Ecole D'ingénieurs Sup Galilée
Télécommunications et Réseaux

Implementation of BGP Protocol in a WAN Network

Option : Networking and Telecommunications

Directed by ;
Pr. Nguyen Thi-Mai-Trang

Presented by:
HANOU Rimy
BELKHODJA Ibrahim

JUIN 2024

Contents

1 Objective

2 BGP and OSPF Introduction

3 Topology and Scenarios

4 Results

5 Conclusion

Objective

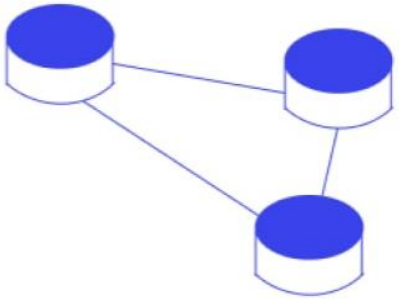
Our main objective was to establish seamless communication between a department in Company A and a department in Company B by using BGP routing protocol to manage the communication between different Autonomous Systems, or AS and OSPF to manage the communication within AS.

01

BGP and OSPF Introduction

BGP Protocol

What is BGP?



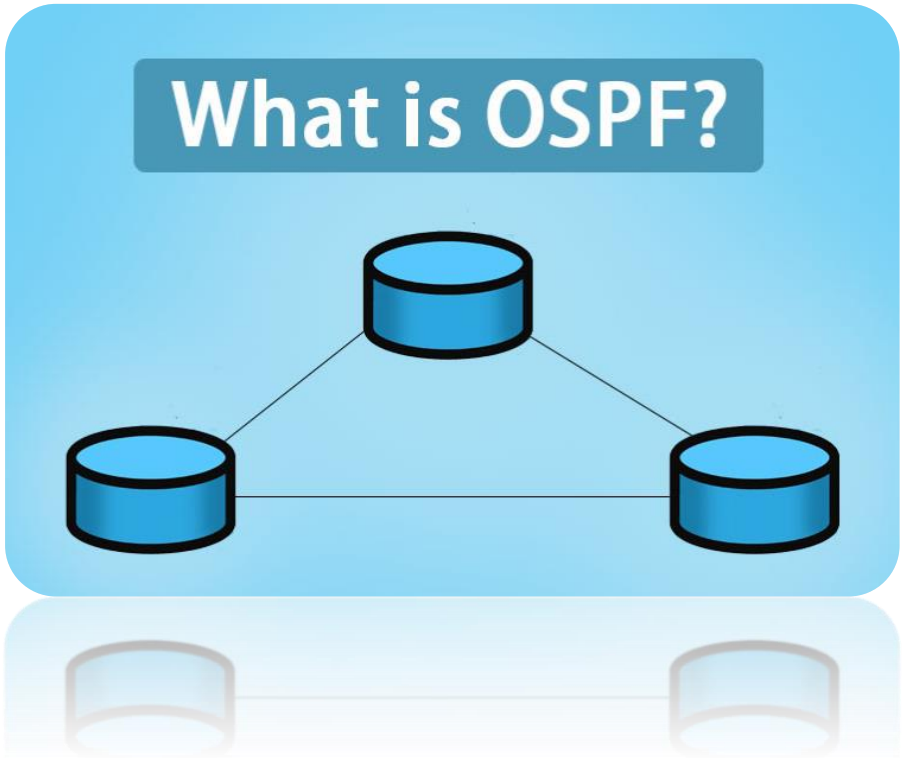
1. BGP (Border Gateway Protocol) is the primary protocol used to route traffic across the internet.

2. Manages how packets are routed between autonomous systems (AS), which are large networks under a common administration.

3. eBGP (externe BGP) is used for communication between different autonomous systems.

4. Path vector mechanism, policy-based routing, and scalability to support the global internet.

OSPF Protocol



1. OSPF (Open Shortest Path First) is a link-state routing protocol used within an autonomous system (AS).
2. Designed for efficient and rapid convergence, ensuring reliable and dynamic routing.
3. Supports multi-area configurations to optimize traffic and reduce routing table size.
4. Suitable for large and complex networks due to its efficient use of resources and hierarchical structure.

02

Topology and Scenarios

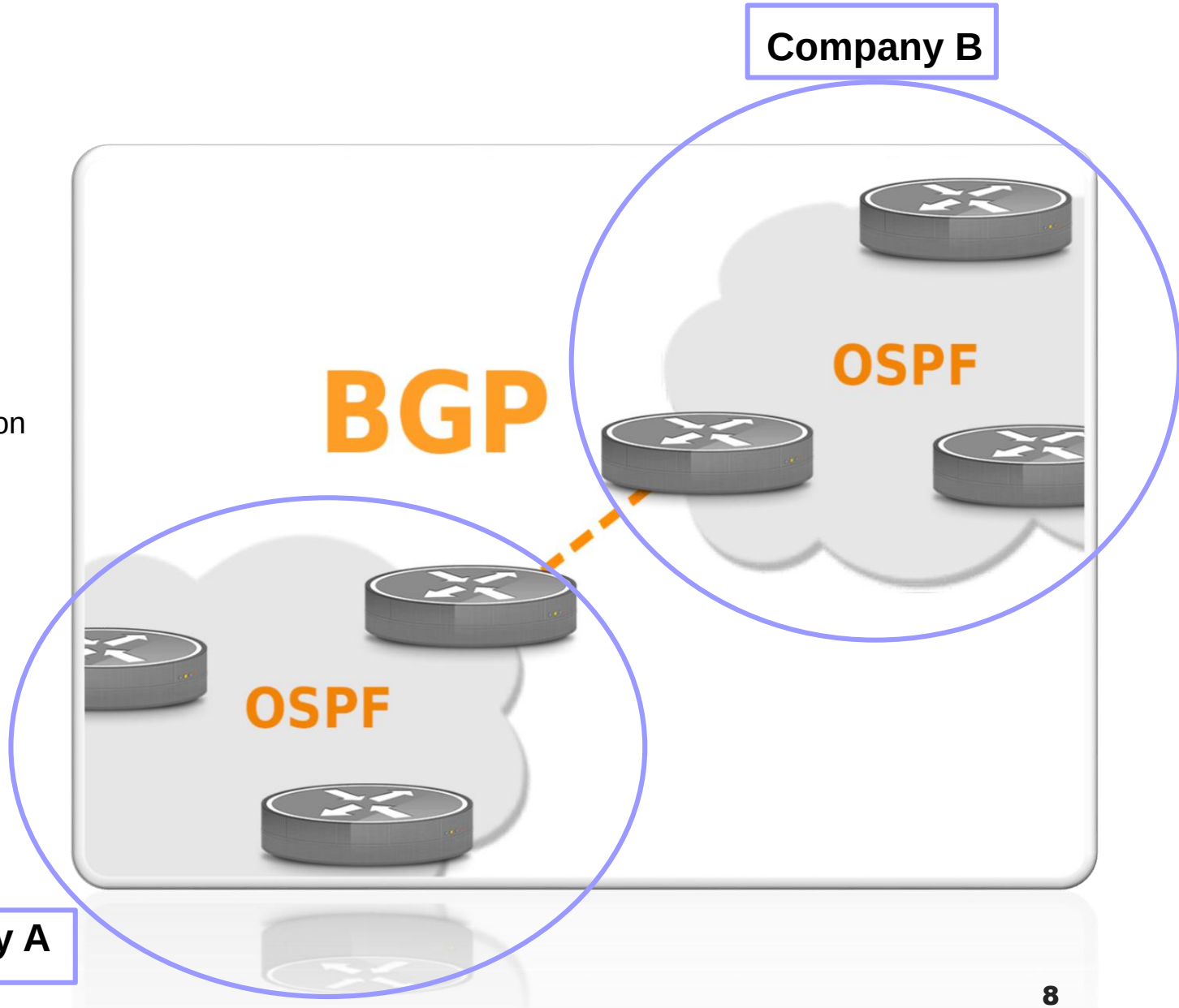
Topology

Company A and Company B:

- Two main entities in the network.
- Interconnected via BGP to enable communication between them.

Internal Structure:

- Each Company connected via OSPF.



Topology

Company A and Company B:

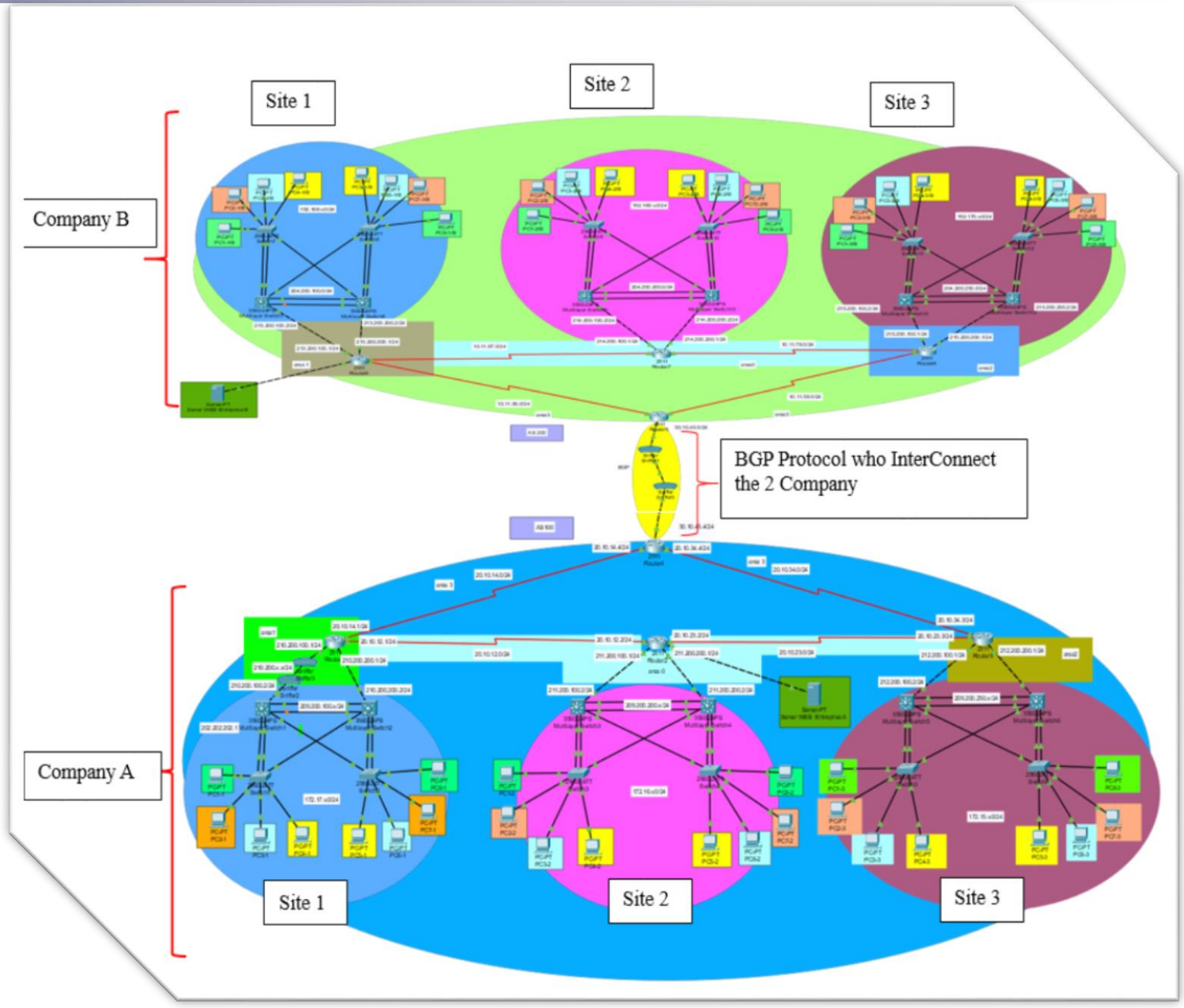
- ❑ Two main entities in the network.
- ❑ Interconnected via BGP to enable communication between them.

Internal Structure:

- ❑ Each Company consists of three sites, connected via OSPF, and includes a web server.
- ❑ Each site contains four departments represented by four different VLANs.

Objective:

- ❑ Create a robust, secure, and optimized network topology with adequate redundancy.



Used Protocols

	HSRP (Hot Standby Router Protocol)	STP (Spanning Tree Protocol)	EtherChannel	PortFast	SSH (Secure Shell)	VPN (Virtual Private Network)
Function	Ensure redundancy of default gateways.	Prevent switching loops	Aggregate multiple physical links into a single logical link.	Accelerate port convergence	Secure remote access to network devices.	Secure communications over public networks
Usage	Configures multiple routers as backup gateways to ensure network connection continuity.	Creates a loop-free topology by disabling redundant paths while ensuring redundancy.	Increases bandwidth and ensures link redundancy between switches.	Used on ports connected to end devices to speed up connection establishment.	Encrypts remote command sessions to protect sensitive information.	Allows secure connections between different company sites over the Internet.

Scenarios

Scenario 1: Intra-Company Communication	Scenario 2: Inter-Company Communication
Objective: Establish communication between different sites within Company A.	**Objective:** Establish communication between departments of Company A and Company B.
Focus: Analyze how packets traverse the private network to reach other sites.	**Focus:** Analyze packet traversal using BGP between AS.
Key Protocols and Features: HSRP, STP, EtherChannel, Portfast, SSH, VPN, OSPF.	**Key Protocol:** BGP
Outcome: Evaluate network performance and resilience.	**Outcome:** Assess BGP effectiveness for inter-enterprise communication.

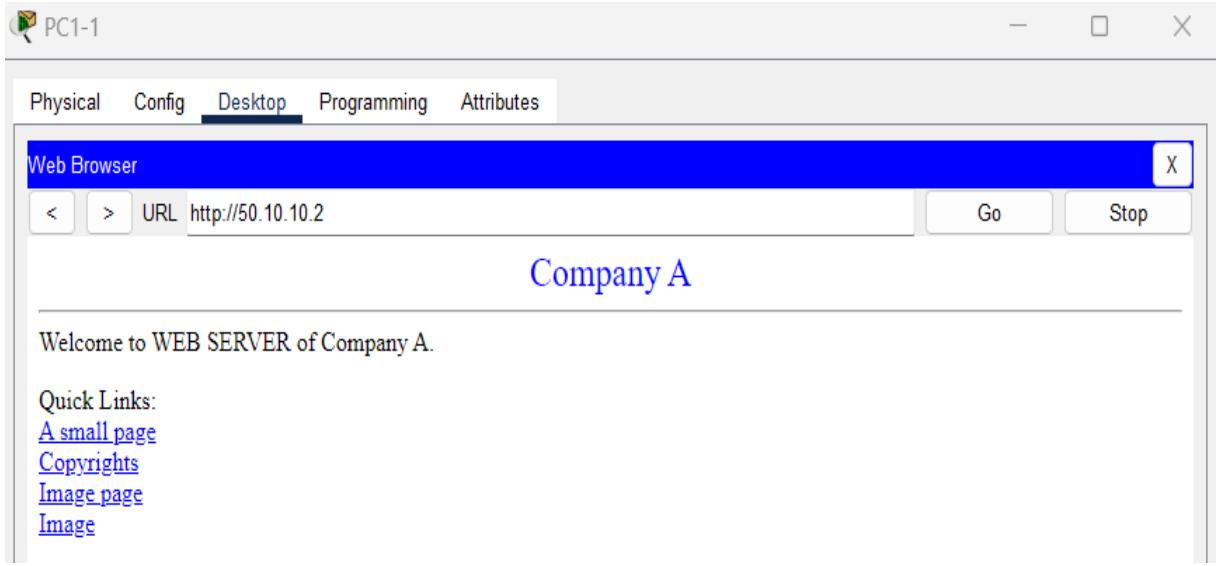
03

Results

Scenario 1

Network Performance: Achieved efficient and reliable communication within Company A.

Resilience: Redundancy mechanisms ensured high availability and quick recovery from failures.



Ping PC 1-Site1 To PC 2- Site 2 in Company A

```
C:\>ping 172.16.30.3

Pinging 172.16.30.3 with 32 bytes of data:

Reply from 172.16.30.3: bytes=32 time=2ms TTL=124
Reply from 172.16.30.3: bytes=32 time=3ms TTL=124
Reply from 172.16.30.3: bytes=32 time=1ms TTL=124
Reply from 172.16.30.3: bytes=32 time=2ms TTL=124

Ping statistics for 172.16.30.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 3ms, Average = 2ms
```

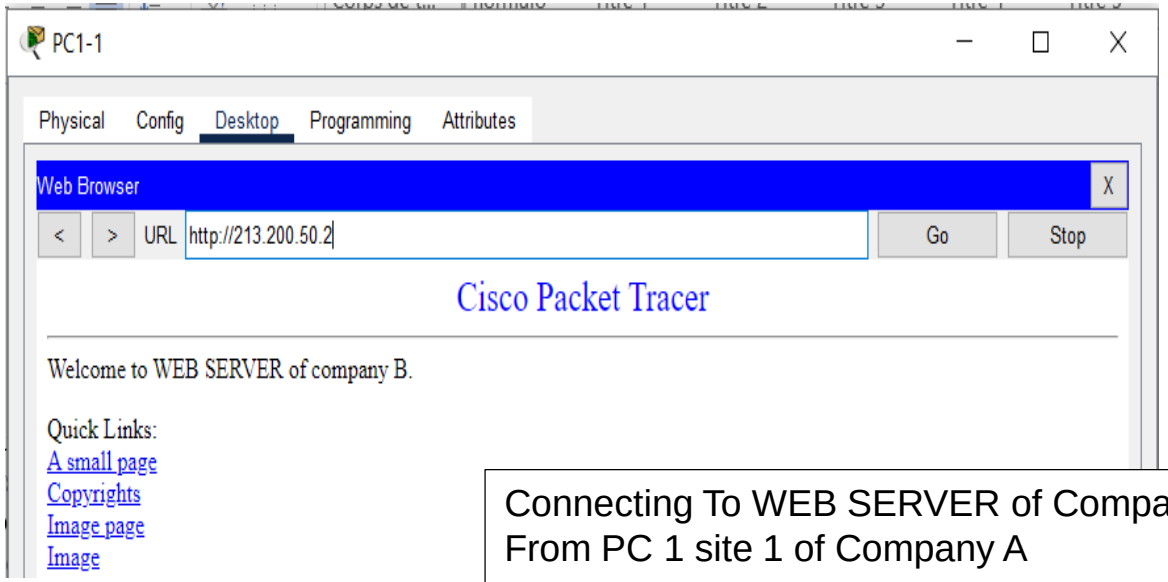
```
C:\>ping 172.15.20.3

Pinging 172.15.20.3 with 32 bytes of data:

Reply from 172.15.20.3: bytes=32 time=3ms TTL=123
Reply from 172.15.20.3: bytes=32 time=3ms TTL=123
Reply from 172.15.20.3: bytes=32 time=24ms TTL=123
Reply from 172.15.20.3: bytes=32 time=10ms TTL=123

Ping statistics for 172.15.20.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 24ms, Average = 10ms
```

Ping PC 1-Site1 To PC 3- Site 3 in Company A

Scenario 2

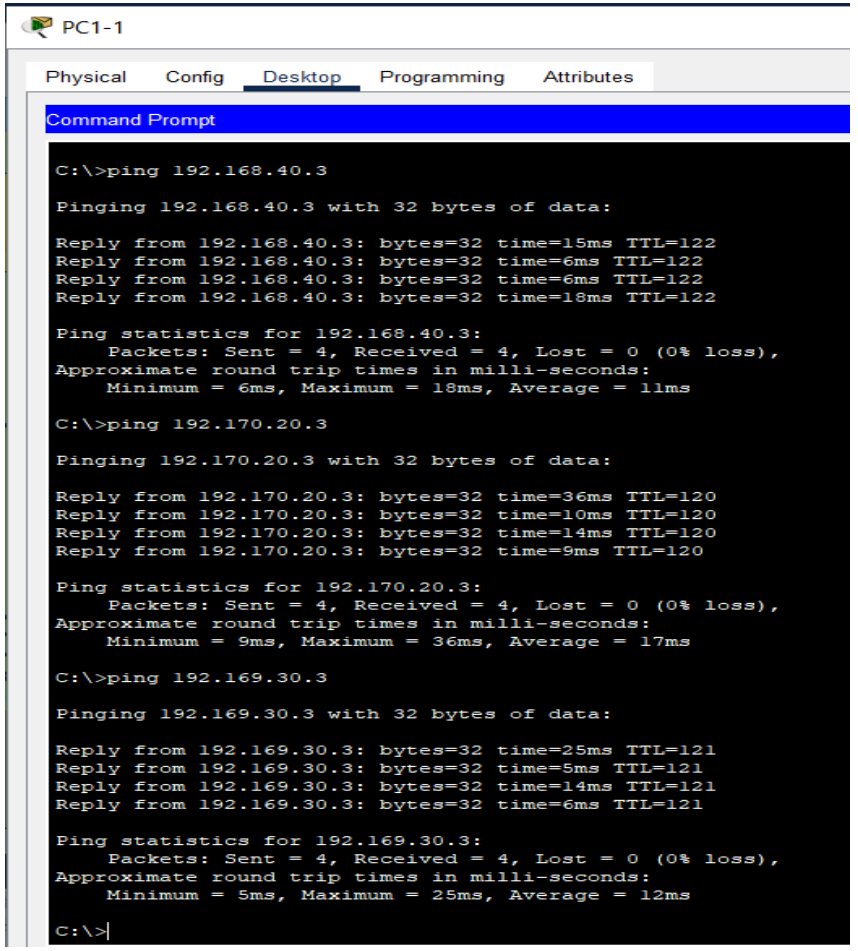
Effectiveness of BGP: Successfully demonstrated BGP's ability to handle inter-Company communication, ensuring robust and secure connectivity.

Performance: Evaluated BGP's role in maintaining stable connections and optimizing routing between Companies.



Connecting To WEB SERVER of Company B From PC 1 site 1 of Company A

Ping From PC 1 site 1 of Company A to PCs of Company B



04

Conclusion

Conclusion

- This project enabled us to apply our networking knowledge in designing, configuring, and managing a complex network using BGP and OSPF protocols..
- Network topology integrating two companies in different countries, connected via a WAN.
- Robust and secure connectivity was achieved using BGP for external connectivity and OSPF for internal routing..
- Redundancy mechanisms like HSRP, STP, EtherChannel, and PortFast ensured network availability and performance optimization.

THANKS FOR WATCHING