUTER NETWORKS

Mini Project Report

Implementing WAN for Remote Branch Connectivity

Submitted

By

Parinitha RK (1RVU23CSE329)

Pavani R Sharma (1RVU23CSE332)

Shreyas Ghanathe (1RVU23CSE445)

Under the guidance of:

Dr./Prof. Jobin Thomas

School of Computer Science and Engineering

RV University, Bangalore



School of Computer Science and Engineering

CERTIFICATE

Certified that the CS2120 Computer Networks Mini Project work titled *Implementing WAN for Remote Branch Connectivity* is carried out by **Parinitha RK (IRVU23CSE329)**, **Pavani R Sharma (IRVU23CSE332)**, **Shreyas Ghanathe (IRVU23CSE445)** who are bonafide students of the School of Computer Science and Engineering, RV University, Bengaluru, during the year 2025–26. It is certified that all corrections/ suggestions from all the continuous internal evaluations have been incorporated into the project and in this report.

Dr./ Prof. Jobin Thomas

Faculty Guide

Dr. Sudhakar K. N

Program Director

INDEX

INDEX	3
1. Problem statement	4
2. Introduction	5
3. Network Diagram	7
4. Configuration setup	8
1. Remote Branch 1:	8
2. Remote Branch 2:	9
3. DC BRANCH(Data Centre Branch):	10
5. Results	11
6. Conclusion	15

1. Problem statement

This project serves to meet the task of configuring an effective Wide Area Network (WAN) for remote branch connectivity of organizations with the use of Cisco Packet Tracer. In real-world scenarios, environments require interruption-free communication amongst geographically distanced offices in order to help in facilitating data exchange, centralized services and conduct very important operations. The simulation entailed creating network architecture to integrate several branch offices to a centralized data center employing WAN technology. This project illustrates the implementation of WAN technology, static routing protocol and correct IP addressing to allow end to end connectivity. Such implementation solves challenges such as safe data transfer, fault tolerant routing and network uptime for remote branch integration.

2. Introduction

1. Implementation of Remote Branch Connectivity using WAN(wide area network)

This project aims to establish secure and efficient connectivity between the different remote branches to the main data center using WAN . The architecture follows a **hub and spoke model**, where the data center router acts as the core interconnecting the branch routers with the help of the WAN links. Each branch is equipped with switches,wireless access points for wireless connectivity and end devices such as laptops, PCs and tablets to ensure there is a seamless communication. Additionally, for the access points we have used WEP (wired equivalent privacy) for encryption (as a password) . When an end device tries to connect to the wireless network it should enter the same WEP key which was configured on the respective access point. Once it is authenticated,the device can access the network. Furthermore, a firewall is being implemented in front of the web server for protection.

2. Relevance of Remote Branch Connectivity using WAN(wide area network)

This network architecture is very important for business continuity,educational institutions and government organizations that require a centralized data center and remote access to resources. Employees or users from branch locations need secure access to the servers, databases and applications that are being hosted in the main data center. Wireless access points enable users to connect from different locations within the branch office. Proper configuration of WAN connectivity ensures seamless communication, remote collaboration, centralized data access and control and cost effective network management across different branches,

3. Technologies / Terminologies of Remote Branch Connectivity using WAN(wide area network)

This network architecture consists of various networking devices such as routers(ISR),switches (2960),wireless access points and firewalls to create a robust infrastructure. The routers handle the traffic between branches and the data center while the switches manage the internal branch connectivity. The access points help in wireless connection of the end devices ensuring that there is flexibility in data communication. The WAN technology is used for connecting remote sites.We have implemented a firewall for the web server to monitor or control which IP addresses can be allowed and which can be rejected.

Additionally, for the access points we have used WEP (wired equivalent privacy) for encryption (as a password) . When an end device tries to connect to the wireless network it should enter the same WEP key which was configured on the respective access point. Once it is authenticated,the device can access the network. This hub and spoke topology ensures that all branch communication flows through the DC router , providing centralized control and monitoring of the branches.

4. Protocols Used in Remote Branch Connectivity using WAN(wide area network)

In our network project we have used,

HTTP (Hypertext Transfer Protocol) for efficient data communication between the client and server, ensuring that there is a smooth data transmission over the web.

HTTPS (Hypertext Transfer Protocol Secure) in our project, which is the secure version of the HTTP, is used for encrypting the data using SSL/TLS, ensuring that there is secure communication between the client and server.

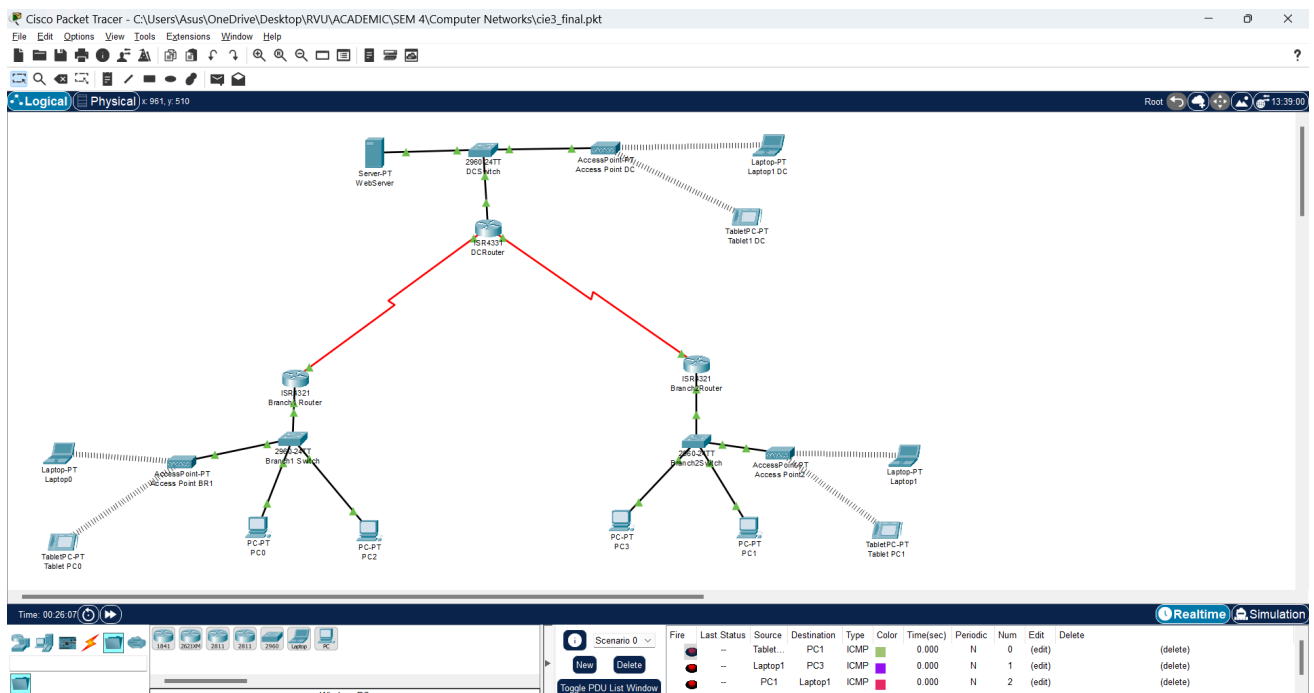
TCP/IP (Transmission control protocol and Internet protocol) handles reliable data transfer and routing of packets across the network to ensure the packets reach their destination in a correct order.

SRP (Static Routing Protocol) for configuration which assigns fixed IP addresses to the devices which ensures stable and predictable communication within the network.

WEP (Wired Equivalent Privacy) a wireless security protocol to provide data encryption and protect wireless communication. When an end device tries to connect to the wireless network it should enter the same WEP key which was configured on the respective access point. Once it is authenticated, the device can access the network.

ICMP(Internet Control Message Protocol) It is crucial in our network architecture as it is used for diagnosing and managing the network connectivity. It allows devices to send error messages and operation information such as when its destination is not reached or when the router is not accessible.

3. Network Diagram



4. Configuration setup

Three Branches present in the architecture:

1. Remote Branch 1:

- Branch 1 Router
 - IP Address: 192.168.1.1
 - Subnet Mask: 255.255.255.0
- PC0:
 - IP Address: 192.168.1.2
 - Subnet Mask: 255.255.255.0
 - Default Gateway: 192.168.1.1
- PC2:
 - IP Address: 192.168.1.3
 - Subnet Mask: 255.255.255.0
 - Default Gateway: 192.168.1.1
- Access Point:
 - SSID: BR2
 - WEP Key: 9876543210
- Laptop0:
 - IP Address: 192.168.1.10
 - Subnet Mask: 255.255.255.0
 - Default Gateway: 192.168.1.1
 - SSID: BR1
 - WEP Key: 0123456789
- Tablet PC-0:
 - IP Address: 192.168.1.11
 - Subnet Mask: 255.255.255.0
 - Default Gateway: 192.168.1.1
 - SSID: BR1
 - WEP Key: 0123456789

2. Remote Branch 2:

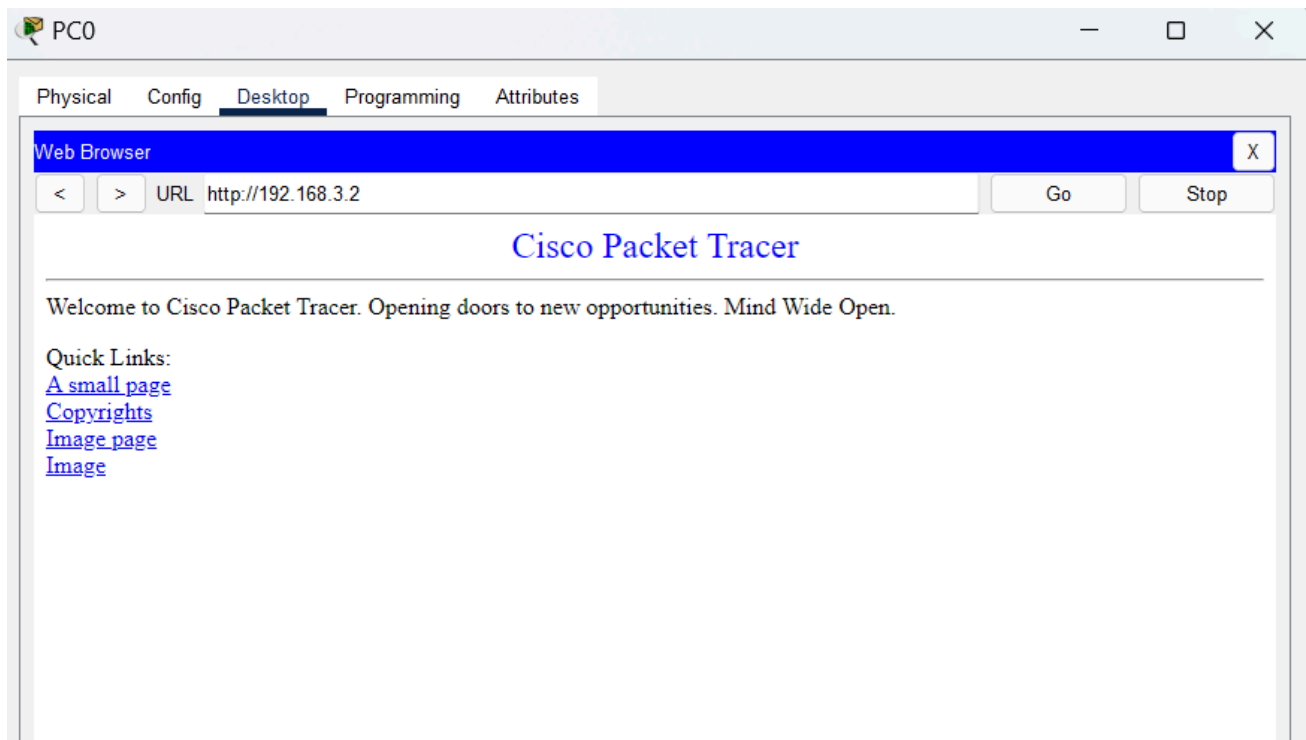
- Branch 2 Router:
IP Address: 192.168.2.1
Subnet Mask: 255.255.255.0
- PC3:
IP Address: 192.168.2.3
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.2.1
- PC1:
IP Address: 192.168.2.2
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.2.1
- Access Point:
SSID: BR2
WEP Key: 9876543210
- Laptop1:
IP Address: 192.168.2.10
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.2.1
SSID: BR1
WEP Key: 9876543210
- Tablet PC-1:
IP Address: 192.168.1.11
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.2.1
SSID: BR2
WEP Key: 9876543210

3. DC BRANCH(Data Centre Branch):

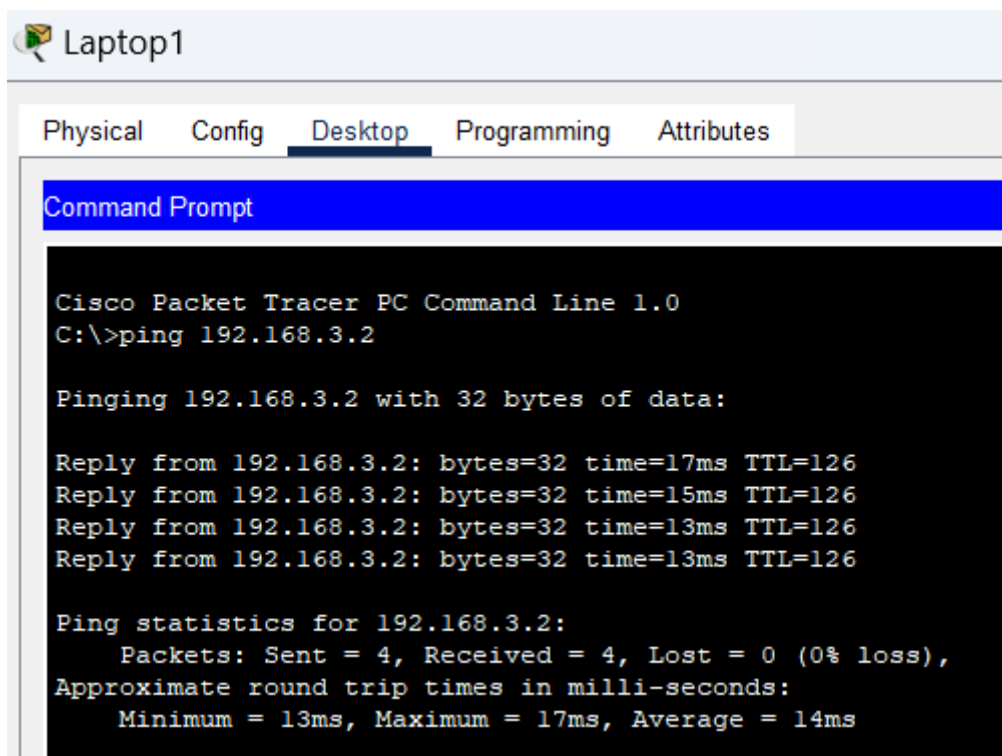
- DC Router(Serial 0/2/0):
IP Address: 192.168.4.1
Subnet Mask: 255.255.255.0
- DC Router(Serial 0/2/1):
IP Address: 192.168.5.1
Subnet Mask: 255.255.255.0
- DC Router(GigaBit Ethernet 0/0/0):
IP Address: 192.168.3.1
Subnet Mask: 255.255.255.0
- Web Server:
IP Address: 192.168.3.2
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.3.1
- Access Point DC:
SSID: DC
WEP Key: 1234567890
- Laptop1 DC:
IP Address: 192.168.3.10
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.3.1
SSID: DC
WEP KEY: 1234567890
- Tablet DC:
IP Address: 192.168.3.11
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.3.1
SSID: DC
WEP KEY: 1234567890

5. Results

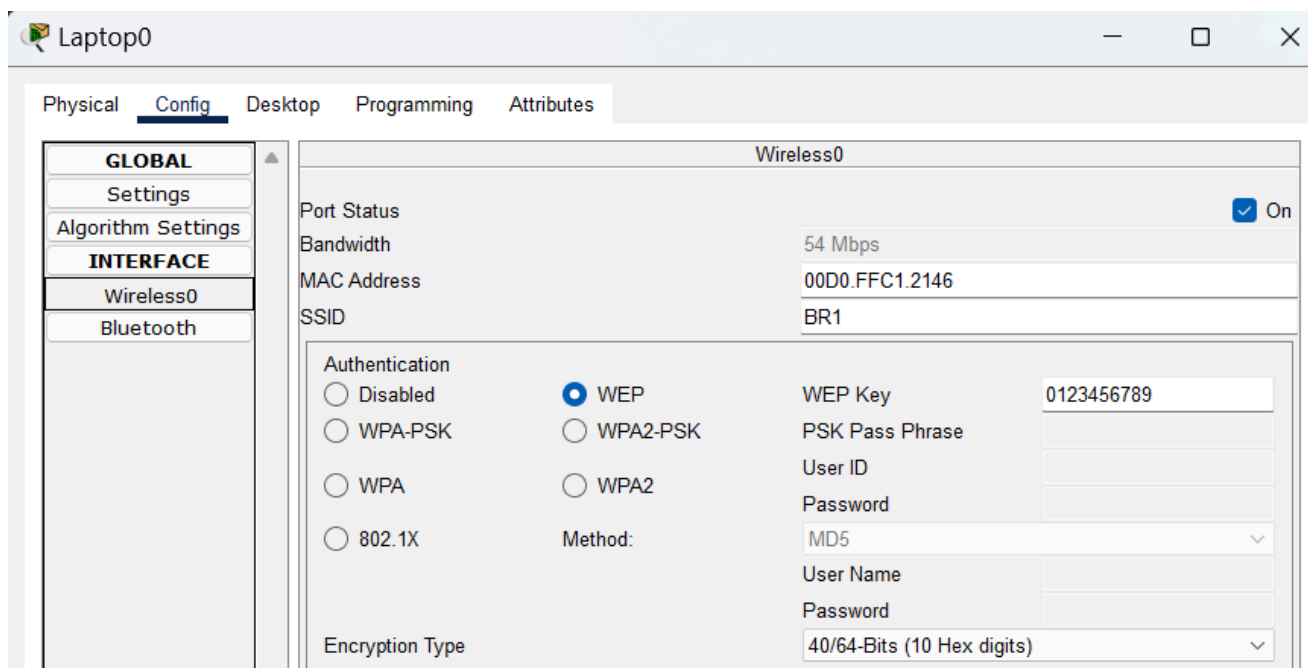
→ Accessing Web Server from Remote Branch1 PC0:











→ Pinging Web Server via Wireless Connection in Laptop1 from Branch 2:



→ Successful connection between end device and access point using WEP(Wired Equivalent Privacy):



→ Successful Packet travel from source to destination:

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	Tablet PC1	PC1	ICMP		0.000	N	0	(edit)	(delete)
	Successful	Laptop1	PC3	ICMP		0.000	N	1	(edit)	(delete)
	Successful	PC1	Laptop1	ICMP		0.000	N	2	(edit)	(delete)
	Successful	PC3	Tablet PC1	ICMP		0.000	N	3	(edit)	(delete)

→ Configured firewall into web server to add security

WebServer

Physical
Config
Services
Desktop
Programming
Attributes

Firewall

Service

☒ On
☐ Off

Interface

FastEthernet0

Inbound Rules

Action

Deny

Protocol

ICMP

Remote IP

192.168.2.0

Remote Wildcard Mask

0.0.0.255

Remote Port

Local Port

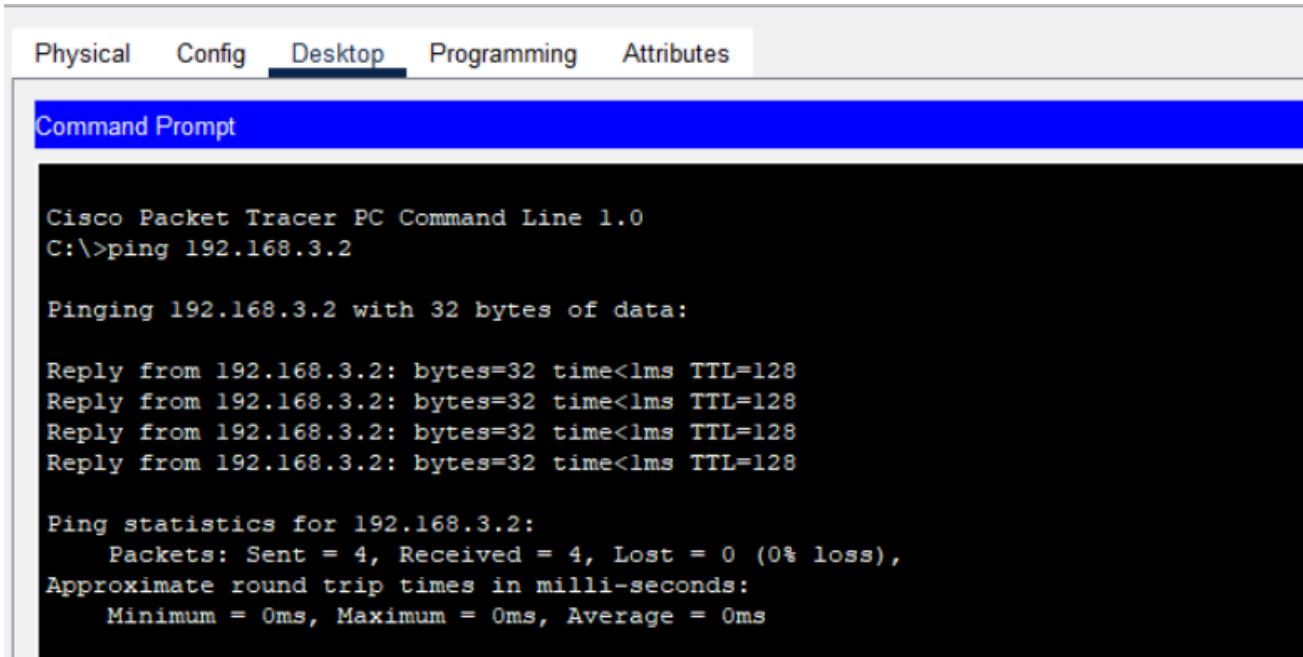
Save

Remove

Add

	Action	Protocol	Remote IP	Remote Wild Card	Remote Port	Local Port
1	Allow	ICMP	192.168.1.0	0.0.0.255	-	-
2	Deny	ICMP	192.168.2.0	0.0.0.255	-	-
3	Allow	ICMP	192.168.3.0	0.0.0.255	-	-
4	Allow	TCP	192.168.1.0	0.0.0.255	any	80
5	Deny	TCP	192.168.2.0	0.0.0.255	any	80
6	Allow	TCP	192.168.3.0	0.0.0.255	any	80

→ Before adding firewall:



The screenshot shows the Cisco Packet Tracer interface with the 'Desktop' tab selected. A 'Command Prompt' window is open, displaying the output of a ping command. The text in the Command Prompt is as follows:

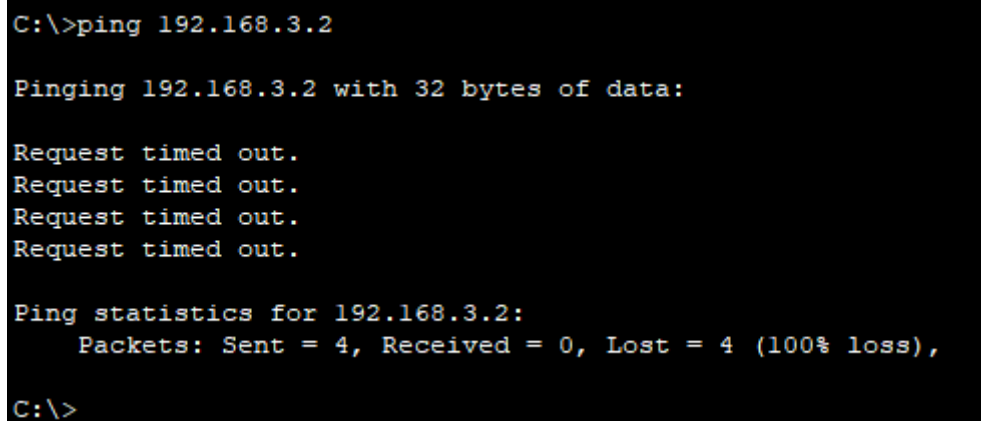
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data:

Reply from 192.168.3.2: bytes=32 time<1ms TTL=128
Reply from 192.168.3.2: bytes=32 time<1ms TTL=128
Reply from 192.168.3.2: bytes=32 time<1ms TTL=128
Reply from 192.168.3.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

→ After adding firewall:



The screenshot shows a Command Prompt window with the output of a ping command. The text in the Command Prompt is as follows:

```
C:\>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.3.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
```

6. Conclusion

This project's goal was to design and implement a Wide Area Network (WAN) using Cisco Packet Tracer for establishing secure and reliable remote branch office connectivity with a central data center. Routers, switches, firewalls, wireless access points, and end-user devices were configured in a manner that resembled a real-world network environment with static routing protocols. This configuration established communication throughout all branches, thus allowing efficient data transfer and access to centralized services. The project demonstrates the need for WAN technology for business operations, remote collaboration, and central management. In the future, this network can be expanded with advanced security protocols, real-time monitoring tools, and cloud integration to enhance performance, scalability, and resilience.