ACKNOWLEDGEMENT

In the name of ALLAH, the Most Gracious and Most Merciful, all praises to ALLAH for the strength and his blessing to me for the completion of the project. I am profoundly grateful to almighty Allah, whose unwavering guidance and blessing have illuminated my path. I extend my heartfelt gratitude to my supervisor, Mr. Ahmaduallah Sir His unyielding support, invaluable guidance and unwavering encouragement have been instrumental in the successful realization of this project. Without his mentorship and expertise, this accomplishment would not have been possible. Mr. Ahmad ullah sir has been a wellspring of motivation and wisdom throughout this journey. I wish to express my profound appreciation for his continuous cooperation and steadfast support, which extend form the project inception to its successful completion. His insight feedback provided the cornerstone upon which we achieved our project objectives. I would like to extend my gratitude. With deep appreciation and humility, I offer my thanks to ALLAH and my supervisor who have contribute to the realization of this project.

ABSTRACT

An enterprise network is a computer network that is used by a business or organization to connect its offices, employees, and resources. The Enterprise network facilitates files and resources sharing between different departments and teams in an organization to the internet. An enterprise network typically includes a wide area network (WAN) to connect the different offices, a local area network (LAN) to connect the devices within each office, and a wireless network for mobile devices. The network may also include other technologies like virtual private networks (VPNs), firewalls, and intrusion detection systems (IDS) to improve security and performance. Other researchers worked on Traditional enterprise network can have Limitations of congestion, slowdown, Security and Management of network. In this work using OSPF over traditional enterprise network include improved scalability, Flexibility, Efficient Routing, Support of Large networks, Optimize Traffic Flow, performance and security. It is more efficient and easier to manage then traditional networks also using OSPF is more cost effective solution for enterprise networks. Throughout OSPF can help to overcome these challenges and provide improved performance and efficiency as well as security.

CHAPTER-I

INTRODUCTION

1.1 Project Background Introduction

In enterprise network OSPF (Open Shortest Path First) is widely utilized for its ability to support large and big networks, provide flexibility, scalability and efficient routing. Large enterprise networks tend to use OSPF internally for its capability to facilitate the exchange of routing information between routers, enabling the identification of most efficient path for data transmission within the network. The role of OSPF in enterprise network extends to support the redundancy and resilience by creation of multiple areas within the network.

This is crucial for ensuring continuous operations in the event of failure or network changes. It allow redistribution of routes form other AS (Autonomous System) into its own facilitating interoperability between different part of the network. Furthermore enterprise networks encompass a wide range of elements form historic roots of major companies to the modern technologies and services that underpin their operations. Enterprise networks have evolved to become expensive that support the communication and data needs of large organizations. Enterprise network encompass a broad spectrum of technologies and services including network infrastructure such as routers, switches, wireless system and many other things. This networks are designed to support the complex need of modern business, enabling seamless communication, data transfer between multiple branches, and also collaborate across various location of departments.

1.2 Background of the Problem

The enterprise networks encompass a range of issues and problems that can impact the performance, security, and functionality of business networks. These issues can include the security vulnerabilities, performance and configuration errors. Understanding and addressing these issues and challenges is crucial for maintaining the reliability and efficiency of enterprise networks.

1. **Connectivity Problem:** enterprise network often face connectivity issues that can disrupt operations and hinder productivity. These problems may arise form misconfigurations, hardware failures, or environmental factors, leading to intermittent or complete loss of the network connectivity.
2. **Security vulnerabilities:** The security of enterprise network is a paramount concern, and emergence of new threats and vulnerabilities poses significant challenges. From

SSL certificate problem to permission denied error in secure shell connectivity, security issues can compromise the integrity and confidentiality of network communication.

3. **Configuration Errors:** Misconfigurations in network devices such as routers, switches, firewalls can lead the security problems and risks. Troubleshooting and resolving these configuration errors are essential for maintaining the stability and security of network.
4. **Performance Bottlenecks:** Business networks are complex, and performance bottleneck can significantly impact user experience and productivity. Identifying and addressing these bottlenecks whether related to network infrastructure or application performance is crucial for ensuring optimal network performance.

5. **Troubleshooting and Resolution:** Troubleshooting which involve network monitoring, diagnostic tools and collaborate with network administrators and support team. Effective troubleshooting is essential for identifying root cause of problem and implementing appropriate solutions.

1.3 Objective of study: The objective for the study in enterprise network may encompass a range of goals aimed at improving network performance, security and operational efficiency. Based on the Research the objective could include:

1.3.1. Provision of legal and Financial Services: Enhancing the network to support provision of legal and financial services, which may involve ensuring secure and reliable data transmission for sensitive information.

1.3.2. Diagnosing and fixing network Problems: Developing the capability to diagnose and resolve network issues effectively, ensuring optimal network performance and reliability.

1.3.3. Improving Collaboration in Regional, National and International Projects: Enhancing network capabilities to facilitate seamless collaboration in regional, national and international projects, emphasizing efficient communication and data sharing.

1.3.4. Enhancing Network Security: Implementing measures to strengthen network security, safeguarding against unauthorized access, data breaches, and other security threats.

1.3.5. Improving infrastructure and Network Assurance: Focusing on enhancing network infrastructure and ensuring network assurance to maintain operational reliability and performance.

1.3.6 **Facilitating Enterprise and Supply Chain Management Performance:** Aiming to improve enterprise and supply chain management performance through the effective use of networking technologies.

1.4 Scope of the Study:

The scope of the study encompass various aspect as evidence by the following sources.

The **CCNP enterprise certifications** involves the ability to diagnose and resolve network issues, as well as configure and verify different networking features for optimal performance.

The **Enterprise network security Market** involves the adoption of emerging technologies and highlights the importance of security within enterprise network.

Invision Automated infrastructure Management focuses on structured cabling and automated infrastructure management for enterprise networks.

Additionally the scope of the study in enterprise network extend to the use of enterprise social networks for learning beyond the classroom as well as their relation to web 2.0 tools.

1.5 Gantt Chart:

Task	Jan	Feb	Mar	Apr	May	June	Jul
Overview	■						
Gathering Project Content	■						
Designing Networking		■					
Routing & Switching		■					
Designing Wireless Network			■				
Data Center Design				■			
Testing and Troubleshooting					■		
Writing Thesis					■	■	
Preparation for Final Presentation							■

CHAPTER II

Literature Review

2.1 INTRODUCTION: Routing protocols are essential components of modern computer networks, enabling devices like routers and switches to determine the most efficient path for sending data across a network. Over the years, several routing protocols have been developed, each with its unique characteristics and suitable use cases. Open Shortest Path First (OSPF), a link-state routing protocol, emerged in the late 1980s as a more scalable, flexible, and efficient alternative to older protocols, such as Routing Information Protocol (RIP). The evolution from these earlier protocols to OSPF highlights the limitations they faced and the challenges OSPF was designed to address. The importance of OSPF can be traced back to the inherent limitations of its predecessors, such as RIP, and the growing demands of large-scale, complex networks. As enterprises expanded and the internet grew, the need for more efficient, scalable, and reliable routing protocols became critical. This section will delve into the historical context that led to the introduction of OSPF, discuss the limitations of older protocols, and explain why OSPF came into the picture.

2.2 The Evolution of Routing Protocols

1. Early Routing Protocols: RIP and Its Limitations

The **Routing Information Protocol (RIP)**, first introduced in the 1980s, was one of the earliest interior gateway protocols (IGPs) used for determining routes within a local or regional network. RIP's primary function is to exchange routing tables between routers to find the shortest path to a destination based on hop count. While RIP served its purpose during its early adoption, it quickly became apparent that it had significant limitations, especially as networks began to grow in size and complexity.

Some key limitations of RIP include:

- **Limited Scalability**: RIP uses a hop count as the metric for determining the shortest path, which limits its scalability. A maximum of 15 hops is supported, meaning networks larger than this would become unreachable. This limitation severely restricted RIP's use in large-scale networks.

- **Slow Convergence**: RIP is known for its slow convergence times, meaning it takes a long time for the network to react to changes, such as the failure of a link or router. This can lead to routing loops or packets being sent along outdated routes during the convergence process.
- **High Bandwidth Consumption**: In RIP, routers exchange full routing tables periodically, regardless of whether the topology has changed. This periodic exchange, coupled with the need to recalculate routes, can lead to high bandwidth consumption, especially in large networks.
- **Lack of Hierarchical Design**: RIP does not support hierarchical network designs. In large enterprise networks, the lack of a way to segment the network into different areas or regions leads to inefficient routing and an increase in the size of routing tables.

2.3 The Birth of OSPF

As networks became larger and more complex, the limitations of RIP became increasingly apparent. The Internet Engineering Task Force (IETF) recognized the need for a new, more scalable, and efficient protocol, and this led to the development of **Open Shortest Path First (OSPF)** in 1989. OSPF was designed to address the limitations of RIP and provide a robust solution for the growing demands of modern networks.

OSPF is a link-state routing protocol, meaning it operates differently than distance-vector protocols like RIP. Instead of sending full routing tables, OSPF routers exchange information about the state of their links with their neighbors. This allows each router to build a complete topology of the network, making the routing process more efficient and reliable.

2.4 Why OSPF Came into the Picture

1. Addressing Scalability

One of the primary reasons OSPF was developed was to address the **scalability** limitations of RIP. With the explosive growth of the internet and corporate networks in the 1990s, the need for a routing protocol that could scale to large, complex networks became evident. OSPF was designed with scalability in mind, allowing it to handle thousands of routers and networks.

Unlike RIP, which uses hop count as the routing metric, OSPF uses **cost** as its metric. This cost is calculated based on the bandwidth of the link, allowing OSPF to prioritize higher-speed links for routing traffic. The use of a more flexible metric makes OSPF suitable for large-scale networks that require more intelligent routing decisions.

Moreover, OSPF's ability to break down a large network into smaller **areas** helps reduce the size of routing tables. Each area in OSPF has a limited scope, so routers only need to store information about their local area, reducing the amount of routing information exchanged between routers. This hierarchical design makes OSPF highly scalable, even in massive enterprise environments.

2. Fast Convergence and Network Stability

Convergence refers to the process of routers updating their routing tables to reflect changes in the network, such as a failed link or router. RIP's slow convergence times, which could take minutes, were unacceptable for larger, dynamic networks where high availability and minimal downtime were crucial.

OSPF was designed for **fast convergence**. When a change occurs in the network, OSPF immediately notifies neighboring routers and recalculates the shortest path tree using the **Dijkstra algorithm**. The time taken to update routing tables is significantly shorter in OSPF compared to RIP, which helps reduce network downtime and instability. Fast convergence is critical for enterprise networks, particularly those supporting real-time applications like voice, video, and financial transactions, where even a short delay can cause significant disruptions.

Efficient Use of Resources

Another significant improvement offered by OSPF is its **efficiency** in the use of network resources, particularly **bandwidth**. Unlike RIP, which sends complete routing tables every 30 seconds, OSPF only sends updates when there is a change in the network topology. These updates are much smaller in size, as they only contain information about the changes rather than the entire routing table. This approach minimizes unnecessary traffic and helps conserve bandwidth.

Additionally, OSPF supports **incremental updates**, where routers only exchange the new or modified routing information rather than sending the entire database. This significantly reduces the amount of data transmitted, further optimizing bandwidth usage.

4. Hierarchical Network Design with Areas

OSPF's support for **hierarchical network design** was another key factor that set it apart from RIP. The concept of areas in OSPF allows large networks to be segmented into smaller, more manageable regions. By dividing the network into areas, OSPF reduces the complexity of routing and ensures that each router only needs to maintain information about its area, rather than the entire network.

The **backbone area (Area 0)** serves as the central hub that connects all other areas in an OSPF network. This hierarchical approach not only makes OSPF more scalable but also enhances network stability and performance by limiting the scope of routing information within each area.

5. Vendor Independence and Open Standard

OSPF was developed as an **open standard** by the IETF, making it independent of any particular hardware or software vendor. This was a significant advantage over earlier proprietary protocols, such as Cisco’s proprietary **IGRP** (Interior Gateway Routing Protocol), which was limited to Cisco routers. The open nature of OSPF allowed it to be implemented by any router manufacturer, leading to broad adoption across different hardware platforms and making it suitable for multi-vendor environments.

This open standardization of OSPF allowed businesses to avoid vendor lock-in and make use of a wide range of networking hardware from different manufacturers while still benefiting from a consistent and interoperable routing protocol.

2.5 Conclusion: The Importance of OSPF

The development of **OSPF** was driven by the need to address the scalability, efficiency, and reliability issues faced by earlier routing protocols like **RIP**. By offering fast convergence, efficient use of resources, hierarchical network design, and scalability, OSPF quickly became the preferred routing protocol for large-scale enterprise networks and service providers.

While OSPF has its limitations, particularly in terms of configuration complexity and overhead in large networks, its benefits in terms of speed, flexibility, and interoperability have made it a cornerstone of modern network routing. As enterprise networks continue to grow in size and complexity, OSPF remains a critical component in ensuring that networks remain reliable, efficient, and capable of handling the demands of today’s data-driven world.

The ongoing development of OSPF, including enhancements for security and support for newer technologies like **IPv6**, ensures that it will continue to play a crucial role in the future of networking, providing a robust and reliable solution for enterprises and service providers worldwide.

CHAPTER-III

REQUIRMENT ANALYSIS & SPECIFICATIONS

3.1 Network Architecture: A network architecture is the design and structure of computer network including the relationship between components such as devices, connectivity and protocols. A network architecture for enterprise network include:

1. **Access layer**
2. **Distribution layer**
3. **Core layer**

1.1 Access layer: access layer connect end users to the network. This is the first layer of the network architecture that responsible for connecting end users to the network e.g. workstations, mobile devices, and IOT and wireless devices.

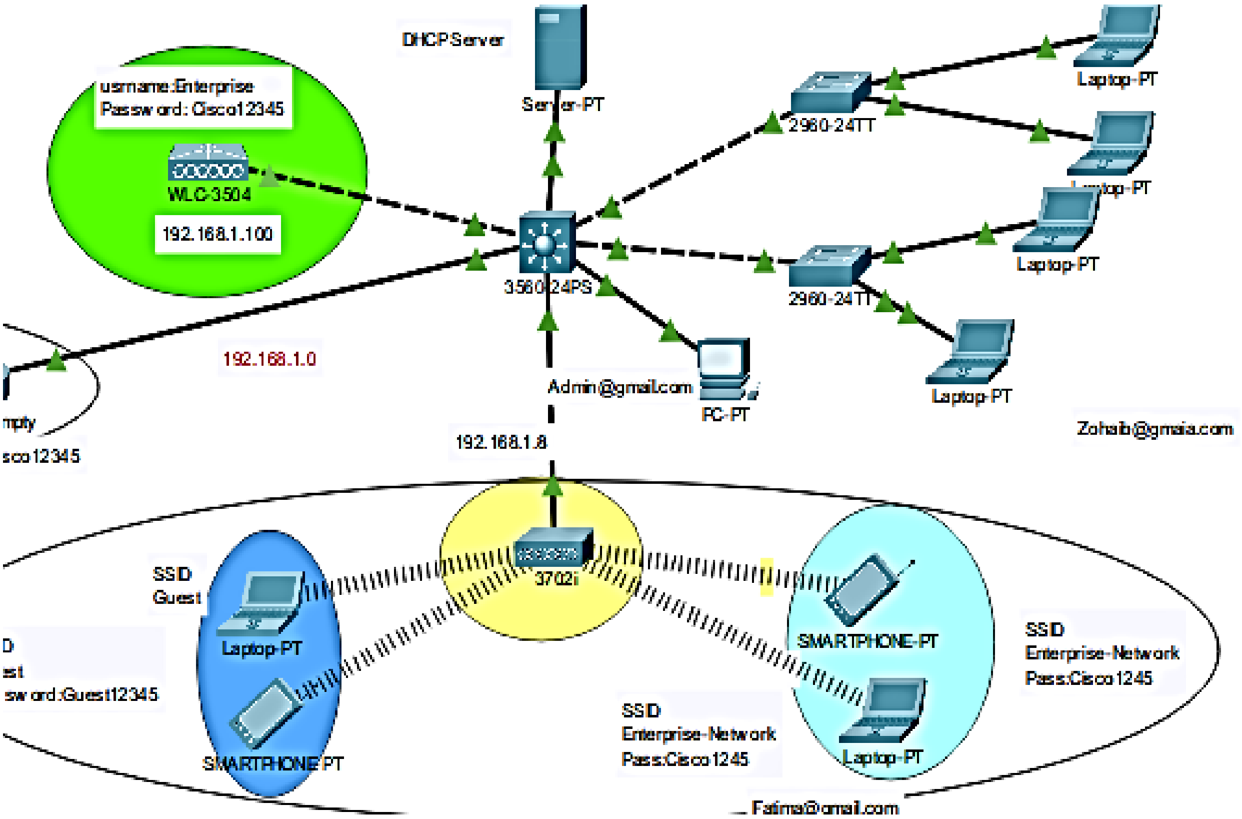


Figure 3.1

In the above figure the network inside the red rectangle represent the access layer of the network.

3.2 Distribution layer: This layer is also known as aggregation layer and this is the second layer of network architecture situated between the access and core layer.

It aggregate multiple access layers connection, and provide connectivity to core layer it enforce the network security policies and optimize network flow and routing.

The distribution layer typically consist of:

- Routers
- Multilayer switches
- Network devices with capability of routing and switching

3.3 Core Layer: This layer is known as the backbone or central layer of the network architecture and responsible for High speed data transfer, low latency switching and routing, Redundancy and fault tolerance, and scalability and reliability. The core layer is designed to connect multiple distribution layers and provide high speed connectivity to the network. It ensure high availability and redundancy to support large scale network growth.

We will discuss the architecture of network briefly in the upcoming chapter.

3.1.2 NETWORK SIZE AND SCOPE:

The network size and scope refers to the scale and boundaries of a network. The network size can be small, Medium, large, Enterprise or Massive. But here we will talk about the Enterprise network.

Enterprise network contain 10,000 to 100,000 devices (data center, cloud infrastructure, Multilayer switches, Routers, End devices, Wireless devices etc.)

The Network Scope:

The network scope include:

- LAN (Local area network): A single geographical location like office building or home or campus.
- MAN (Metropolitan area network): Covers a large geographical area like town, city or metropolitan area.
- WAN (Wide area network): A connection of multiple geographical locations such as country or globe.
- WLAN (Wireless Local area network): a wireless network that cover a specific area in the organization or home or office.

Factors that effects the network size and scope:

- Organization size and scope
- Geographical dispersion
- Number of users and devices
- Technology and infrastructure requirements

3.1.3 Network Performance: The network performance refers to the efficiency and effectiveness of a network in transmitting the data, facilitating communication and support applications. It encompass various aspect:

1. Throughput: the rate at which data is successfully transmitted, measures in bits per seconds (bps).
2. Latency: the delay between data transmission and reception, measure in milliseconds.
3. Packet Loss: data packets failed to be delivered, impacting network reliability.
4. Availability: the network ability to remain operational and accessible.
5. Response time: The time taken for the data to be transmitted and processed.
6. Network Utilization: the percentage of available bandwidth used.

Optimizing the network performance is crucial for:

1. Productivity
2. User Experience
3. Reliability
4. Security

3.1.4 SECURITY: Security is one the crucial aspect of enterprise network which require careful consideration to ensure the network integrity and performance.

Some security aspects are given below:

1. AAA (Authentication, Authorization and accounting) services to control user access.
2. Network segmentation to isolate sensitive areas.
3. Encryption to protect data during transmission
4. Incident response plane to quickly respond to security breaches.

3.1.5 Scalability: Scalability is also a crucial aspect in enterprise networking. It distribute architecture to handle increased traffic and users.

- ➢ Load balancing to distribute traffic across multiple devices.
- ➢ Redundancy and failover mechanisms to ensure high availability.

- Scalable switching and routing infrastructure.
- Upgrade and migration strategies to adapt to evolving network demands.

3.2 Requirement Analysis:

The requirement analysis for our network is:

- 3 Branches and 1 data center connect with each other
- Throughput up 1Gbps
- Packet loss <1%
- Encryption of data while in transit
- SSH on each router
- Uptime 99.99%
- Down time < 1hour/month
- User growth 20%/year
- Device growth 30%/year
- Bandwidth growth 50%/year
- Respond time <3 sec
- Data center availability 99.99%
- Configuration management
- Mentoring: Simulation base
- ACLs for critical users
- Redundancy: Duplication of critical components
- Wireless network
- Fast convergence using OSPF
- Email, Web, DHCP, NTP, Syslog Services
- Email id for each client in each branch

3.2.2 User Requirements:

- Connectivity (reliable and secure access to the network)
- High speed network connectivity
- Application access (email, file sharing, printing)
- High availability for critical applications/ services
- Protection of sensitive data
- User authentication and authorization
- Access control
- Secure remote access to the network and resources

- Support for mobile devices
- Network reliability and uptime (minimal down time)
- Rapid issue resolution and technical support
- User friendly network services
- Fast response time

3.2.3 DEVICE REQUIRMENTS (SOFTWARE AND HARDWARE)

Software Requirements:

- Cisco packet tracer
- Operating system (Windows 10)

Hardware Requirements

- Core i5 4th Generation Laptop or PC
- RAM 8GB
- 2.5Ghz processer

CHAPTER-IV

NETWORK DESIGNING

4.1 INTRODUCTION: A network designing is the process of planning, designing, and building a computer network infrastructure to meet the specific requirements and functionalities. It involve creating a conceptual and logical design, developing a detailed physical design, selecting and configuring network devices, ensuring network security, scalability and performance.

A network designing consider network topology and architecture, network protocols and services, network management, network security and access control and network scalability and performance. A good network design meet user requirements and business needs, ensure reliable and secure connectivity, support network growth, optimize network performance and efficiency, and facilitating network management and troubleshooting.

A good network design involves understanding network fundamentals, analyze user requirements, designing network architecture, selecting network devices, configure network protocols and services and testing and validating network design. To follow these structure approach we can design a good network that meet user requirements and it will be a robust, efficient and secure network that support their operations and goals.

A good network design approach contain these steps:

- Assessing needs
- Designing topology
- Selecting components
- Configuring protocols
- Ensuring scalability
- Optimizing performance
- Implementing security
- Testing and validation

The effective network design ensure:

- Reliable connectivity
- High availability
- Scalability
- Security
- Manageability

- Optimal performance

4.2 CISCO 3 TEIR ARCHITECTURE MODEL: A CISCO 3 tier architecture is a network design model that include access layer, distribution layer, and core layer. Each layer has a specific role in directing the traffic and ensuring efficient network performance.

4.2.1 Access layer: it is the first layer of network design and responsible for connecting edge or end devices. It provide access for the devices like Computers, laptops, mobile devices, tablets, IoT devices, access points and wireless controllers.

This layer typically consist of:

- Network access devices
- Network interface cards
- Wi-Fi

The primary function of this layer is to provide connectivity, Authentication, policy enforcement, traffic forwarding. This layer is critical for user access and authentication, network security, Quality of services and network availability and reliability. A well design access layer ensure secure, reliable, and high-performance connectivity for end-users, setting the foundation for a robust and efficient network design.

4.2.2 Distribution layer: This layer is also known as aggregation layer and this is the second layer of network architecture situated between the access and core layer.

It aggregate multiple access layers connection, and provide connectivity to core layer it enforce the network security policies and optimize network flow and routing.

The distribution layer typically consist of:

- Routers
- Multilayer switches
- Network devices with capability of routing and switching

4.2.3 Core Layer: This layer is known as the backbone or central layer of the network architecture and responsible for High speed data transfer, low latency switching and routing, Redundancy and fault tolerance, and scalability and reliability. The core layer is designed to connect multiple distribution layers and provide high speed connectivity to the network. It ensure high availability and redundancy to support large scale network growth.

Figure 4.1

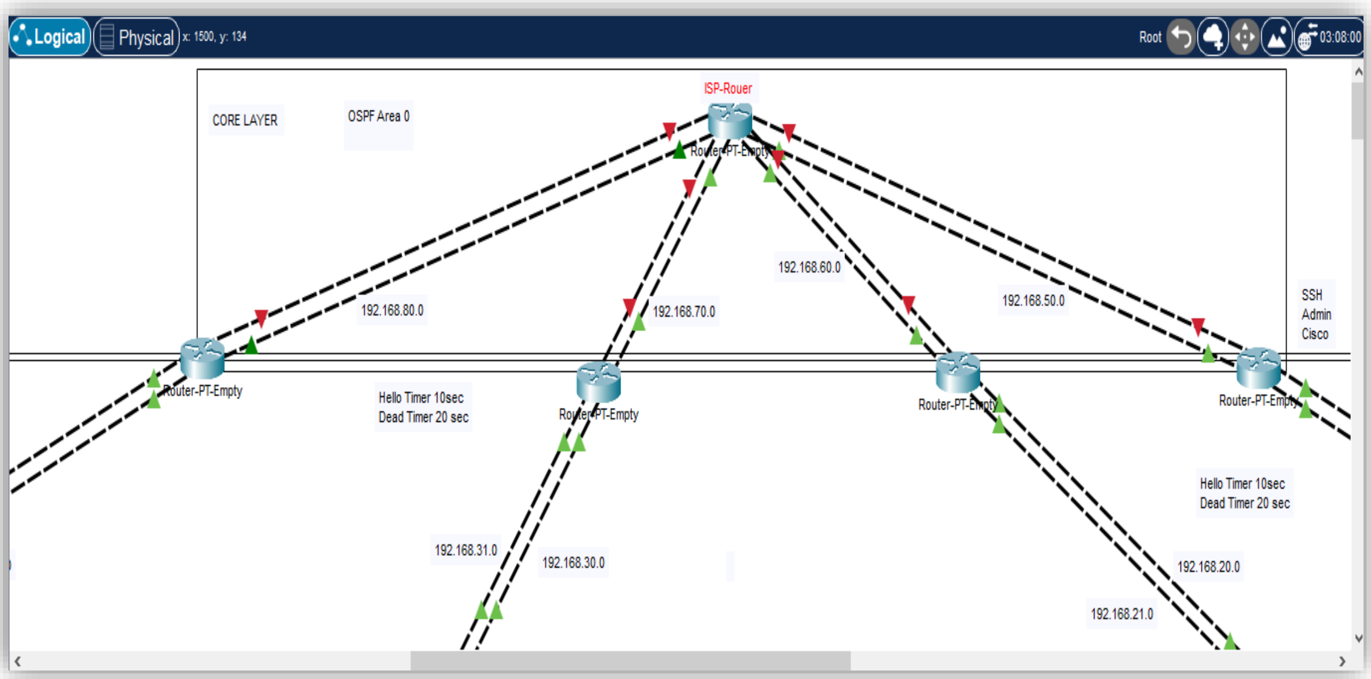


Figure 4.1

In the above figure the Karachi branch are connect through the router to the ISP-Router.

4.3 CONNECTING 4 BRANCHES VIA ISP: Now we will connect our 4 branches via ISP router and we will establish a wide area network connection between the branches with redundant links.

In my topology the router that locate in the core layer is act as an ISP-Router and we will connect all of our branches to ISP-Router.

Connection steps:

1. Select ISP-Router
2. Go to each interface
3. Provide IP address to a particular interface that connect to the ISP router
4. Configure OSPF as a routing protocol
5. Ensure that each branch has a unique subnet
6. Provide loopback address to each router

4.3.1 Karachi Branch Connection:

The Karachi branch contains the DHCP server and both wired and wireless network through the DHCP server all the branches can get the ip addresses according to their subnet. And can properly communicate to each other's.

4.3.2 Islamabad Branch Connection

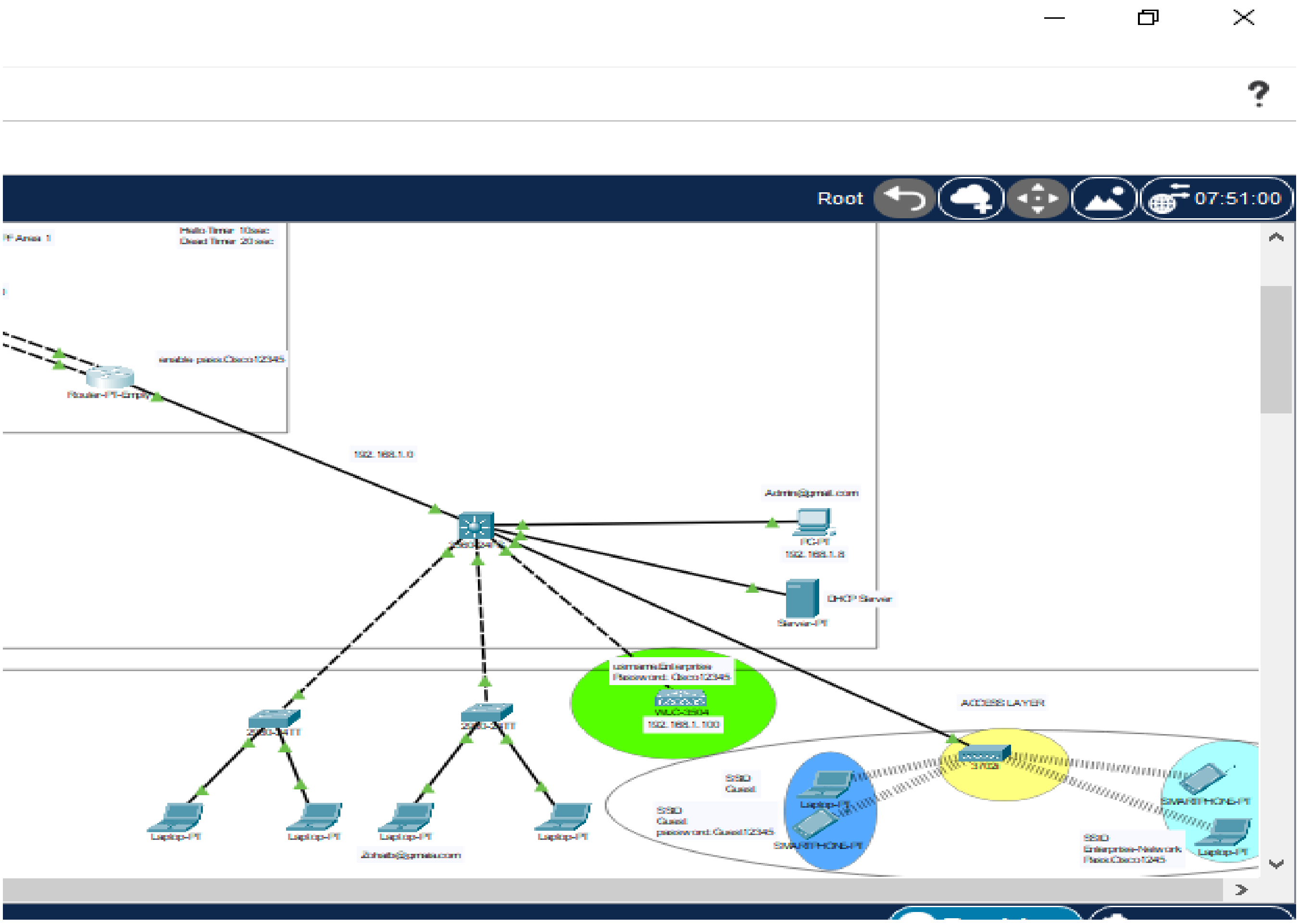


Figure 4.1

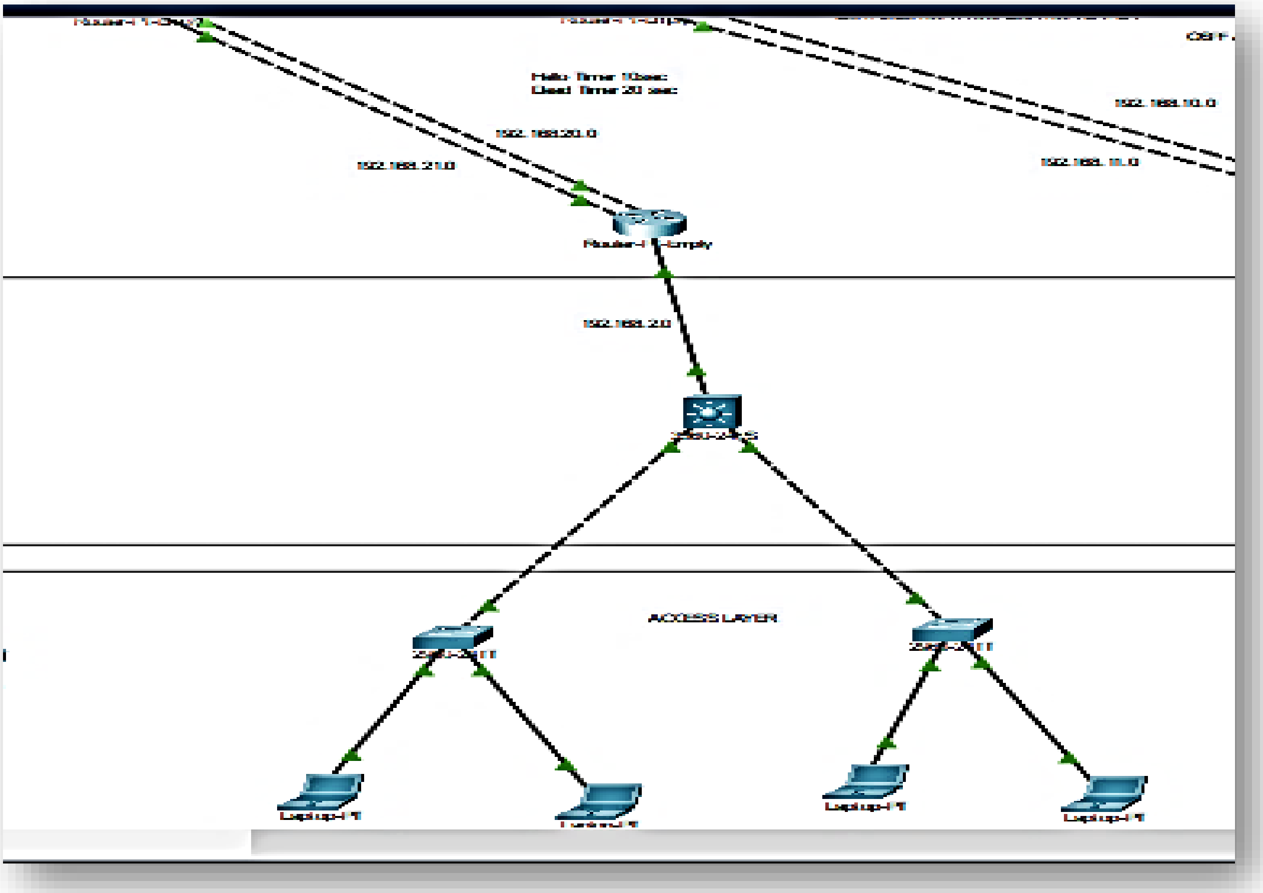


Figure 4.2

The above figure Islamabad branch are connected to the distribution layer and having the subnet of 192.168.2.0 and the redundant links subnet are 192.168.20.0 and 192.168.21.0.

4.3.3 Lahor Branch Connection:

The lahor branch are connected through the distribution layer and can communicate all over the network. The subnet of lahor branch is 192.168.3.0 for internal network and for distribution layer the subnet is 192.168.30.0 and 192.168.31.0 for redundant links. This branch include both wired and wireless networks.

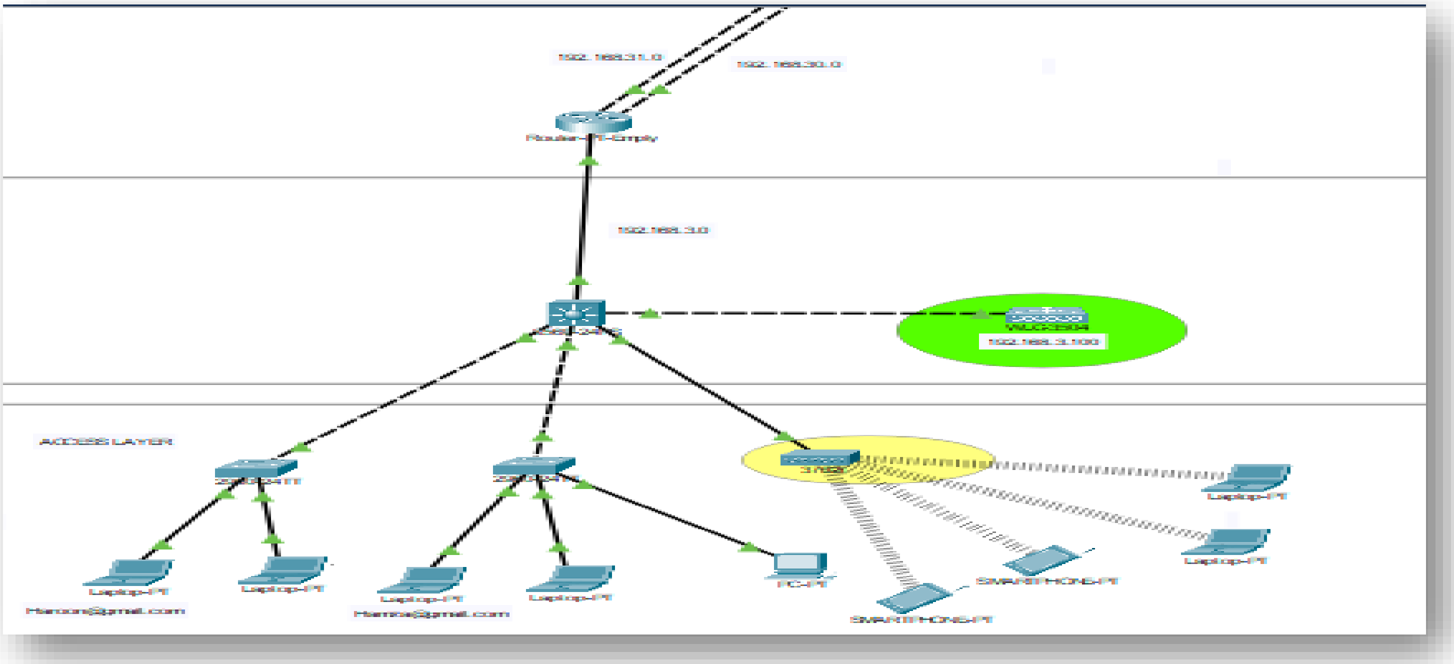


Figure 4.3

4.3.4 IT Data Center Connection: The data center contains the web server, DNS server, Email server, NTP server and Syslog server that give facilities and services across the network or any branch of the network. The data center play a crucial role in enterprise network and the services that are mentioned above also crucial that's why we add these services in our network.

Also we have a redundancy and switching techniques (STP, Ether channels) in our data center to provide better services with 0% delay also providing redundant systems, load balancing and high availability solutions. The data center services enable the enterprise networks to improve data center efficiency, enhance scalability, and flexibility, increase data availability and security.

By outsourcing the data center services enterprise network can leverage expertise, reduce risks, and improve overall IT infrastructure.

4.4Network Devices Selection: A network device selection is important for any network. When selecting network devices the following factors can be consider:

- Performance
- Security
- Scalability
- Compatibility
- Reliability
- Distance
- Environment

- Budget

4.5 Network devices:

- L2 Switches 2950 model
- L3 Switch 3560 model
- Router PT 1000 model version 12.2
- AP 3702 model
- WLC 3504 model
- Smart phones
- PCs
- Laptop
- DHCP server
- NTP server
- Syslog server
- DNS server
- Web server
- Email server

4.6 Implementation & Deployment: implementation and deployment is the process of setting up and configuring network devices, services, protocols and device configurations to meet the organization requirements.

It involve network designing, device procurements, configuration and testing.

Deployment is the process of:

4.6.1 Staging: prepare device for deployment by configuring basics setting and test the connectivity.

4.6.2 Installation: install devices in their final location connect them and cabling.

4.6.3 Configuration: configure device settings and activity services.

4.6.4 Integration: integrate new devices with existing network infrastructure and services.

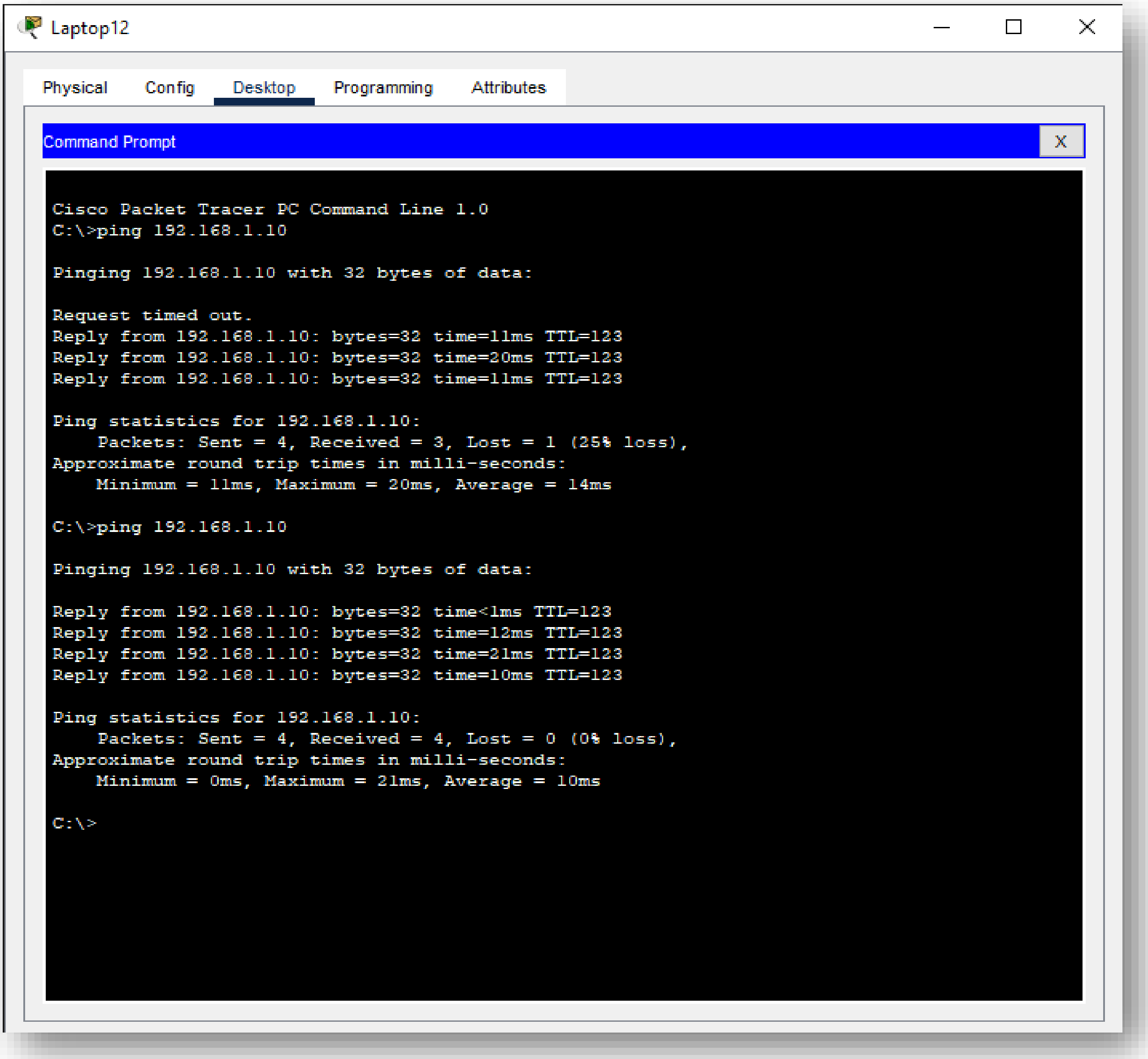
4.6.5 Verification: verify that the network is properly functioning, meeting performance and security requirements.

4.6.6 Documentation: update network documentation to reflect new devices configurations.

4.6.7 Maintenance: Perform maintenance, monitoring and troubleshooting to ensure network reliability.

4.7 Testing and Validation: Testing and Validation is the important step in the network process to ensure that the network function, working is correct, efficient and secure. Testing can be unit testing, integration testing, compatibility testing, performance testing and acceptance testing. By testing we can verify that network meet the required specifications, working properly and secure which is essential for reliable communication and data transfer.

4.7.1 Validation: Validation mean verify the connectivity that each device can connect to the network, verify the configuration, verify performance, and verify security, compatibility, scalability, reliability and compliance to ensure that the network meet the regulatory and industry standers.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.10: bytes=32 time=11ms TTL=123
Reply from 192.168.1.10: bytes=32 time=20ms TTL=123
Reply from 192.168.1.10: bytes=32 time=11ms TTL=123

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 11ms, Maximum = 20ms, Average = 14ms

C:\>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Reply from 192.168.1.10: bytes=32 time<1ms TTL=123
Reply from 192.168.1.10: bytes=32 time=12ms TTL=123
Reply from 192.168.1.10: bytes=32 time=21ms TTL=123
Reply from 192.168.1.10: bytes=32 time=10ms TTL=123

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 21ms, Average = 10ms

C:\>
```

Figure 4.4

In the above figure the data center employee want to communicate with Karachi branch employee and when he/she ping the Karachi branch employee then ping is successful. It mean the connectivity between the devices is OK. And everyone from the data center to Karachi branch can successfully communicate with each other and can transfer the data among each other's.

CHAPTER-V

Routing

5.1 Introduction: A routing is the process of directing data packets between the networks, ensuring that data packets reach to their destination. It is the critical function in networking that enable data exchange between devices on different network.

Routing involve determining the best path for the data to travel, forwarding data between networks, using routing table to store network address information, and update routing table with new information. Router and multilayer switches perform routing on the base of destination ip address, network mask, routing protocol and metric value. Efficient routing ensure reliable transmission, optimal network performance, reduce latency, and scalability.

5.2 OSPF: Introduction to OSPF:

Open Shortest Path First

- IEEE developed this open source protocol which work on shortest path first algorithms and support biggest possible networks.
- It is a link state routing protocol. The metric of OSPF is "COST".

  Cost= 10^8/Bandwidth
- The AD (Administrative Distance) Value of OSPF is 110
- OSPF works on Dijkstra Algorithms
- OSPF normally uses 224.0.0.5 as its multicast IP
- OSPF creating and maintain all three Tables:
  - Routing Table
  - Topology table
  - Neighbor table

5.2.1 Why Link State?

A major drawback of distance vector protocols is that they not only send routing updates at a regularly schedule time, but these routing updates contain full routing table for that protocol.

If the sending router know of more the 25 RIP routes, the updates will requires multiple packets, since a RIP update packet contain a max of 25 routes.

This take up valuable bandwidth and puts unnecessary drain on the receiving router CPU and memory.

Now Link state protocol do not exchange routes and metrics. Link-state protocol exchange just that the state of their links, and the cost associated with those link.

As these link state Advertisement (LSA) arrive form OSPF neighbors, the router perform a series of computations on these LSAs giving the router a complete picture of the network.

This series of computations is known as Shortest Path First (SPF) Algorithms also referred as the Dijkastra Algorithms.

This exchange of LSAs between neighbors helps bring about one major advantage of link state protocols. All routers in the network will have similar view of the overall network.

In comparison to RIP update every 30 sec OSPF LSAs aren't sent out all the often, they're flooded when there's an actual change in the network and each LSA is refreshed every 30 minutes.

Before any LSA exchange can begin, a neighbor relationship must be formed. Neighbor must be discovered and form an adjacency, after which LSAs will exchanged.

5.2.2 LSA Sequence Numbers: To ensure that OSPF router have the most recent information possible in their database the LSA are assigned sequence number.

When an OSPF enabled router receive an LSA that router check its OSPF database for any pre-existing entries for that link.

If there is any entry for the link the sequence numbers come into play:

Sequence number is the same: LSA is ignored no additional action taken

Sequence number is lower: The router ignores the update and transmits an LSU containing as LSA back to the original sender. Basically the router with the most recent information in telling the original sender "Hey, you send me old information, here's the latest information on that link"

Sequence number is higher: The router add the LSA to its database and sends an LSA acknowledge back to the original sender. The route floods the LSA and updates its own routing table by running the SPF algorithms against the now-updated database.

5.2.3 PROCESS_ID: In OSPF the Process-ID play important role in the configuration of OSPF.

The process-id in OSPF is a locally significant identifier used to distinguish between multiple OSPF processes running on the same router. It is used to differentiate different instances of OSPF on the same device.

The Process-ID value is arbitrary and can be any number the administrator choose. It is considered best practice to use the same process-ID an all OSPF router within the same autonomous system.

The full command for configuration OSPF with the Process ID is

Router OSPF <process-id>

5.2.4 WILDCARD MASK: the wildcard mast is used in the network command to identify which interface will participate in OSPF and in which area.

The wildcard mask is not a subnet mask but a way to specify which bits of IP address should be considered when matching interfaces to the network command.

The wildcard mask is used in the network command in the format

Network IP-Address wildcard mask area and area-id

It is important to note that OSPF uses wildcard mask not subnet mask in the network command for interface matching.

5.2.5 HELLO-PACKETS: Hello packets are the heartbeat of OSPF. OSPF enabled interfaces send help packets at regularly scheduled intervals.

Hello packets perform two main task in OSPF.

1. OSPF hellos allow neighbor to dynamically discover each other.
2. OSPF hello allow the neighbor to remind each other that they are still there, which mean they are still neighbors.

5.2.6 OSPF Packet Type:

- T1(HELLO Packets)
- T2(LSBD Packets)
- T3(LSR)
- T4(LSU)
- T5(LSA)

5.2.7 Neighbor Condition:

- Same Area
- Same Network Segment
- Same Authentications
- Same Timer
- Same MTU

5.2.8 OSPF FINITE STATE MACHINE:

1. Down: No OSPF process running at either side
2. Init: OSPF initiated at one side
3. 1-Way: OSPF running on the link
4. 2-Way: Router-ID seen by both of the routers
5. Exstart: LSBD packets exchange started
6. Exchange: LSBD packets exchange process complete.
7. Loading: SPF algorithms running and creating SPT.

Here our OSPF routing table with the help of “show ip route” command

```
#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - Periodic downloaded static route
Gateway of last resort is not set
C 1.0.0.0/8 is directly connected, Loopback0
2.0.0.0/32 is subnetted, 1 subnets

O IA 2.2.2.2 [110/5] via 192.168.10.2, 00:01:28, FastEthernet9/0
[110/5] via 192.168.11.2, 00:01:28, FastEthernet0/0
3.0.0.0/32 is subnetted, 1 subnets

O IA 3.3.3.3 [110/5] via 192.168.10.2, 00:01:28, FastEthernet9/0
[110/5] via 192.168.11.2, 00:01:28, FastEthernet0/0
4.0.0.0/32 is subnetted, 1 subnets

O IA 4.4.4.4 [110/5] via 192.168.10.2, 00:01:28, FastEthernet9/0
[110/5] via 192.168.11.2, 00:01:28, FastEthernet0/0
5.0.0.0/32 is subnetted, 1 subnets
```

```
O IA 5.5.5.5 [110/2] via 192.168.10.2, 00:01:38, FastEthernet9/0
[110/2] via 192.168.11.2, 00:01:38, FastEthernet0/0
6.0.0.0/32 is subnetted, 1 subnets

O IA 6.6.6.6 [110/4] via 192.168.10.2, 00:01:38, FastEthernet9/0
[110/4] via 192.168.11.2, 00:01:38, FastEthernet0/0
7.0.0.0/32 is subnetted, 1 subnets

O IA 7.7.7.7 [110/4] via 192.168.10.2, 00:01:38, FastEthernet9/0
[110/4] via 192.168.11.2, 00:01:38, FastEthernet0/0
8.0.0.0/32 is subnetted, 1 subnets

O IA 8.8.8.8 [110/4] via 192.168.10.2, 00:01:38, FastEthernet9/0
[110/4] via 192.168.11.2, 00:01:38, FastEthernet0/0
9.0.0.0/32 is subnetted, 1 subnets

O IA 9.9.9.9 [110/3] via 192.168.10.2, 00:01:38, FastEthernet9/0
[110/3] via 192.168.11.2, 00:01:38, FastEthernet0/0

C 192.168.1.0/24 is directly connected, FastEthernet8/0

O IA 192.168.2.0/24 [110/5] via 192.168.10.2, 00:01:28, FastEthernet9/0

[110/5] via 192.168.11.2, 00:01:28, FastEthernet0/0

O IA 192.168.3.0/24 [110/5] via 192.168.10.2, 00:01:28, FastEthernet9/0

[110/5] via 192.168.11.2, 00:01:28, FastEthernet0/0

O IA 192.168.4.0/24 [110/5] via 192.168.10.2, 00:01:28, FastEthernet9/0

[110/5] via 192.168.11.2, 00:01:28, FastEthernet0/0
```

```
C 192.168.10.0/24 is directly connected, FastEthernet9/0

C 192.168.11.0/24 is directly connected, FastEthernet0/0

O IA 192.168.20.0/24 [110/4] via 192.168.10.2, 00:01:28, FastEthernet9/0
[110/4] via 192.168.11.2, 00:01:28, FastEthernet0/0

O IA 192.168.21.0/24 [110/4] via 192.168.10.2, 00:01:28, FastEthernet9/0
[110/4] via 192.168.11.2, 00:01:28, FastEthernet0/0

O IA 192.168.30.0/24 [110/4] via 192.168.10.2, 00:01:28, FastEthernet9/0
[110/4] via 192.168.11.2, 00:01:28, FastEthernet0/0

O IA 192.168.31.0/24 [110/4] via 192.168.10.2, 00:01:28, FastEthernet9/0
[110/4] via 192.168.11.2, 00:01:28, FastEthernet0/0

O IA 192.168.40.0/24 [110/4] via 192.168.10.2, 00:01:28, FastEthernet9/0
[110/4] via 192.168.11.2, 00:01:28, FastEthernet0/0

O IA 192.168.41.0/24 [110/4] via 192.168.10.2, 00:01:28, FastEthernet9/0
[110/4] via 192.168.11.2, 00:01:28, FastEthernet0/0

O IA 192.168.50.0/24 [110/2] via 192.168.10.2, 00:01:38, FastEthernet9/0
[110/2] via 192.168.11.2, 00:01:38, FastEthernet0/0

O IA 192.168.60.0/24 [110/3] via 192.168.10.2, 00:01:38, FastEthernet9/0
[110/3] via 192.168.11.2, 00:01:38, FastEthernet0/0

O IA 192.168.70.0/24 [110/3] via 192.168.10.2, 00:01:38, FastEthernet9/0
[110/3] via 192.168.11.2, 00:01:38, FastEthernet0/0

O IA 192.168.80.0/24 [110/3] via 192.168.10.2, 00:01:38, FastEthernet9/0
[110/3] via 192.168.11.2, 00:01:38, FastEthernet0/0
```

The following table show all the routes that are belong to our network

3.1 OSPF Configuration on each Router:

Here the details of Router that how we configure OSPF on each router

```
router ospf 1
log-adjacency-changes
network 192.168.10.0 0.0.0.255 area 1
network 192.168.1.0 0.0.0.255 area 1
network 1.1.1.1 0.0.0.0 area 1
network 192.168.11.0 0.0.0.255 area 1
```

Here the OSPF 1 is the process id of our network and 192.168.10.0 is the network id and 0.0.0.255 are the wildcard mask of the network and the network belong to area 1 of the OSPF while are 0 are the backbone area and our Core router and distribution routers are in the area 0 which is the backbone area, and every router must be connected to the backbone router otherwise adjacency cannot be established.

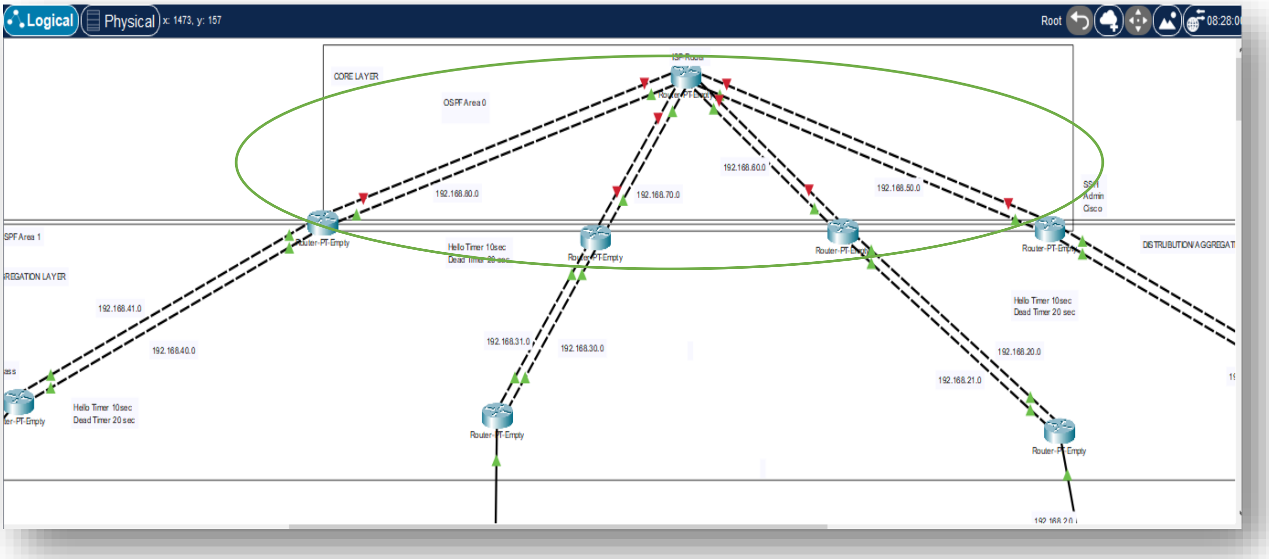
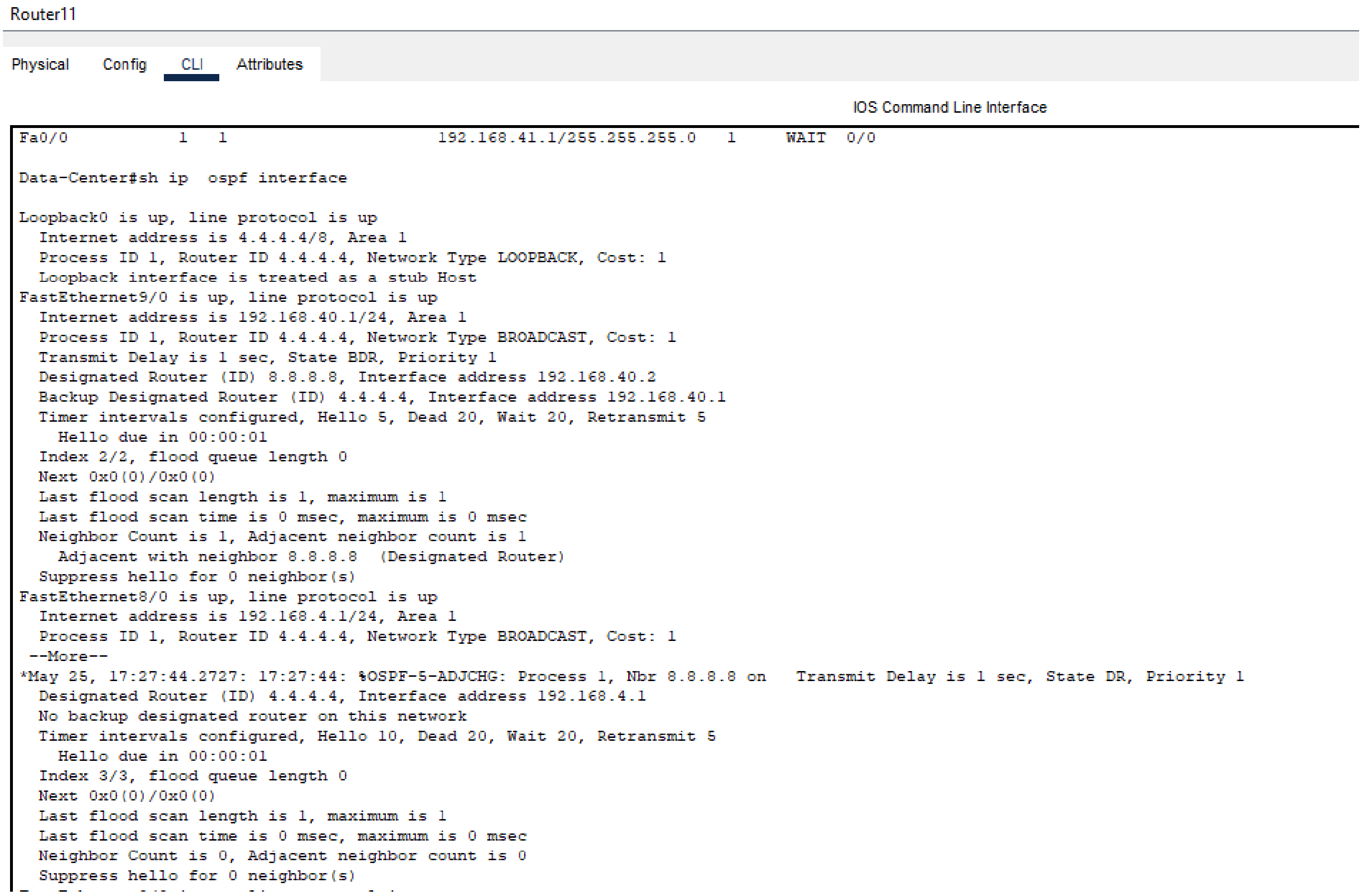


Figure 5.1

In the above figure the green circle represent the area 0 every router is connect to the backbone area which is area 0.

4.1 Hello and dead packet timer: Hello and dead packet in OSPF play a crucial role in maintaining neighbor relationship and detecting network failures.



```
Fa0/0           1   1                    192.168.41.1/255.255.255.0   1     WAIT  0/0

Data-Center#sh ip  ospf interface

Loopback0 is up, line protocol is up
  Internet address is 4.4.4.4/8, Area 1
  Process ID 1, Router ID 4.4.4.4, Network Type LOOPBACK, Cost: 1
  Loopback interface is treated as a stub Host
FastEthernet9/0 is up, line protocol is up
  Internet address is 192.168.40.1/24, Area 1
  Process ID 1, Router ID 4.4.4.4, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 8.8.8.8, Interface address 192.168.40.2
  Backup Designated Router (ID) 4.4.4.4, Interface address 192.168.40.1
  Timer intervals configured, Hello 5, Dead 20, Wait 20, Retransmit 5
    Hello due in 00:00:01
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 8.8.8.8  (Designated Router)
  Suppress hello for 0 neighbor(s)
FastEthernet8/0 is up, line protocol is up
  Internet address is 192.168.4.1/24, Area 1
  Process ID 1, Router ID 4.4.4.4, Network Type BROADCAST, Cost: 1
 --More--
*May 25, 17:27:44.2727: 17:27:44: %OSPF-5-ADJCHG: Process 1, Nbr 8.8.8.8 on   Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 4.4.4.4, Interface address 192.168.4.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 20, Wait 20, Retransmit 5
    Hello due in 00:00:01
  Index 3/3, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
```

Figure 5.2

5.1.1 Hello interval: the hello interval define how the routers send hello packets to their neighbors to establish and maintain neighbor relationship. It is essential mechanism for router to discover and maintain neighbor relationship within the OSPF network.

5.1.2 Dead interval: The dead interval define how long a router should wait for the hello packets form a neighbor before declaring the neighbor as unreachable. Typically the dead interval is set to four time the hello interval but this is not a strict rule.

In the above figure the encircle line show the hello and dead interval of a router.

5.2OSPF Database: The OSPF database also known as the Link state Database is a critical component of OSPF routing protocol. It is a repository of information that stores the network topology, including routers, links and networks. Each OSPF router maintain a copy of database, which is synchronized with its neighbors to ensure consistency.

5.2.1 Key components of OSPF Database: LSA (Link state Advertisement) are the packets that contain information about the network topology. There are different types of LSAs including Type 1(Router LSA), Type 2(Network LSA), Type 3(Summary LSA), and Type 5(External LSA).

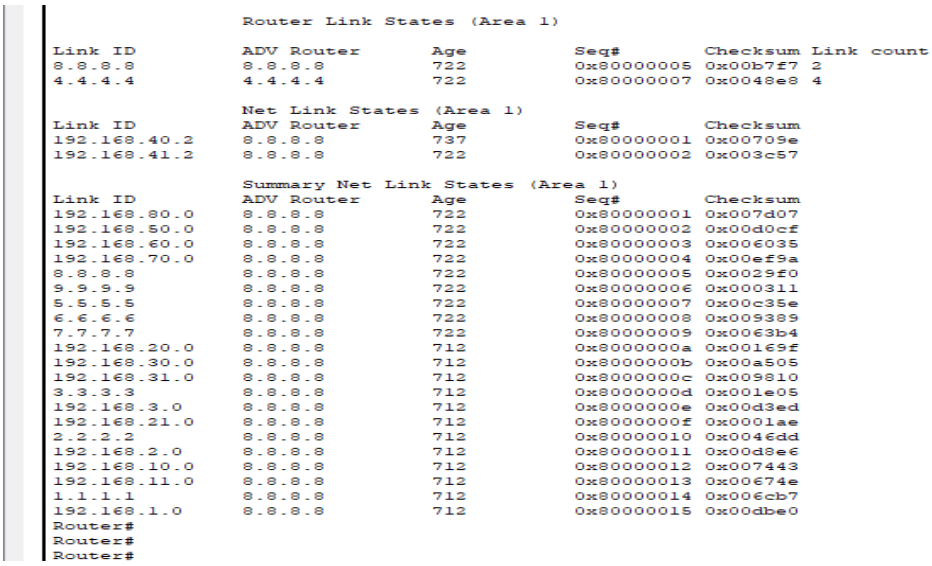
5.2.2 LSR (Link State Record) these are entries in the database that correspond to LSAs received form neighbor routers.

5.2.3 Link State Age: This is the timer that indicates the age of LSA

How OSPF database work:

1. Each OSPF router send LSAs to its neighbors which are then stored in the database.
2. The database is synchronized among routers through a process called flooding.
3. Router use information in the database to construct a map of the network topology.
4. The SPF algorithms is used to calculate the best path to each destination network.

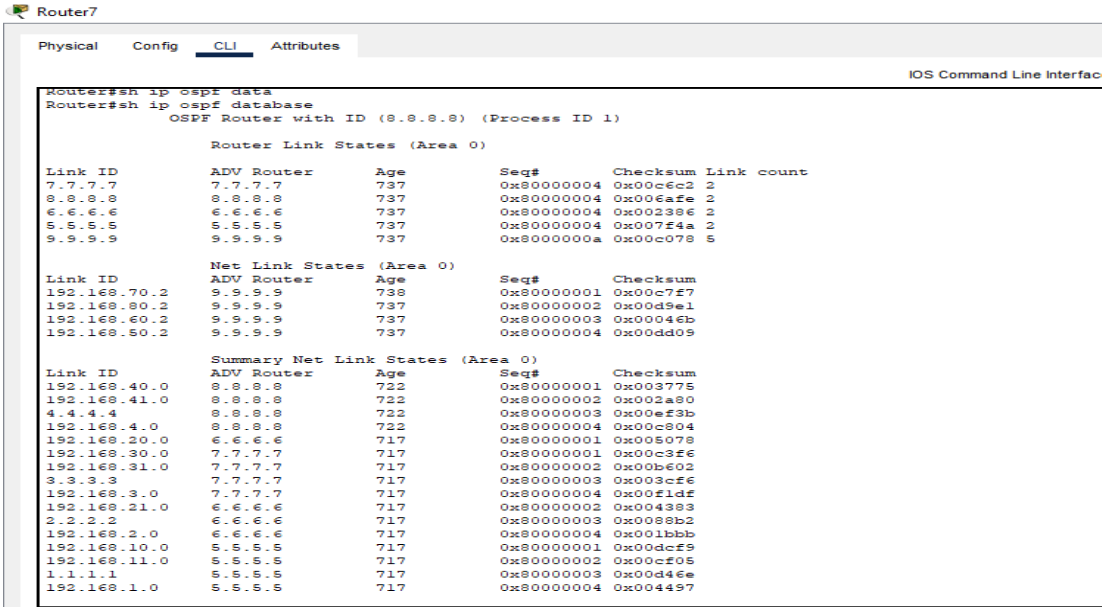
We can see the OSPF Database with the help of the following command



```
                Router Link States (Area 1)

Link ID         ADV Router      Age         Seq#       Checksum Link count
8.8.8.8         8.8.8.8         722         0x80000005 0x00b7f7 2
4.4.4.4         4.4.4.4         722         0x80000007 0x0048e8 4

                Net Link States (Area 1)
Link ID         ADV Router      Age         Seq#       Checksum
192.168.40.2    8.8.8.8         737         0x80000001 0x00709e
192.168.41.2    8.8.8.8         722         0x80000002 0x003c57

                Summary Net Link States (Area 1)
Link ID         ADV Router      Age         Seq#       Checksum
192.168.80.0    8.8.8.8         722         0x80000001 0x007d07
192.168.50.0    8.8.8.8         722         0x80000002 0x00d0cf
192.168.60.0    8.8.8.8         722         0x80000003 0x006035
192.168.70.0    8.8.8.8         722         0x80000004 0x00ef9a
8.8.8.8         8.8.8.8         722         0x80000005 0x0029f0
9.9.9.9         8.8.8.8         722         0x80000006 0x000311
5.5.5.5         8.8.8.8         722         0x80000007 0x00c35e
6.6.6.6         8.8.8.8         722         0x80000008 0x009389
7.7.7.7         8.8.8.8         722         0x80000009 0x0063b4
192.168.20.0    8.8.8.8         712         0x8000000a 0x00169f
192.168.30.0    8.8.8.8         712         0x8000000b 0x00a505
192.168.31.0    8.8.8.8         712         0x8000000c 0x009810
3.3.3.3         8.8.8.8         712         0x8000000d 0x001e05
192.168.3.0     8.8.8.8         712         0x8000000e 0x00d3ed
192.168.21.0    8.8.8.8         712         0x8000000f 0x0001ae
2.2.2.2         8.8.8.8         712         0x80000010 0x0046dd
192.168.2.0     8.8.8.8         712         0x80000011 0x00d8e6
192.168.10.0    8.8.8.8         712         0x80000012 0x007443
192.168.11.0    8.8.8.8         712         0x80000013 0x00674e
1.1.1.1         8.8.8.8         712         0x80000014 0x006cb7
192.168.1.0     8.8.8.8         712         0x80000015 0x00dbe0
Router#
Router#
Router#
```

Figure 5.3

“Show IP OSPF database”



```
Router#sh ip ospf data
Router#sh ip ospf database
            OSPF Router with ID (8.8.8.8) (Process ID 1)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
7.7.7.7         7.7.7.7         737         0x80000004 0x00c6c2 2
8.8.8.8         8.8.8.8         737         0x80000004 0x006afe 2
6.6.6.6         6.6.6.6         737         0x80000004 0x002386 2
5.5.5.5         5.5.5.5         737         0x80000004 0x007f4a 2
9.9.9.9         9.9.9.9         737         0x8000000a 0x00c078 5

                Net Link States (Area 0)
Link ID         ADV Router      Age         Seq#       Checksum
192.168.70.2    9.9.9.9         738         0x80000001 0x00c7f7
192.168.80.2    9.9.9.9         737         0x80000002 0x00d9e1
192.168.60.2    9.9.9.9         737         0x80000003 0x00046b
192.168.50.2    9.9.9.9         737         0x80000004 0x00dd09

                Summary Net Link States (Area 0)
Link ID         ADV Router      Age         Seq#       Checksum
192.168.40.0    8.8.8.8         722         0x80000001 0x003775
192.168.41.0    8.8.8.8         722         0x80000002 0x002a80
4.4.4.4         8.8.8.8         722         0x80000003 0x00ef3b
192.168.4.0     8.8.8.8         722         0x80000004 0x00c804
192.168.20.0    6.6.6.6         717         0x80000001 0x005078
192.168.30.0    7.7.7.7         717         0x80000001 0x00c3f6
192.168.31.0    7.7.7.7         717         0x80000002 0x00b602
3.3.3.3         7.7.7.7         717         0x80000003 0x003cf6
192.168.3.0     7.7.7.7         717         0x80000004 0x00f1df
192.168.21.0    6.6.6.6         717         0x80000002 0x004383
2.2.2.2         6.6.6.6         717         0x80000003 0x0088b2
192.168.2.0     6.6.6.6         717         0x80000004 0x001bbb
192.168.10.0    5.5.5.5         717         0x80000001 0x00dcf9
192.168.11.0    5.5.5.5         717         0x80000002 0x00cf05
1.1.1.1         5.5.5.5         717         0x80000003 0x00d46e
192.168.1.0     5.5.5.5         717         0x80000004 0x004497
```

Figure 5.4

In the above figure the OSPF database are shown

The OSPF database is essential for the OSPF routers to determine the best path to destination network. It allow routers to learn about the network topology, calculate the shortest path to destination network, and to adapt to changes in the network topology.

5.1 DR/BDR Selection: Designated Router and Backup Designated router selection is crucial for process in OSPF routing protocol.

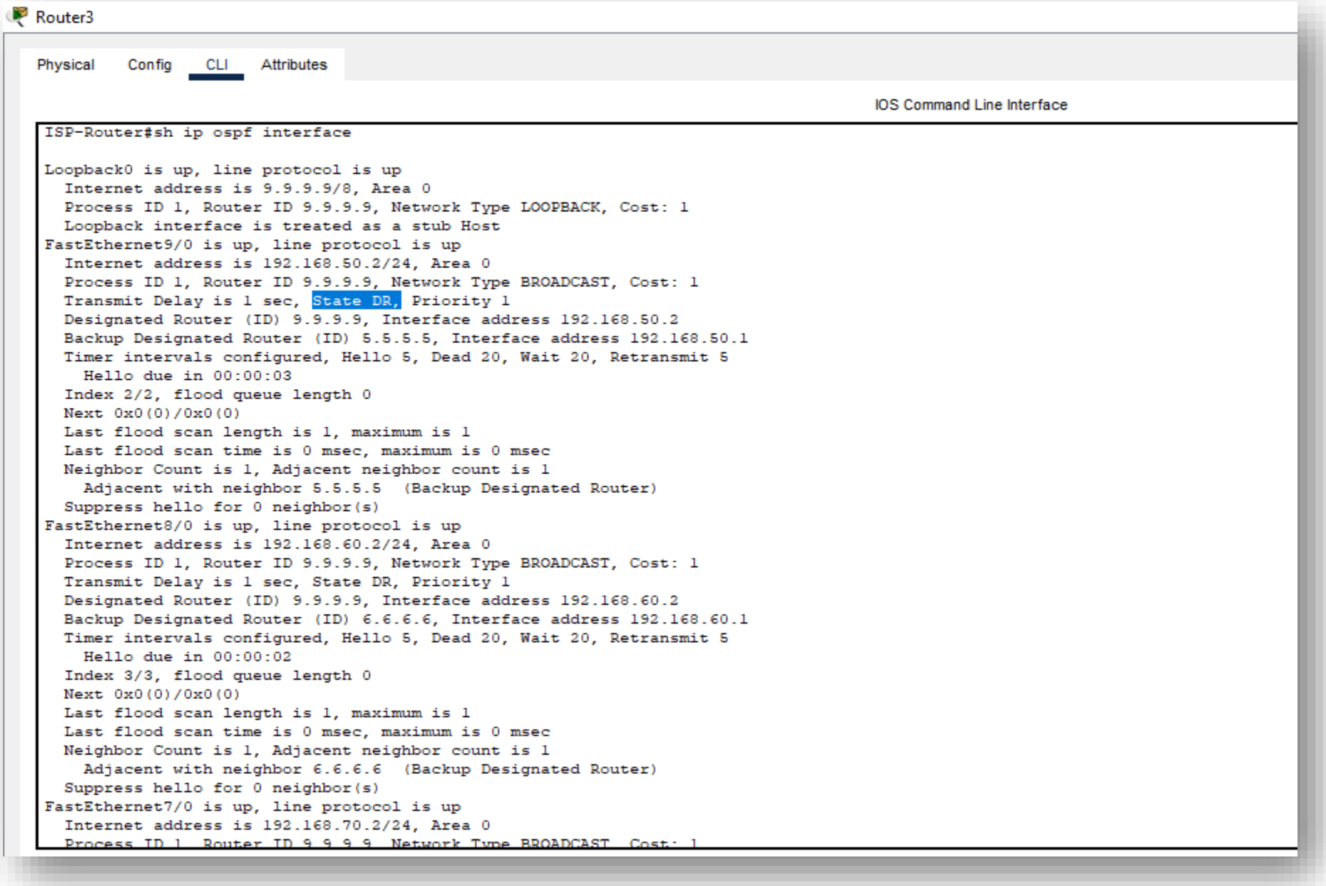
What is DR and BDR: DR router that is responsible for sending and receiving OSPF packets on broadcast or non-broadcast multicast network?

Backup Designated router that assume the role of the DR in the case of DR failure.

5.1.1 Selection Process:

1. Highest Router ID
2. Highest priority
3. First to send hello packets

Now to check the DR/BDR router go to router and type “show ip ospf interface” or ”show ip ospf neighbor”



```
ISP-Router#sh ip ospf interface

Loopback0 is up, line protocol is up
  Internet address is 9.9.9.9/8, Area 0
  Process ID 1, Router ID 9.9.9.9, Network Type LOOPBACK, Cost: 1
  Loopback interface is treated as a stub Host
FastEthernet9/0 is up, line protocol is up
  Internet address is 192.168.50.2/24, Area 0
  Process ID 1, Router ID 9.9.9.9, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 9.9.9.9, Interface address 192.168.50.2
  Backup Designated Router (ID) 5.5.5.5, Interface address 192.168.50.1
  Timer intervals configured, Hello 5, Dead 20, Wait 20, Retransmit 5
    Hello due in 00:00:03
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 5.5.5.5  (Backup Designated Router)
  Suppress hello for 0 neighbor(s)
FastEthernet8/0 is up, line protocol is up
  Internet address is 192.168.60.2/24, Area 0
  Process ID 1, Router ID 9.9.9.9, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 9.9.9.9, Interface address 192.168.60.2
  Backup Designated Router (ID) 6.6.6.6, Interface address 192.168.60.1
  Timer intervals configured, Hello 5, Dead 20, Wait 20, Retransmit 5
    Hello due in 00:00:02
  Index 3/3, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 6.6.6.6  (Backup Designated Router)
  Suppress hello for 0 neighbor(s)
FastEthernet7/0 is up, line protocol is up
  Internet address is 192.168.70.2/24, Area 0
  Process ID 1, Router ID 9.9.9.9, Network Type BROADCAST, Cost: 1
```

Figure 5.5

In the above figure the ISP-Router state is DR router and the rest of the routers are act as BDR.

CHAPTER-VI

SWITCHING

6.1. INTRODUCTION: Switching in networking refers to the process of forwarding data packets between devices on a computer network. A network switch is a device that connects multiple devices, such as computers, servers, and printers, within a local area network (LAN). It receives incoming data packets and directs them to the intended destination device, ensuring efficient and secure communication.

Switching occurs at the Data Link layer of the OSI model, where the switch examines the packet's MAC address to determine the destination device. This process enables:

- Efficient data transfer
- Reduced network congestion
- Improved network reliability
- Enhanced security features, such as VLANs and port authentication

In essence, switching facilitates the seamless exchange of data within a network, making it a critical component of modern networking infrastructure.

6.2. Assigning IP Addresses: Assigning IP Addresses:

- ➢ IP addresses are unique identifiers for devices on a network.
- ➢ IP addresses consist of four numbers (octets) separated by dots (e.g., 192.168.1.1).

There are two main types of IP addresses:

- ➢ Static IP addresses (manually configured)
- ➢ Dynamic IP addresses (assigned by a DHCP server)

IP addresses are assigned using the following methods:

- ➢ Manual configuration (static IP)
- ➢ DHCP (Dynamic Host Configuration Protocol)
- ➢ Automatic Private IP Addressing (APIPA)

Key considerations when assigning IP addresses:

- ➢ Ensure unique addresses for each device
- ➢ Use appropriate subnet masks and gateways
- ➢ Configure IP addresses correctly for network communication
- ➢ Manage IP address allocation using DHCP or other tools

Some common IP address assignment methods include:

- Static IP address assignment for servers and critical devices
- DHCP for dynamic address allocation
- APIPA for automatic address assignment in small networks

6.3 DEFINE VLANS FOR EACH NETWORK: Virtual Local Area Networks (VLANs) are logical groupings of devices within a network, segregated to improve security, organization, and network management. VLANs create separate broadcast domains, allowing devices to communicate only with others in the same VLAN.

Campus Network, VLANs segment different departments or buildings, enhancing security and reducing network congestion.

Enterprise Network, VLANs separate various divisions or teams, improving organization and resource allocation.

Data Center Network, VLANs isolate different applications or services, ensuring efficient traffic management and security.

Industrial Network, VLANs segregate different production lines or areas, enhancing security and reducing network interference.

Home Network, VLANs separate different devices or areas, improving organization and security.

VLANs provide numerous benefits, including:

- Improved security through segregation
- Enhanced network organization and management
- Reduced network congestion and interference
- Increased scalability and flexibility
- Control broadcast

By configuring VLANs, networks can optimize performance, security, and management, creating a more efficient and organized network infrastructure.

6.4. ENABLE SSH ON ROUTERS FOR SECURE REMOTE ACCESS:

Enabling SSH (Secure Shell) on routers provides a secure way to manage and access the device. Here's a step-by-step guide to enable SSH on routers:

Cisco Routers:

1. Enter the configuration mode: configure terminal
2. Enable SSH: crypto key generate rsa (generate an RSA key)
3. Specify the key size: crypto key generate rsa general-keys modulus <size> (e.g., 2048)

4. Enable SSH on the vty lines: line vty 0 4 and transport input ssh

5. Set the SSH password: password <password> and login

6. Exit the configuration mode: end

General Tips:

Ensure you have the necessary permissions and credentials to enable SSH.

Use a strong password and consider using public-key authentication for added security.

Regularly update your router's firmware to ensure the latest security patches.

By enabling SSH, you can securely access and manage your router, reducing the risk of unauthorized access and improving network security.

6.4. STP AND STP PORTFAST BENIFITES

6.4.1 STP Benefits:

1. Prevents Network Loops: STP eliminates network loops, ensuring data transmission is efficient and preventing broadcast storms.

2. Improves Network Reliability: STP prevents network failures by detecting and blocking redundant links, ensuring high availability.

3. Enhances Network Security: STP reduces the risk of unauthorized access by limiting network exposure.

4. Simplifies Network Management: STP streamlines network management by automatically configuring and managing network topology.

6.4.2 Port Fast Benefits:

1. Faster Network Convergence: Port Fast enables faster network convergence, reducing downtime and improving network responsiveness.

2. Improved Network Performance: Port Fast optimizes network performance by minimizing STP convergence delays.

3. Enhanced Network Resilience: Port Fast ensures rapid recovery from network failures, ensuring high network uptime.

4. Simplified Network Configuration: Port Fast simplifies network configuration by eliminating the need for manual STP configuration.

By leveraging STP and Port Fast, networks can improve reliability, security, and performance, ensuring efficient and uninterrupted data transmission

6. Ether channels: Ether Channel: A Network Optimization Technique

Ether Channel is innovative technology that consolidates multiple physical Ethernet links into a single, high-capacity logical link. This advanced feature enables network administrators to boost network performance, ensure redundancy, and simplify network configuration.

6.5 Key Benefits of ether Channel

1. Bandwidth Multiplication: ether Channel aggregates the bandwidth of multiple physical links, amplifying network throughput and supporting high-traffic applications.
2. Redundancy and Fault Tolerance: EtherChannel ensures uninterrupted network connectivity by automatically redirecting traffic to available links in case of a failure.
3. Intelligent Load Balancing: EtherChannel distributes network traffic efficiently across multiple links, preventing congestion and optimizing network resource utilization.
4. Streamlined Network Management: EtherChannel simplifies network configuration and management by presenting a single, logical link to the network.
5. Cost-Effective Scalability: EtherChannel enables network expansion and upgrade without requiring new hardware, making it a cost-effective solution for growing networks.

By leveraging EtherChannel, networks can achieve improved performance, reliability, and scalability, making it an essential technology for modern network infrastructure.

CHAPTER-VII

WLAN (Wireless Local Area Network)

7.1 INTRODUCTION: A wireless Local Area Network is a computer network that connect Computers and other networking devices wirelessly, without the use of cables. It use radio waves to transmit data between devices, allowing for greater mobility and flexibility. In wireless network devices connect to the network using wireless adapters or interfaces, the network cover the limited geographical area such as home office building or campus. Wi-Fi, AP (Access points), WLC (Wireless LAN Controller) are

The most commonly used wireless networking devices based on IEEE 802.11 standard. Using WLAN we can share files, internet access, printing, smart home devices, and it provide benefits like mobility, flexibility, cost effective and easy to install and manage.

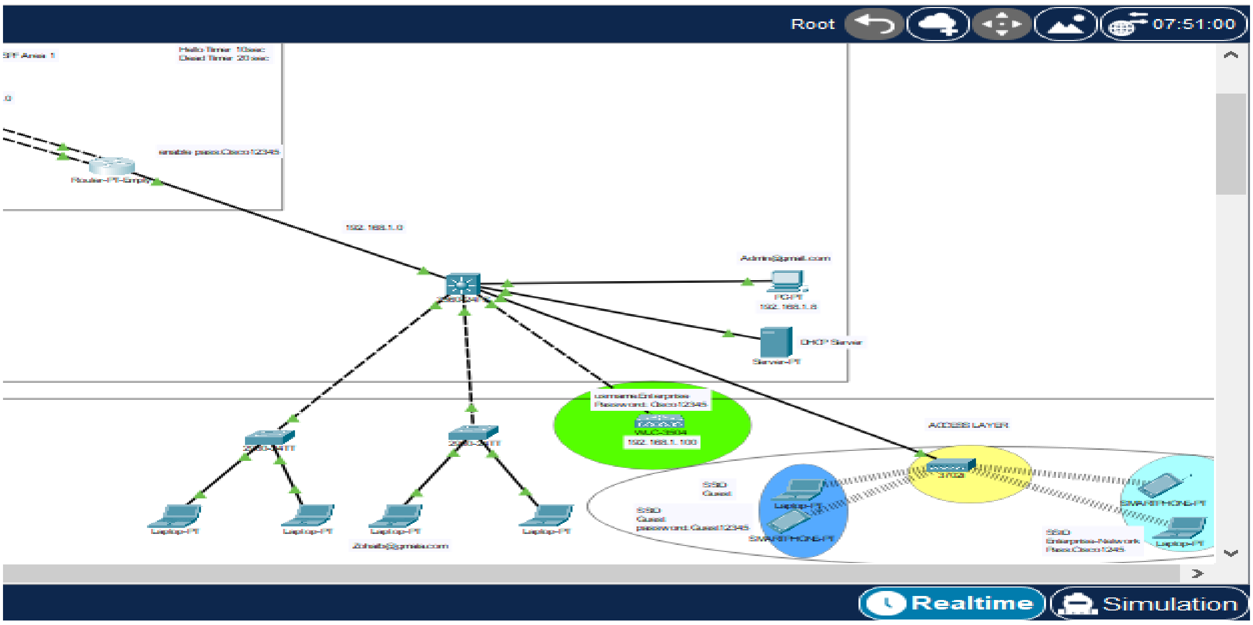


Figure 7.1

The above figure the network contain wireless network that connect devices through Aps and can be control using the WLC.

7.2 WLAN Designing: A wireless network play a crucial role in enterprise networking. To design a wireless network we need to follow some guidance for the design.

1. Site Survey: Assess the environment and identify the potential sources of interferences. Determine the number of users and devices, and define coverage area and boundaries.

2. Network Requirements: Determine the required network speed and capacity. Identify the type and application that will be used.
3. WLAN Architecture: Choose an appropriate WLAN architecture and select the number and type of APs and define the wireless network topology.
4. Access Points Placement: Determine the optimal AP placement based on the site survey and network equipment's, consider factors such as signal strength, coverage and interference.
5. Security and Authentication: Define the security policy and protocols (WPA2, WPA3. 802.1x). Configure the authentication and authorization mechanism.

7.3 WLC and AP Selection: When building a wireless network, choosing the right Wireless LAN Controller (WLC) and Access Points (APs) is crucial. The WLC is the brain of the network, managing and controlling the APs, while the APs provide the connectivity for your devices.

Key factors to consider when selecting a WLC:

- ➢ Network size and scalability
- ➢ Security features and protocols
- ➢ Network management and monitoring capabilities
- ➢ Compatibility with existing infrastructure

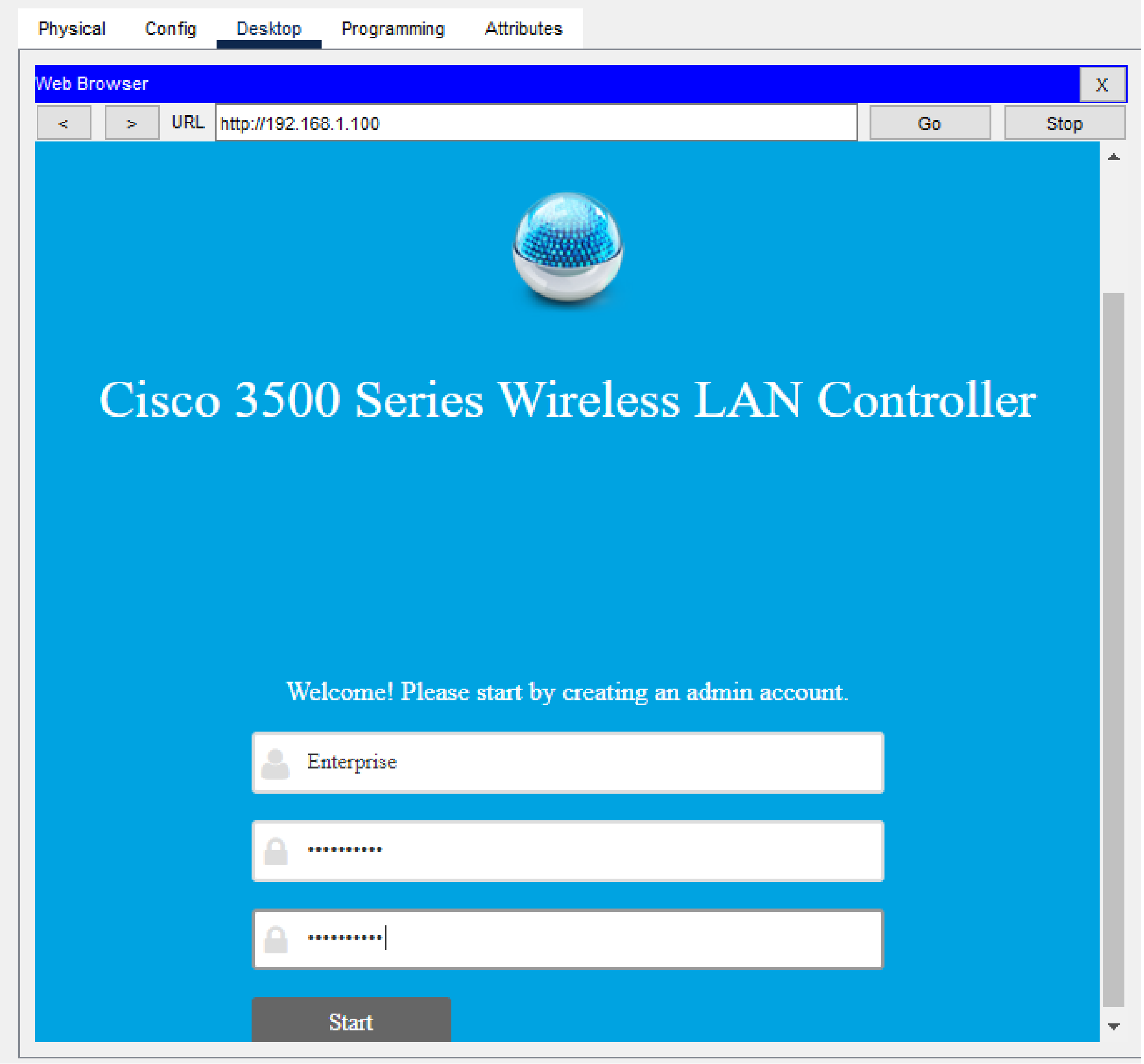
Key factors to consider when selecting APs:

- ➢ Coverage area and range
- ➢ Number of concurrent users and devices
- ➢ Radio frequency (RF) capabilities and antenna type
- ➢ Power over Ethernet (PoE) support

Now setting up the WLC: The first step to setup the WLC we can go to the any PC and open a webpage. Then enter the ip add of the WLC with HTTP method then we will get the following interface.

The first step we need to set the username and password for the WLC.

So the username is “Enterprise” and the password is “Cisco12345”



http://192.168.1.100

Cisco 3500 Series Wireless LAN Controller

Welcome! Please start by creating an admin account.

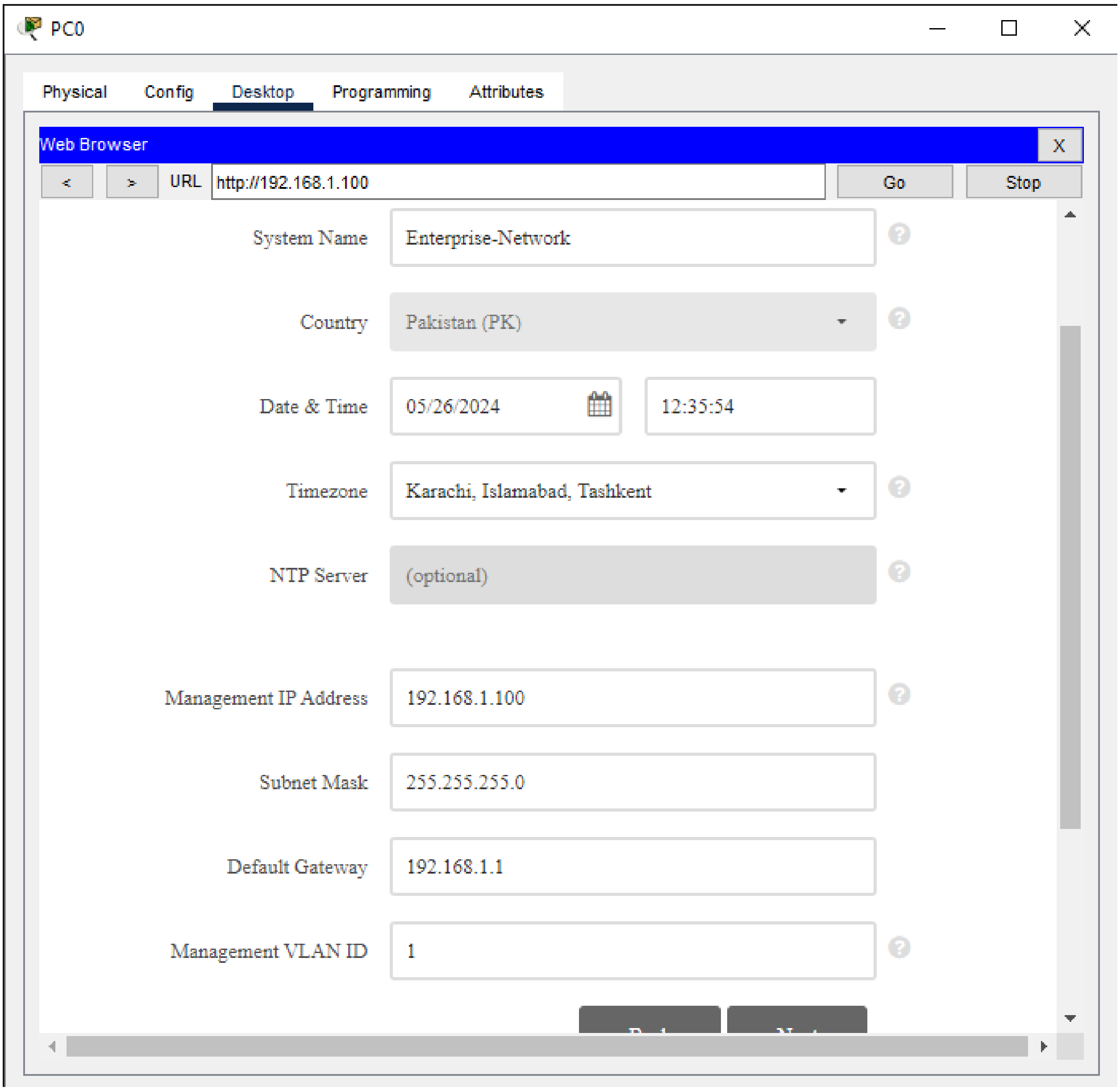
Enterprise

••••••••••

••••••••••

Figure 7.2

The second step we have the following interface.



URL http://192.168.1.100

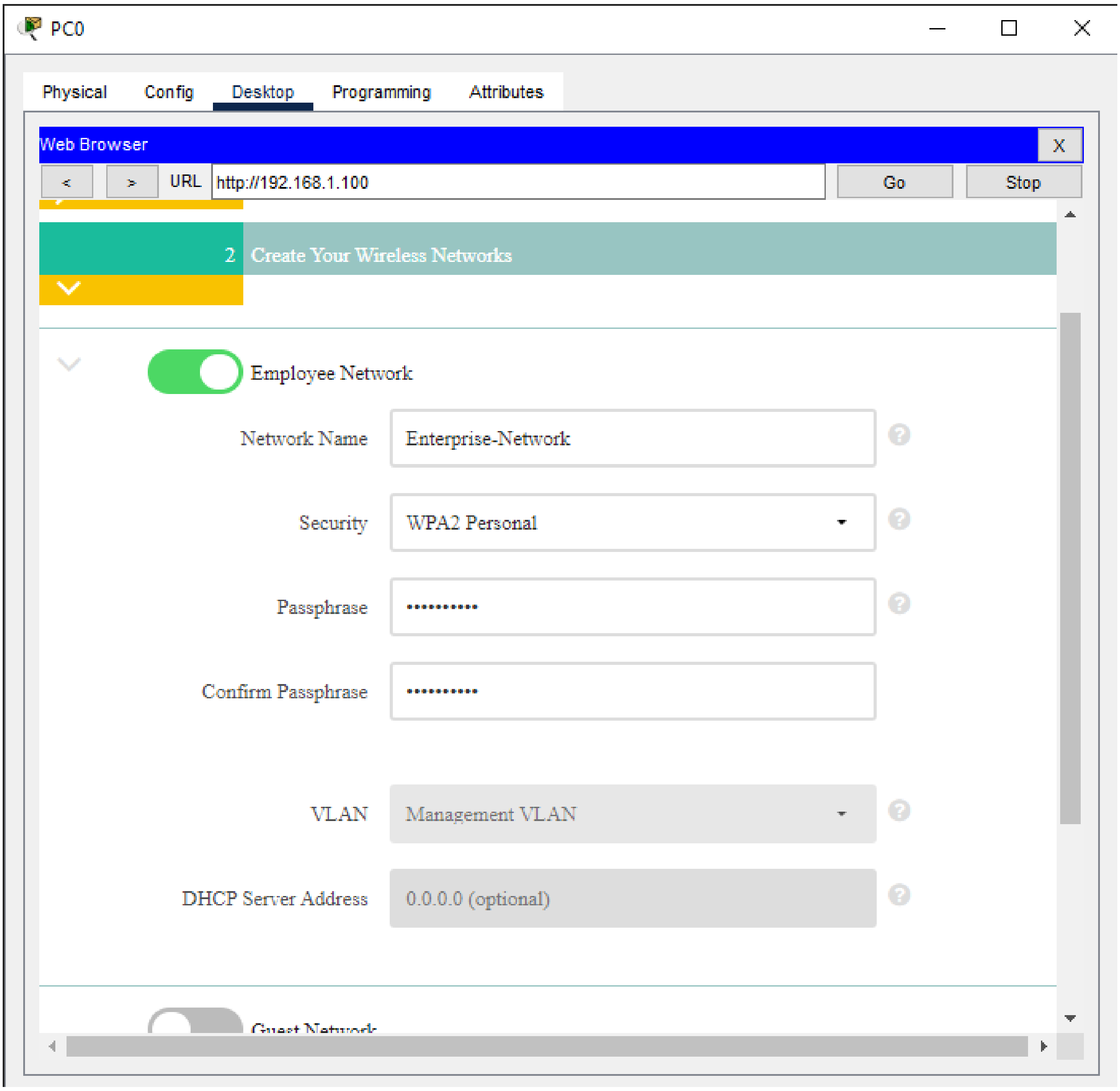
System Name	Enterprise-Network	
Country	Pakistan (PK)	
Date & Time	05/26/2024	12:35:54
Timezone	Karachi, Islamabad, Tashkent	
NTP Server	(optional)	
Management IP Address	192.168.1.100	
Subnet Mask	255.255.255.0	
Default Gateway	192.168.1.1	
Management VLAN ID	1	

Figure7.3

Here we can setup the basic setting like data & time, Time zone, Management IP address, subnet mask and default gateway.

Third option we have the following interface.

In this phase we need to set the SSIDs and security for each SSID like WPA2 personal security and password then next we have:



http://192.168.1.100

2 Create Your Wireless Networks

Employee Network

Network Name: Enterprise-Network

Security: WPA2 Personal

Passphrase: ••••••••••

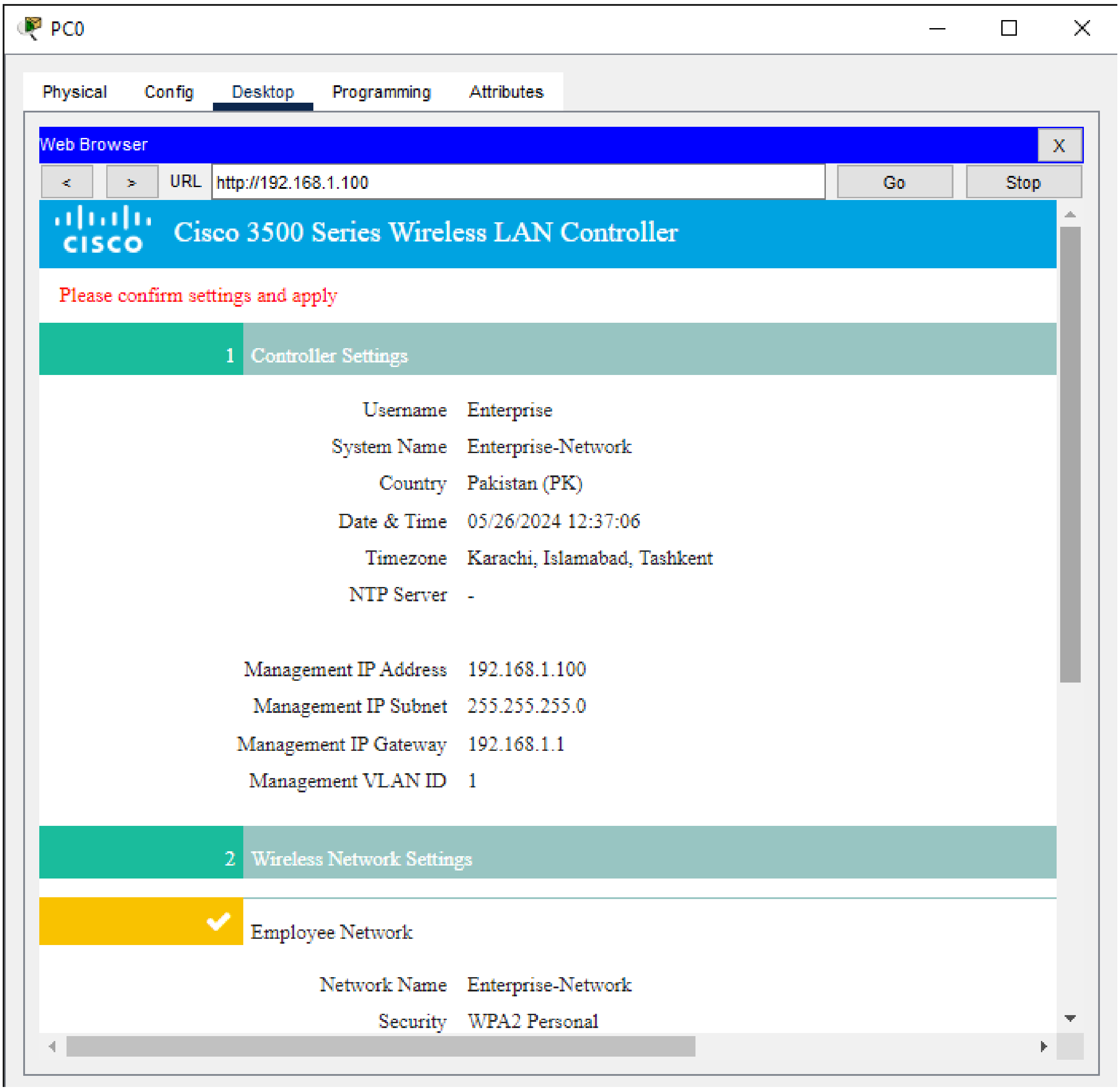
Confirm Passphrase: ••••••••••

VLAN: Management VLAN

DHCP Server Address: 0.0.0.0 (optional)

Guest Network

Figure 7.4



http://192.168.1.100

Cisco 3500 Series Wireless LAN Controller

Please confirm settings and apply

1 Controller Settings

Username	Enterprise
System Name	Enterprise-Network
Country	Pakistan (PK)
Date & Time	05/26/2024 12:37:06
Timezone	Karachi, Islamabad, Tashkent
NTP Server	-
Management IP Address	192.168.1.100
Management IP Subnet	255.255.255.0
Management IP Gateway	192.168.1.1
Management VLAN ID	1

2 Wireless Network Settings

✓ Employee Network

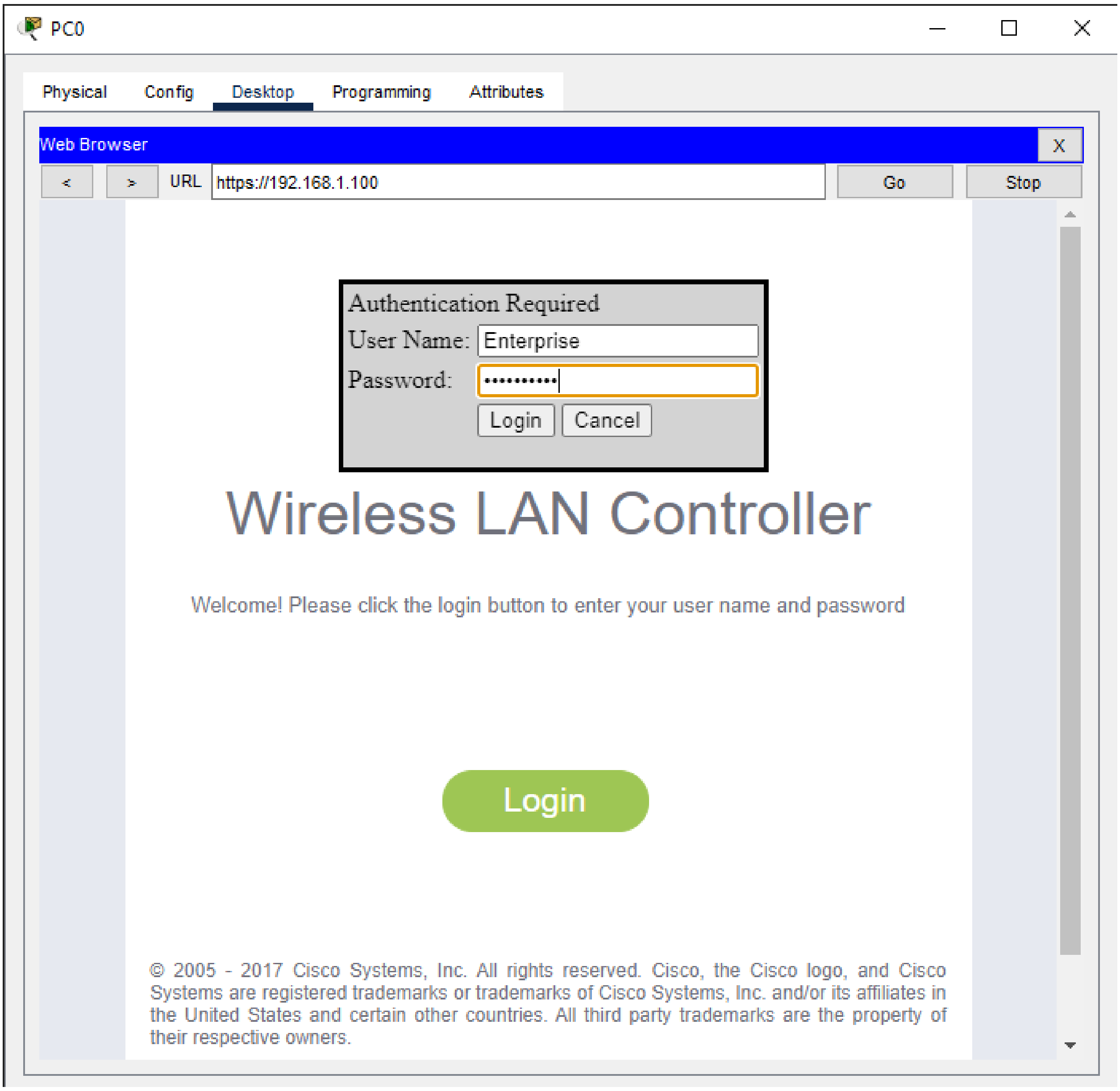
Network Name	Enterprise-Network
Security	WPA2 Personal

Figure 7.5

Now we have the confirmation setting and apply to save changes.

This is the initial setting for the WLC now it’s time to get the access to the WLC graphical interface with the help of HTTPS by entering the IP address of the WLC into web browser.

Now here by entering the username and password we will get the graphical interface of WLC.



URL https://192.168.1.100

Authentication Required

User Name: Enterprise

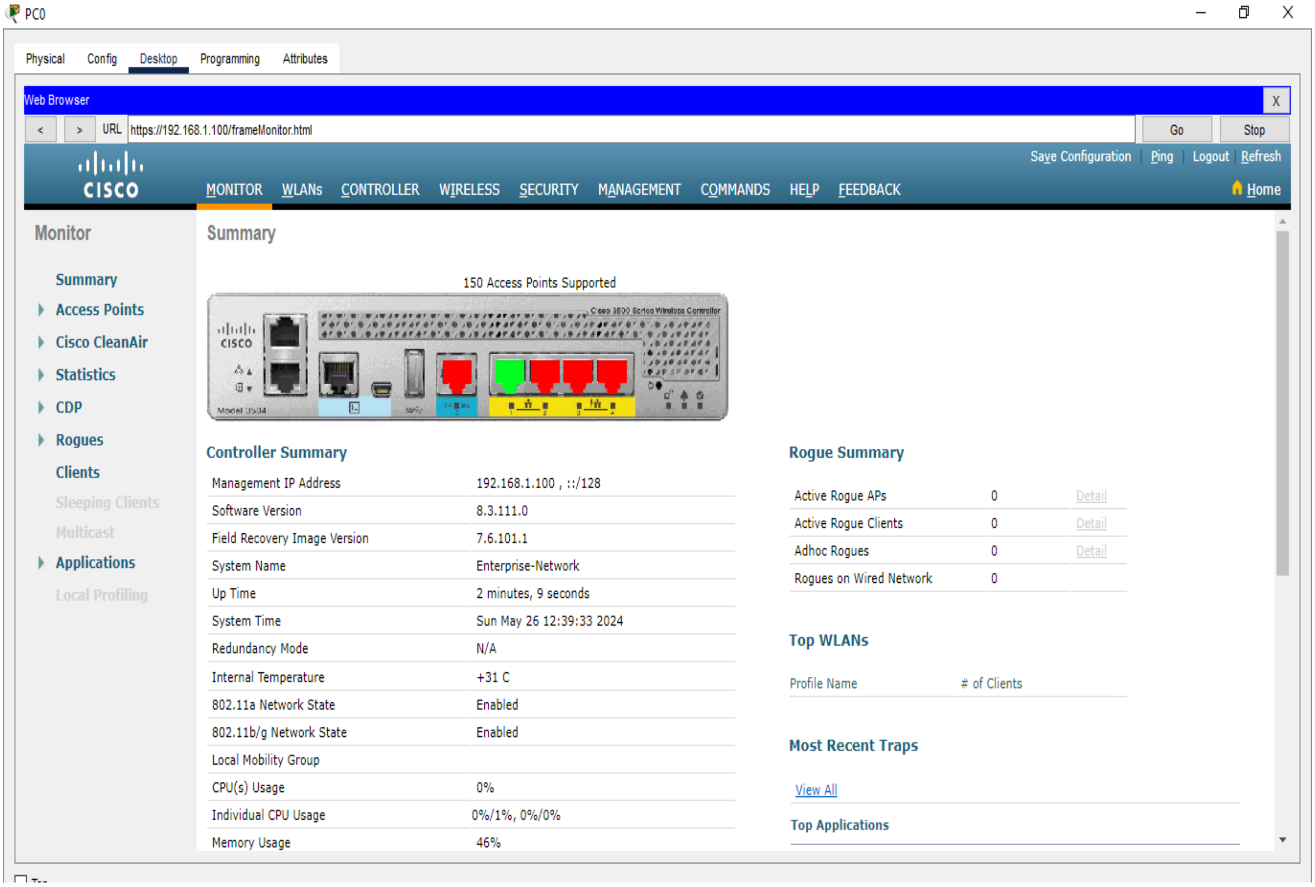
Password: ••••••••••

Wireless LAN Controller

Welcome! Please click the login button to enter your user name and password

© 2005 - 2017 Cisco Systems, Inc. All rights reserved. Cisco, the Cisco logo, and Cisco Systems are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. All third party trademarks are the property of their respective owners.

Figure 7.6



URL: https://192.168.1.100/frameMonitor.html

Summary

Controller Summary

Management IP Address	192.168.1.100 , ::/128
Software Version	8.3.111.0
Field Recovery Image Version	7.6.101.1
System Name	Enterprise-Network
Up Time	2 minutes, 9 seconds
System Time	Sun May 26 12:39:33 2024
Redundancy Mode	N/A
Internal Temperature	+31 C
802.11a Network State	Enabled
802.11b/g Network State	Enabled
Local Mobility Group	
CPU(s) Usage	0%
Individual CPU Usage	0%/1%, 0%/0%
Memory Usage	46%

Rogue Summary

Active Rogue APs	0	Detail
Active Rogue Clients	0	Detail
Adhoc Rogues	0	Detail
Rogues on Wired Network	0	

Top WLANs

Profile Name	# of Clients

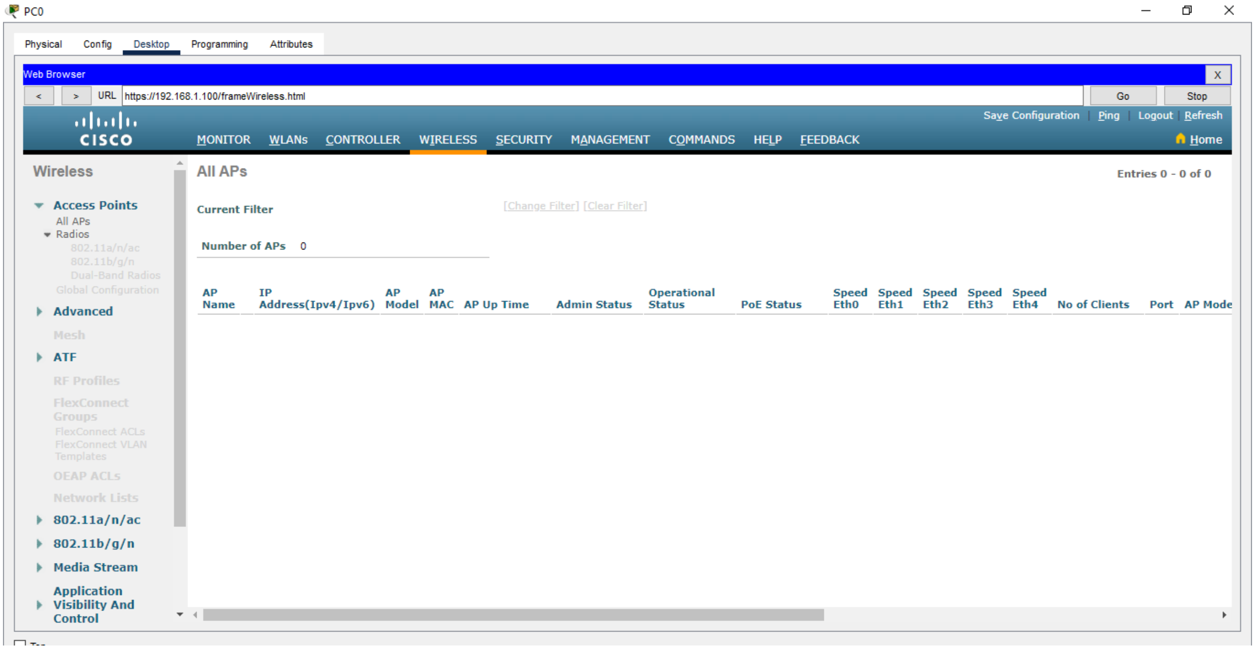
Most Recent Traps

View All

Top Applications

Figure 7.7

Now the interface is here. Here is the basic information and a lot of options are available here but in Packet tracer we have limitation we can only create the SSIDs, adding the AP and enabling some security features.



URL: https://192.168.1.100/frameWireless.html

All APs

Entries 0 - 0 of 0

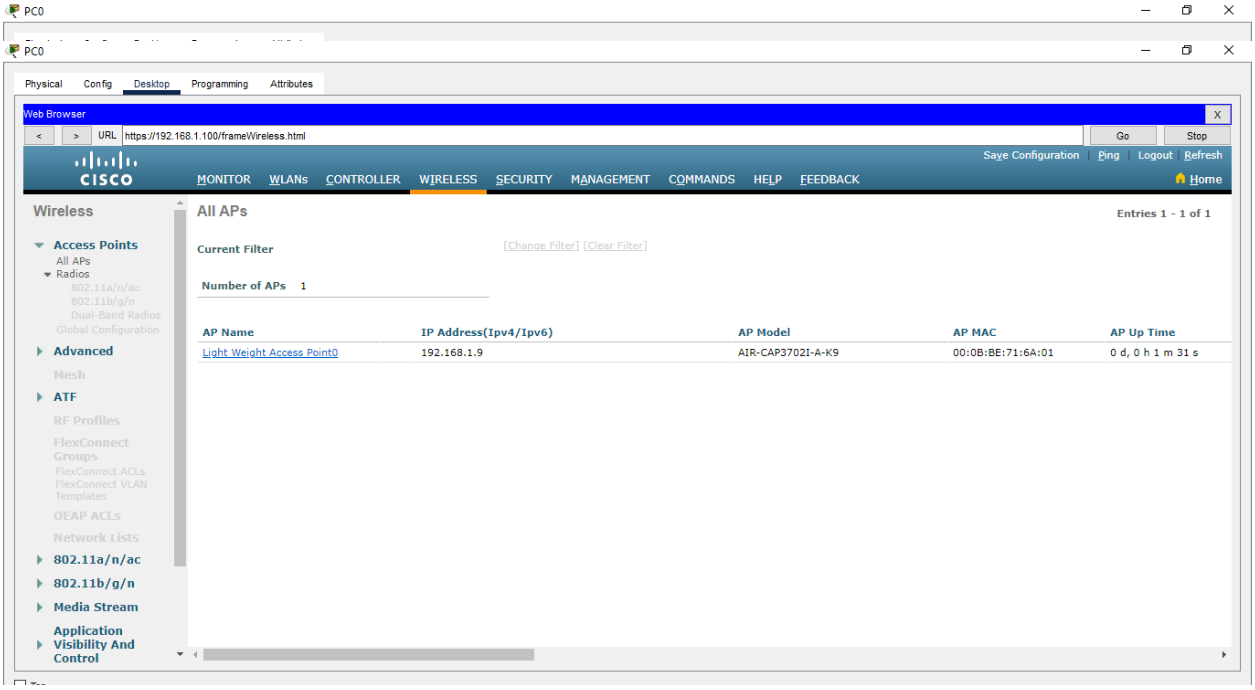
Current Filter [Change Filter] [Clear Filter]

Number of APs 0

AP Name	IP Address(Ipv4/Ipv6)	AP Model	AP MAC	AP Up Time	Admin Status	Operational Status	PoE Status	Speed Eth0	Speed Eth1	Speed Eth2	Speed Eth3	Speed Eth4	No of Clients	Port	AP Mode

Figure 7.8

So now we install the AP and we can see it here. AP name and IP address AP model and MAC address and lot of information about AP are here.



All APs

Entries 1 - 1 of 1

Current Filter

Number of APs 1

AP Name	IP Address(Ipv4/Ipv6)	AP Model	AP MAC	AP Up Time
Light Weight Access Point0	192.168.1.9	AIR-CAP3702I-A-K9	00:0B:BE:71:6A:01	0 d, 0 h 1 m 31 s

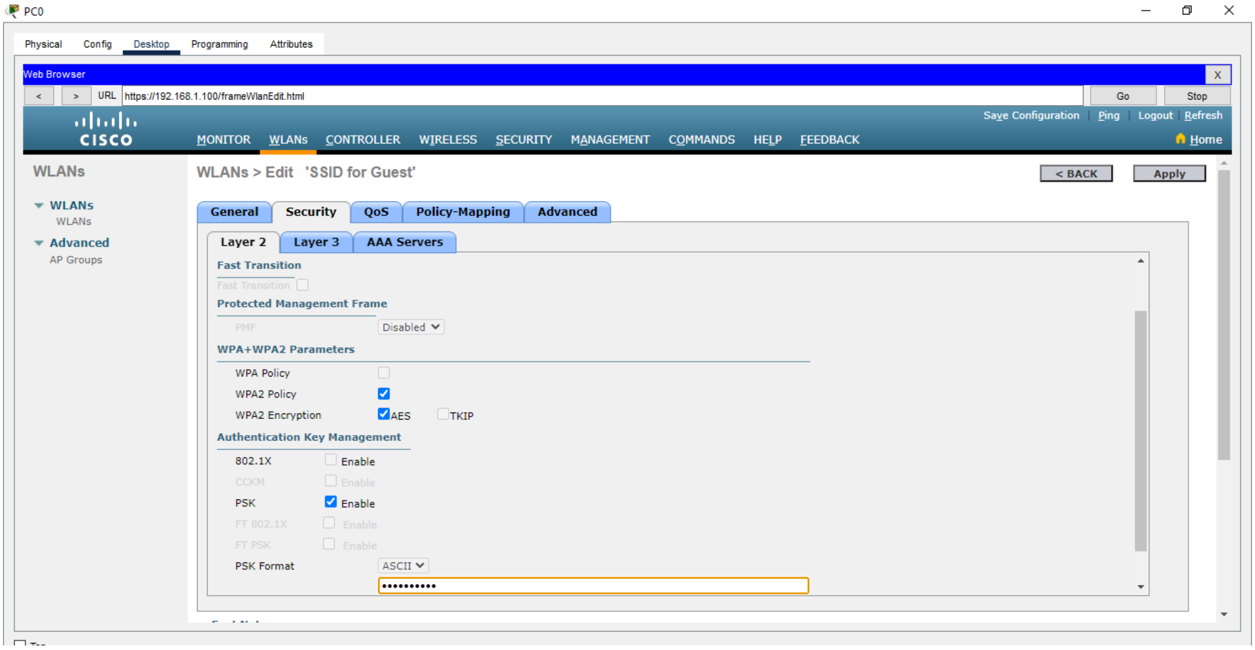
Figure 7.9

This is the place where we can create SSIDs.

7.4 Creating SSID:

Now if we want to create SSID we can go to the WLAN portion and select the Profile name and SSID and enter the apply button. So our SSID will be create.

Now in advance setting we can setup the Password and security type form here and click apply.



URL https://192.168.1.100/frameWlanEdit.html

WLANs > Edit 'SSID for Guest'

Fast Transition

Fast Transition □

Protected Management Frame

PMF Disabled

WPA+WPA2 Parameters

WPA Policy □

WPA2 Policy ☑

WPA2 Encryption ☑AES □TKIP

Authentication Key Management

802.1X □ Enable

CCKM □ Enable

PSK ☑ Enable

FT 802.1X □ Enable

FT PSK □ Enable

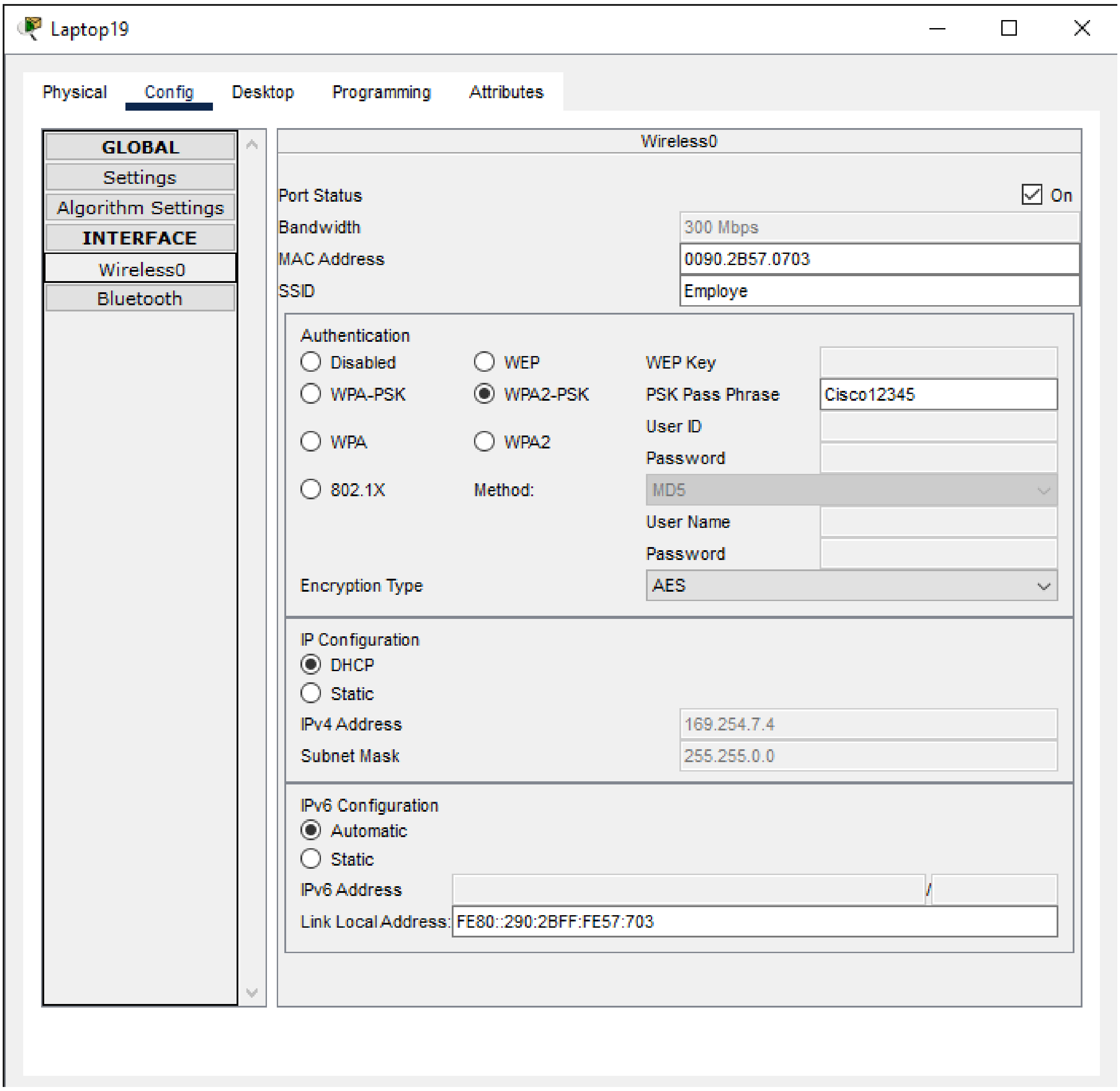
PSK Format ASCII

••••••••••

Figure 7.10

Now it’s time that how we can connect our mobile phone and Laptops to the Wireless network? So first of all go to laptop and open the configuration setting and go to wireless setting.

Here enter the SSID name in the 2nd portion and select the Security method and type the password and hit enter and after a while it will connect to the AP.



Laptop19

Wireless0

Port Status ☑ On
Bandwidth 300 Mbps
MAC Address 0090.2B57.0703
SSID Employe

Authentication
○ Disabled ○ WEP WEP Key
○ WPA-PSK ● WPA2-PSK PSK Pass Phrase Cisco12345
User ID
○ WPA ○ WPA2 Password
○ 802.1X Method: MD5
User Name
Password
Encryption Type AES

IP Configuration
● DHCP
○ Static
IPv4 Address 169.254.7.4
Subnet Mask 255.255.0.0

IPv6 Configuration
● Automatic
○ Static
IPv6 Address /
Link Local Address: FE80::290:2BFF:FE57:703

Figure 7.11

And here we successfully see that the mobiles and PCs are connected to the AP.

7.5 Creating DHCP pool: By creating the DHCP pool on the switch every device can get ip address form that pool and also we have excluded addresses as well that we reserve for the wired network.

```
Ip dhcp excluded-address 192.168.1.1 192.168.1.100
!
Ip dhcp pool Wireless
Network 192.168.1.0 255.255.255.0
Default-router 192.168.1.1
Option 150 ip 192.168.1.100
```

CHAPTER-VIII

DATA CENTER

8.1 Introduction to Data Center in an Enterprise Networks: The Heart of Enterprise Networks In the digital age, data has become the lifeblood of modern enterprises. As the volume, velocity, and variety of data continue to grow, organizations require a robust and reliable infrastructure to store, process, and manage their data. This is where data centers come into play.

A data center is a purpose-built facility or a dedicated space within an enterprise that houses computer systems, storage systems, networking equipment, and other IT infrastructure. It serves as the central hub for data processing, storage, and distribution, connecting users, applications, and services across the enterprise.

Data centers play a critical role in supporting business operations, enabling:

- ➢ Data storage and management
- ➢ Application hosting and virtualization
- ➢ Network services and connectivity
- ➢ IT service continuity and disaster recovery
- ➢ Business intelligence and analytics

In essence, data centers are the heart of enterprise networks, powering the digital transformation of businesses and driving innovation, growth, and success.

8.2 DNS, DHCP, NTP, Syslog, Email, DNS and Web server:

8.2.1 DNS Server:

The Domain Name System (DNS) Server: A Cornerstone of the Internet

The internet relies on a complex system to translate human-readable domain names into machine-readable IP addresses, enabling us to access websites, communicate via email, and connect with online services. At the heart of this system lies the Domain Name System (DNS) server.

A DNS server is a critical component of the internet infrastructure, serving as a lookup service that translates domain names into IP addresses. This process, known as DNS resolution, allows devices to communicate with each other and access online resources.

Think of a DNS server as a digital phonebook, where:

- Domain names (e.g., (link unavailable)) are like names in the phonebook

- IP addresses (e.g., 192.0.2.1) are like phone numbers

When you enter a URL or send an email, your device queries a DNS server to resolve the domain name to an IP address, enabling the connection to take place.

In essence, DNS servers are vital for the smooth functioning of the internet, making them a fundamental building block of modern communication and information exchange.

8.2.2 DHCP Server: DHCP Servers in Enterprise Networks: Efficient IP Address Management.

In enterprise networks, managing IP addresses is a crucial task. Dynamic Host Configuration Protocol (DHCP) servers play a vital role in assigning and managing IP addresses, ensuring that devices can communicate with each other and access network resources.

A DHCP server is a network component that:

- Assigns IP addresses and subnet masks to devices
- Provides additional network settings, such as default gateways and DNS server addresses
- Supports dynamic allocation and reallocation of IP addresses
- Enables efficient management of IP address pools

In an enterprise network, DHCP servers offer several benefits, including:

- - Centralized management of IP addresses
- - Automated IP address assignment
- - Reduced IP address conflicts
- - Scalability and flexibility
- - Improved network reliability and performance

By implementing DHCP servers, enterprises can streamline their IP address management, reduce administrative burdens, and ensure a robust and reliable network infrastructure. In our network the Karachi branch contain the DHCP server that allocate the dynamic IP addresses across the network.

8.2.3 NTP (Network Timing Protocol):

A Network Time Protocol (NTP) server is a computer or device that provides a reliable source of time information, ensuring that computer clocks remain accurate and synchronized. NTP servers use the Network Time Protocol to distribute time signals, enabling devices to adjust their clocks to a reference time.

Key Functions of NTP Servers:

- Time Synchronization: NTP servers provide a precise time reference, allowing devices to synchronize their clocks.
- Time Accuracy: NTP servers ensure that devices maintain accurate time, essential for many applications, such as financial transactions and scientific research.
- Clock Synchronization: NTP servers enable devices to adjust their clocks to a reference time, ensuring that all devices on a network have the same time.

8.2.4 Syslog Server:

A syslog server, also known as a syslog collector or syslog receiver, is a device or software that collects and stores log messages from various network devices, such as routers, switches, firewalls, and servers. Syslog servers provide a centralized platform for monitoring, analyzing, and storing log data, enabling network administrators to:

- Monitor network device logs in real-time
- Identify security threats and system errors
- Conduct network forensics and incident response
- Comply with regulatory requirements

Key Features of Syslog Servers:

- Log collection and aggregation
- Log filtering and sorting
- Log analysis and alerting
- Log storage and archiving

8.2.5 WEB Server:

A web server is a software application or hardware device that hosts and serves websites, web applications, and web services over the internet or an intranet. Web servers use protocols like HTTP (Hypertext Transfer Protocol) or HTTPS (Hypertext Transfer Protocol Secure) to communicate with clients, such as web browsers or mobile apps.

Key Functions of Web Servers:

- Host and serve web pages, images, videos, and other content
- Handle HTTP requests and responses
- Support scripting languages like PHP, Python, or Ruby
- Manage SSL/TLS certificates for secure connections
- Configure access controls and authentication

In our network the web server are contain the information about our network and each branch and everyone can access form any branch of the network and know about the function of our network.

This web server contain a small website that contain the information about the data center, Karachi branch, Lahor branch and Islamabad branch.

8.2.6 Email Server:

An email server, also known as a mail server or mail transfer agent (MTA), is a software application or hardware device that manages and distributes email messages between senders and recipients. Email servers use protocols like SMTP (Simple Mail Transfer Protocol), POP (Post Office Protocol), and IMAP (Internet Message Access Protocol) to handle email communication.

Key Functions of Email Servers:

- Receive and forward email messages
- Manage email accounts and authentication
- Support email protocols and encryption
- Filter spam and malware
- Store and retrieve email messages

In our network each branch contain the users and for each user there is username and email id so using that they can send mail to each branch of our network.

8.3 Creating User Email and names for Each Branch: Creating user email is essential for communication. Here are some essential step while creating an email account.

1. Create an Email Account:

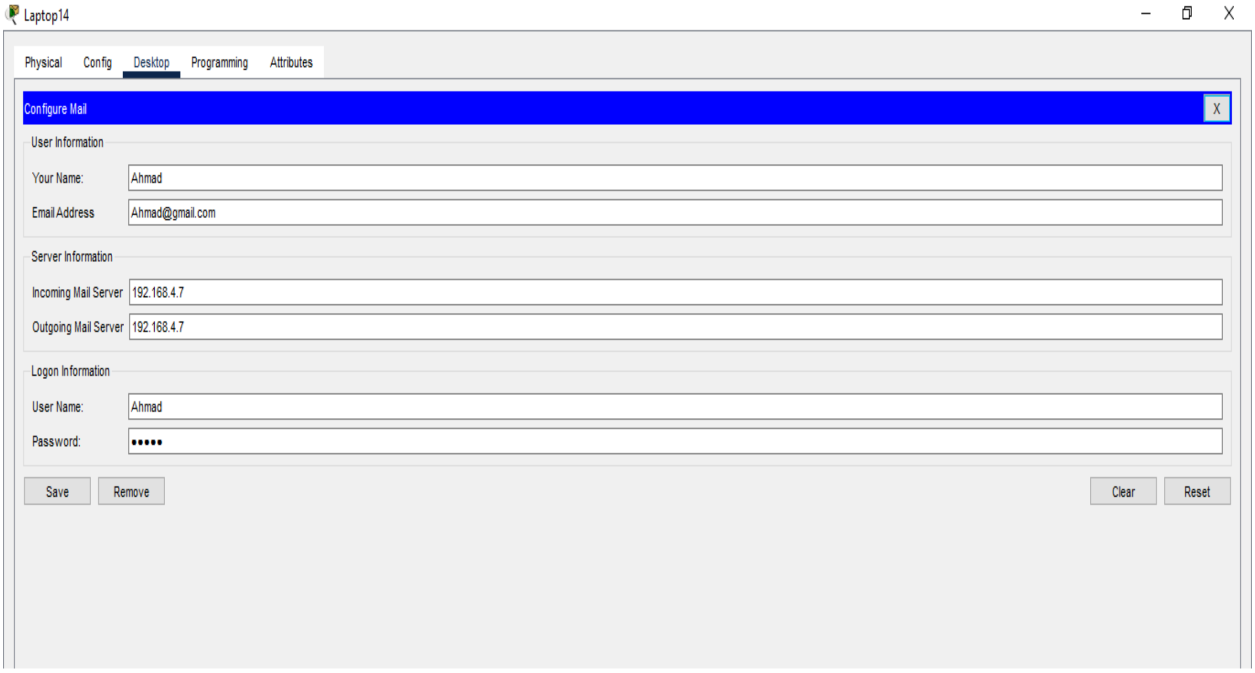
- According to a Cisco Community post, you need NetAcad credentials to use Packet Tracer as a user. You can create an email account or use your existing email address for this purpose.

2. Configure Email Client:

- Once you have the email account, go to the Desktop tab of the PC in Packet Tracer and click on Email. Then, configure the email client by filling in the user, server, and login information. Be sure to save the settings after configuration.

3. Domain Setup for Email Server:

- If you need to set a domain for the email server, navigate to Services>Email in Packet Tracer. There, you will find the option to set the domain name of the email server.



User Information

Your Name: Ahmad

Email Address Ahmad@gmail.com

Server Information

Incoming Mail Server 192.168.4.7

Outgoing Mail Server 192.168.4.7

Logon Information

User Name: Ahmad

Password: •••••

Figure 8.1

In the above figure the Email account has been created for the user “Ahmad”

8.4 conclusion: the effective management and integration of DNS, DHCP, Syslog, NTP, and Email servers are pivotal to the operational efficiency and reliability of a data center. Each of these components plays a crucial role in ensuring seamless network communication, accurate time synchronization, systematic log management, and robust email communication.

DNS (Domain Name System) facilitates the translation of human-readable domain names into machine-understandable IP addresses, making it indispensable for navigating the internet and internal networks. Effective DNS management ensures that services are reachable and performance is optimized.

DHCP (Dynamic Host Configuration Protocol) automates the assignment of IP addresses and network configuration parameters, reducing administrative overhead and minimizing configuration errors. A well-configured DHCP system ensures devices on the network receive the correct settings swiftly and efficiently.

Syslog serves as a centralized logging solution, collecting and storing log messages from various network devices and servers. This centralized approach to log management enhances troubleshooting capabilities, system monitoring, and security auditing, providing a comprehensive view of the network’s operational status.

NTP (Network Time Protocol) is essential for synchronizing the clocks of servers and devices within the data center. Accurate timekeeping is critical for various network operations, including log timestamping and time-sensitive applications, ensuring consistency and reliability across the network.

Email servers manage the flow of electronic communications, handling the sending, receiving, and storing of email messages. Proper configuration and maintenance of email servers are crucial for effective communication and data integrity within an organization.

Integrating and managing these services effectively requires a thorough understanding of each component’s role and interaction within the data center environment. By ensuring that DNS, DHCP, Syslog, NTP, and Email servers are properly configured and maintained, organizations can achieve greater operational efficiency, improved network performance, and enhanced reliability. This holistic approach to data center management not only supports current needs but also lays a solid foundation for future scalability and adaptability.

CHAPTER-XI

SECURITY

9.1 Network Security:

Network security refers to the practices, policies, and technologies designed to safeguard digital communication and data transmitted over computer networks. Its primary goal is to ensure confidentiality, integrity, and availability of network resources and data.

9.1.1 Key Objectives of Network Security

1. Confidentiality: Protect sensitive information from unauthorized access.
2. Integrity: Ensure data accuracy and prevent modification or deletion.
3. Availability: Guarantee access to network resources for authorized users.

9.1.2 Network Security Threats

1. Malware: Viruses, worms, Trojans, and spyware.
2. Phishing: Social engineering attacks via email or messaging.
3. DDoS: Distributed Denial of Service attacks overwhelming networks.
4. Man-in-the-Middle (MitM): Intercepting communication between two parties.

9.1.3 Network Security Measures

1. Firewalls: Filtering incoming/outgoing traffic.
2. Virtual Private Networks (VPNs): Encrypting internet communication.
3. Intrusion Detection/Prevention Systems (IDPS/IPS): Monitoring and blocking malicious activity.
4. Encryption: Protecting data with algorithms and keys.
5. Access Control: Authenticating users and limiting access.

9.1.4 Network Security Types

1. Wired Security: Protecting wired networks from unauthorized access.
2. Wireless Security: Securing wireless networks from interception.
3. Application Security: Safeguarding software applications.
4. Endpoint Security: Protecting devices connected to the network.

9.1.5 Best Practices for Network Security

1. Regular software updates and patches.
2. Strong passwords and multi-factor authentication.
3. Network segmentation and isolation.

4. Continuous monitoring and incident response planning.

9.1.6 Network Security Benefits

1. Protects sensitive data and intellectual property.
2. prevents financial losses and reputational damage.
3. Ensures compliance with regulations and standards.
4. Maintains business continuity and operations.

Implementing a robust network security measures, organizations can safeguard their digital assets, protect sensitive information, and maintain trust with customers and partners**.**

9.2 Access Control Lists: Enhancing Security and Resource Management

Access Control Lists (ACLs) are a crucial security mechanism for regulating access to computer resources, networks, and files. By implementing ACLs, administrators can ensure that only authorized individuals or systems can access, modify, or execute specific resources.

9.2.1 Core Components of ACL

1. Subjects: Entities requesting access, such as users or processes.
2. Objects: Resources being accessed, including files, directories, or networks.
3. Permissions: Specific actions allowed, such as reading, writing, or executing.
4. Access Control Entries (ACEs): Individual rules defining permissions.

9.2.2 ACL Types

1. Standard ACL
2. Extended ACL

But here we will use the Extended ACL which offer us better Management of how to block the entire network, entire subnet as well as how to block a particular services like in our scenario we Block Ping, Web browser, and FTP access to data center from different branches.

9.2.3 Benefits of ACLs

1. Enhanced Security: Restrict access to sensitive resources.
2. Granular Control: Precise management of permissions.
3. Flexibility: Easy modification of access rules.
4. Audit Trail: Tracking access attempts.

9.2.4Applications of ACLs

1. File systems
2. Network devices
3. Operating systems

4. Database management systems

9.2.5 Practical Applications

1. Limiting access to sensitive data.
2. Controlling network access.
3. Restricting script execution

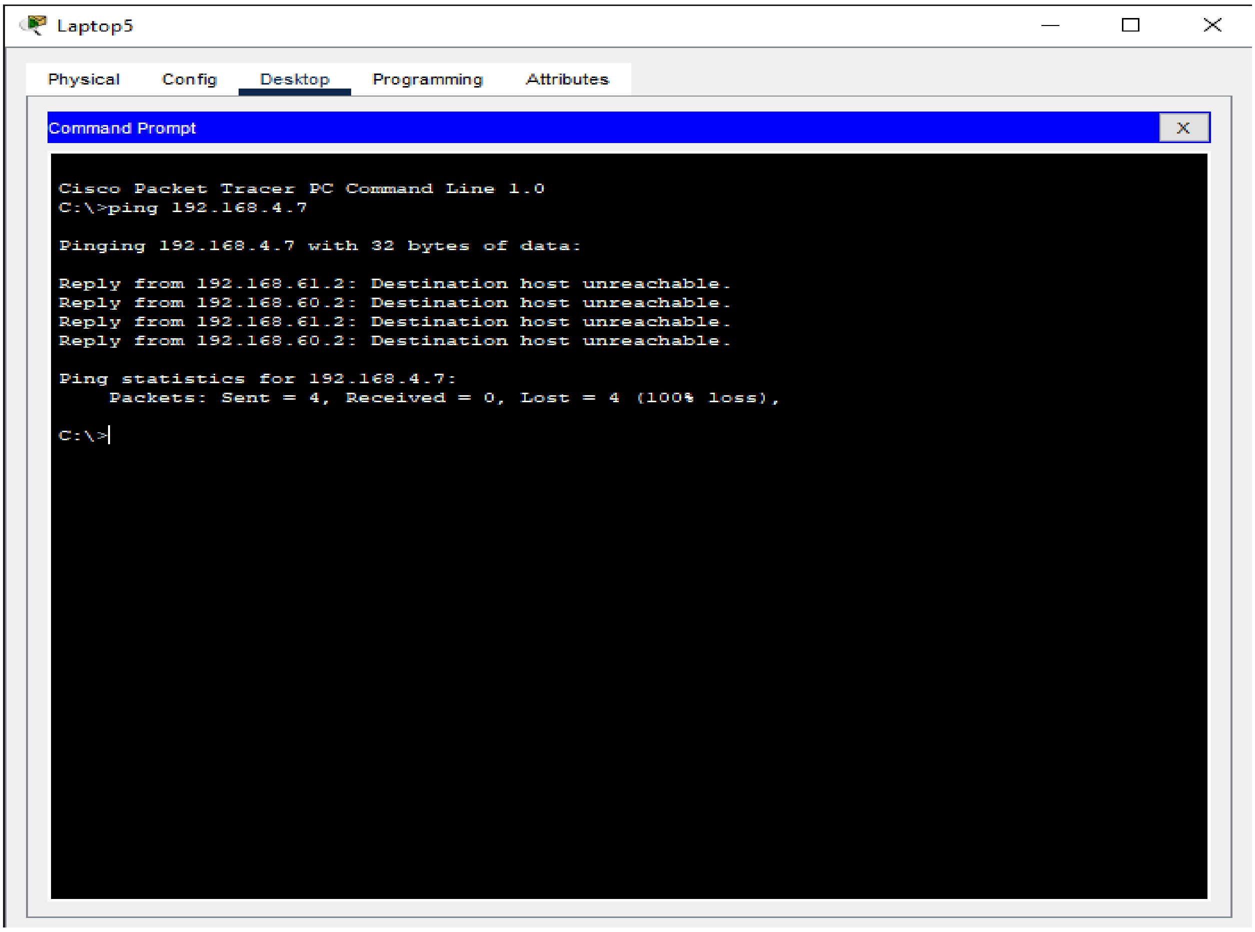
Utilizing ACLs, organizations can effectively manage access, protect resources, and maintain a secure environment.

Here’s How to configure ACL in Router.

9.2.6 ACL (Access Control List):

```
ISP-Router(config)#access-list 100 deny tcp host 192.168.3.7 host 192.168.4.10 eq ft
ISP-Router(config)#access-list 100 deny tcp host 192.168.3.7 host 192.168.4.10 eq ftp
ISP-Router(config)#access-list 100 deny tcp host 192.168.1.6 host 192.168.4.10 e
ISP-Router(config)#access-list 100 deny tcp host 192.168.1.6 host 192.168.4.10 eq ww
ISP-Router(config)#access-list 100 deny tcp host 192.168.1.6 host 192.168.4.10 eq www
ISP-Router(config)#access-list 100 deny ic
ISP-Router(config)#access-list 100 deny icmp hos
ISP-Router(config)#access-list 100 deny icmp host 192.168.2.10 host 192.168.4.7
ISP-Router(config)#
ISP-Router(config)#
ISP-Router(config)#
ISP-Router(config)#
ISP-Router(config)#
ISP-Router(config)#access-list 100 ip permit any any
ISP-Router(config)#int fa1/0
ISP-Router(config-if)#ip access-group 100 out
ISP-Router(config-if)#ip access-group 100 out
ISP-Router(config-if)#exit
ISP-Router(config)#int fa6/0
ISP-Router(config-if)#ip access-group 100 out
ISP-Router(config-if)#exit
```

Now let’s check that ACL is successfully implemented or not

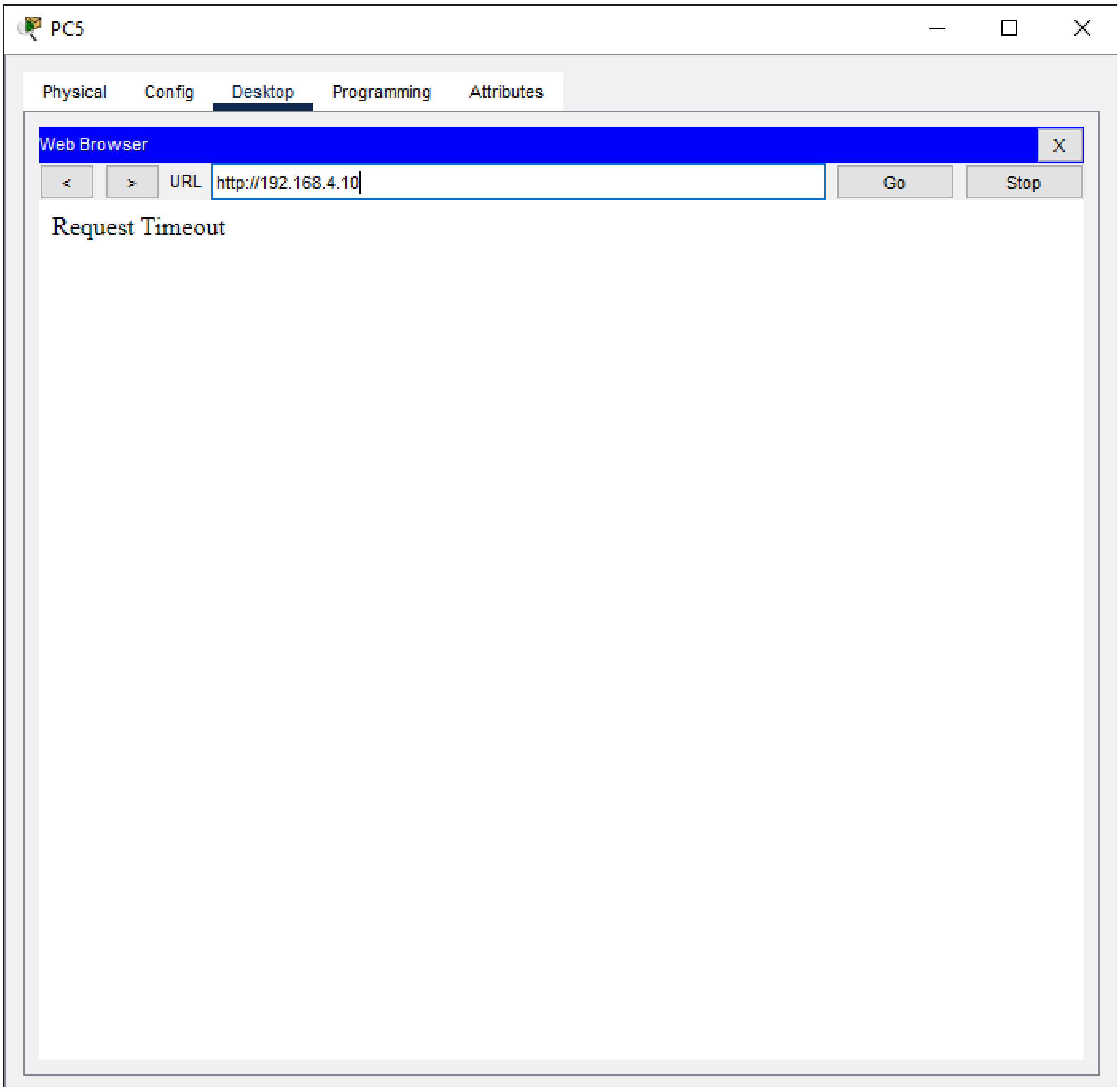


```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.4.7

Pinging 192.168.4.7 with 32 bytes of data:

Reply from 192.168.61.2: Destination host unreachable.
Reply from 192.168.60.2: Destination host unreachable.
Reply from 192.168.61.2: Destination host unreachable.
Reply from 192.168.60.2: Destination host unreachable.

Ping statistics for 192.168.4.7:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Figure 9.1

So as mentioned in the above figure the PC 9 is not able to ping the Email server and ACL is successfully implemented and working.

Now let check that PC can access the web browser or not



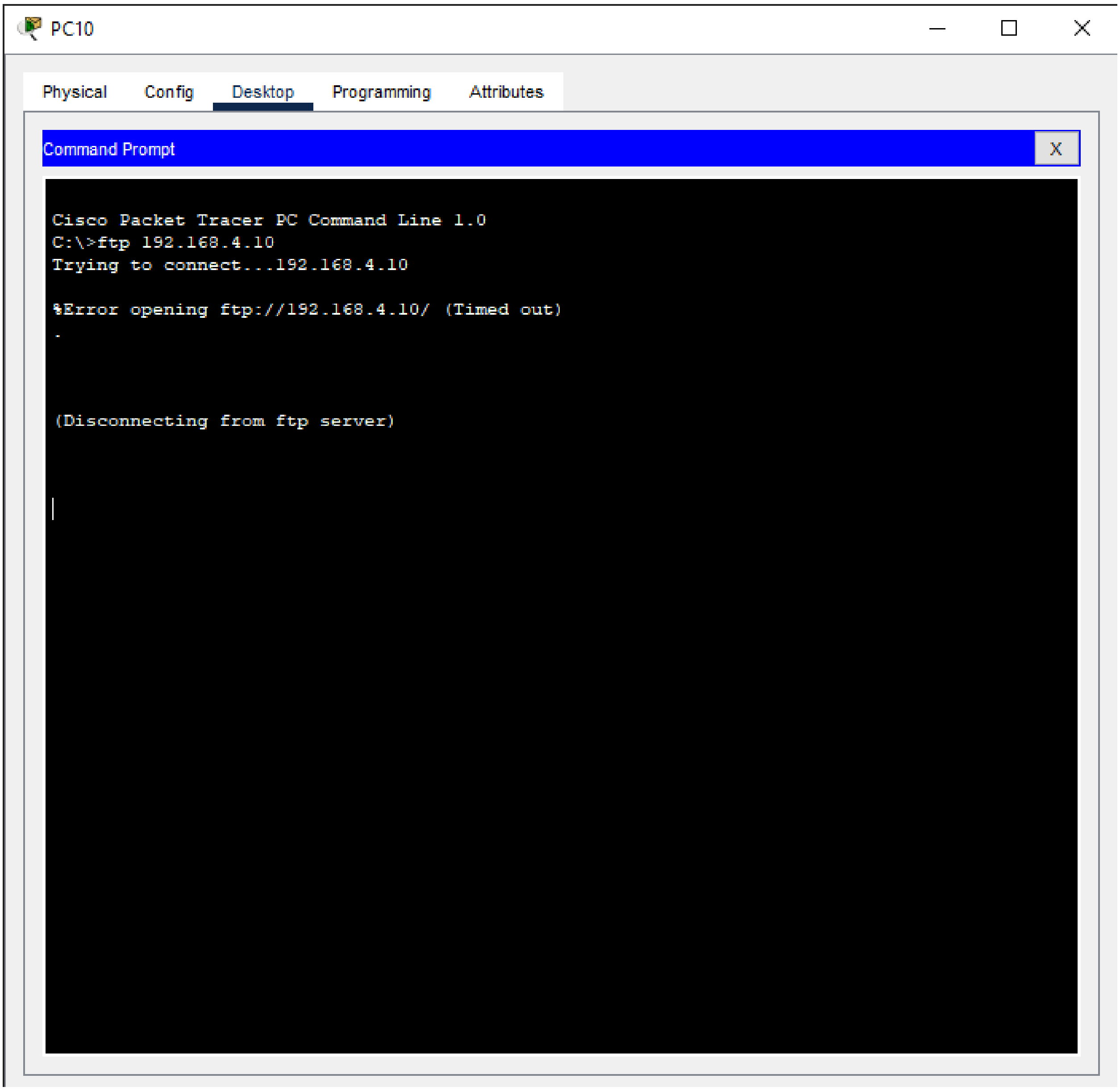
http://192.168.4.10

Request Timeout

Figure 9.2

So as mentioned in the above figure the PC 5 is not able to access the web server

Now let’s check the FTP connectivity



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ftp 192.168.4.10
Trying to connect...192.168.4.10

%Error opening ftp://192.168.4.10/ (Timed out)
.



(Disconnecting from ftp server)
```

Figure 9.3

So as mentioned in the above figure the PC10 is not able to access the FTP server

So its mean that ACL is successfully implemented and working according to the rules of ACLs

9.3 IP-SEC VPN:

IPSec (Internet Protocol Security) is widely used protocol suite that secures IP communication by authenticating and encrypting each IP packet in a communication session. When implemented as a point to point VPN it offer several advantages over the Enterprise network.

1. **Enhanced Security:** IPSec provides robust encryption and authentication mechanism, ensuring data transmitted over the network is secure from various eavesdropping and tampering. This is particularly important for enterprise to handle sensitive information.
2. **Data Integrity:** With IPSec data integrity is maintained through hashing algorithms that verify that the data has not been altered during transmission. This is crucial for enterprise that require reliable data exchange.
3. **Flexible Configuration:** IPSec can be configured to operate in Two Modes. **Transparent mode** and **Tunnel mode** this flexibility allow enterprises to choose the appropriate mode based on their specific needs whether for end-to-end communication or for site-to-site connection.
4. **Interoperability:** IPSec is compatible with various operating systems and devices , making it easier for enterprises to implement across diverse environments. This interoperability ensure that different systems can communicate securely without compatibility issues.
5. **Scalability:** As enterprise network grow their needs evolve. IPSec VPN can be easily scaled to accommodate more users or additional sites, allowing business to expend their operation without compromising security.
6. **Cost-Effective:** By utilizing existing internet infrastructure for secure communication, enterprise can reduce cost associated with dedicated leased lines or other expensive private networking solutions.
7. **Remote Access:** IPSec VPN enable secure remote access for employees, allowing them to connect to the enterprise network form anywhere in the world. This is increasingly important in today’s remote work environment, enhancing productivity while maintaining security.

9.3.1Configuration of IP-Sec VPN among data center and Branch 1:

Data center side

```
//license boot module c1900 technology-package securityk9
to enable vpn in router
cypto isakmp policy 10
authentication pre-share
encryption aes
```

```
hash sha
group 2
lifetime 86400
exit
license udi pid CISCO1941/K9 sn FTX1524T0X3-
license boot module c1900 technology-package securityk9
!
!
!
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 2
!
crypto isakmp key Enterprise address 192.168.11.1
!
!
!
crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
!
crypto map VPN-MAP 10 ipsec-isakmp
 set peer 192.168.11.1
 set transform-set VPN-SET
 match address VPN-ACL
!

ip access-list extended VPN-ACL
 permit ip 192.168.4.0 0.0.0.255 192.168.1.0 0.0.0.255
```

BR 1 side

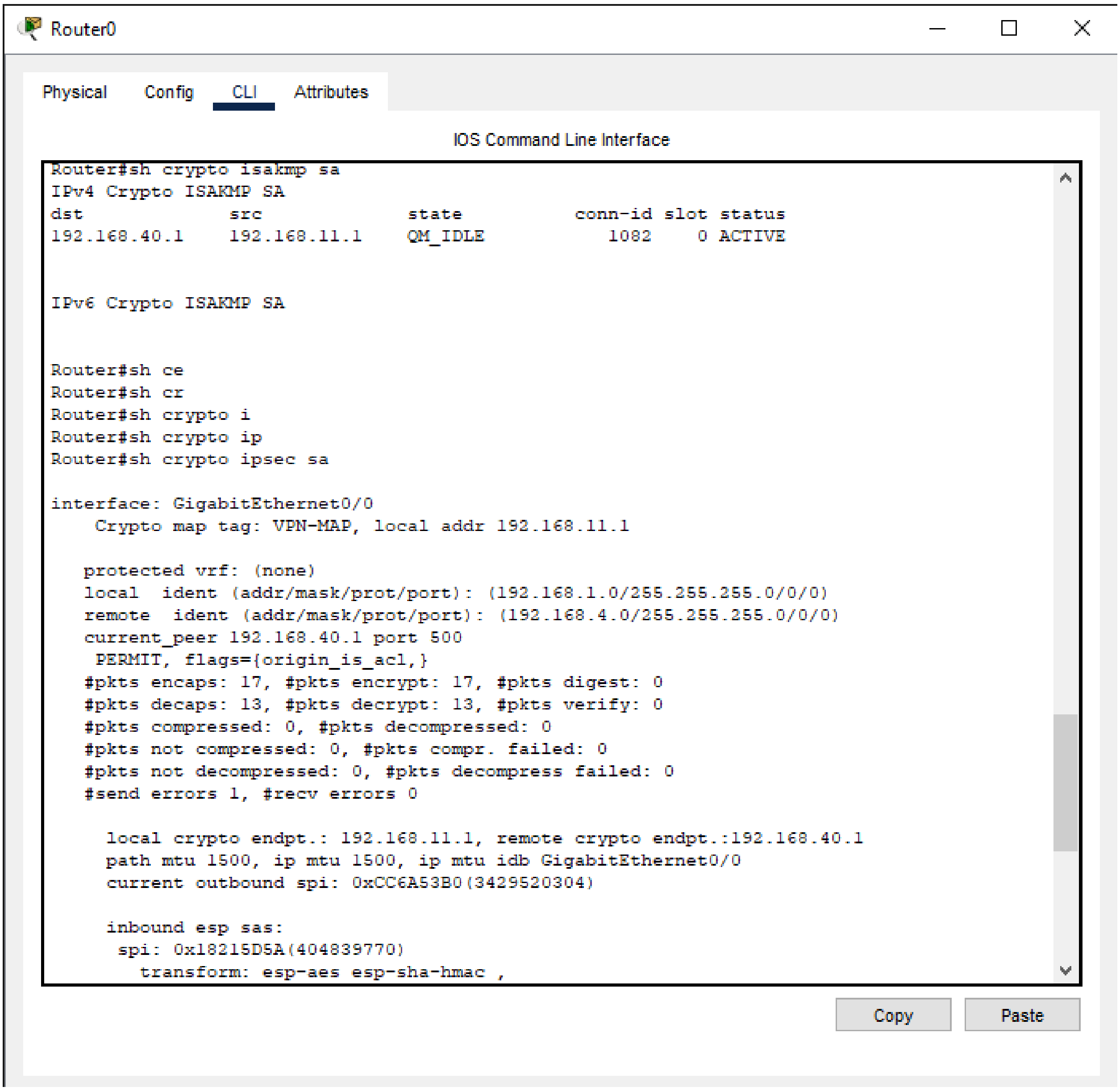
```
//license boot module c1900 technology-package securityk9
```

to enable vpn in router

```
cypto isakmp policy 10
```

```
authentication pre-share
encryption aes
hash sha
group 2
lifetime 86400
exit


!
license udi pid CISCO1941/K9 sn FTX1524G1XL-
license boot module c1900 technology-package securityk9
!
!
!
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 2
!
crypto isakmp key Enterprise address 192.168.40.1
!
!
!
crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
!
crypto map VPN-MAP 10 ipsec-isakmp
 set peer 192.168.40.1
 set transform-set VPN-SET
 match address VPN-ACL
!
ip access-list extended VPN-ACL
 permit ip 192.168.1.0 0.0.0.255 192.168.4.0 0.0.0.255
```

!



```
Router#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
192.168.40.1    192.168.11.1    QM_IDLE           1082    0 ACTIVE


IPv6 Crypto ISAKMP SA


Router#sh ce
Router#sh cr
Router#sh crypto i
Router#sh crypto ip
Router#sh crypto ipsec sa

interface: GigabitEthernet0/0
    Crypto map tag: VPN-MAP, local addr 192.168.11.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (192.168.4.0/255.255.255.0/0/0)
   current_peer 192.168.40.1 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 17, #pkts encrypt: 17, #pkts digest: 0
   #pkts decaps: 13, #pkts decrypt: 13, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 1, #recv errors 0

     local crypto endpt.: 192.168.11.1, remote crypto endpt.:192.168.40.1
     path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0
     current outbound spi: 0xCC6A53B0(3429520304)

     inbound esp sas:
      spi: 0x18215D5A(404839770)
        transform: esp-aes esp-sha-hmac ,
```

Figure 9.4

In the above figure the iskamp tunnel has been successfully created and active so it mean that the Encryption and hashing parameters are successfully exchanged between site A and data center.

CHAPTER-X

TESTING AND EVALUATION

10.1 INTRODUCTION: Testing and evaluation in networking refer to the processes of verifying and assessing the performance, security, and reliability of a network or networked system. Here are some key aspects:

Testing:

1. Network Performance Testing: Measures network speed, throughput, latency, and packet loss.
2. Network Security Testing: Identifies vulnerabilities and assesses the effectiveness of security controls.
3. Network Functionality Testing: Verifies that network services and applications work as expected.
4. Interoperability Testing: Ensures that different network devices and systems work together seamlessly.

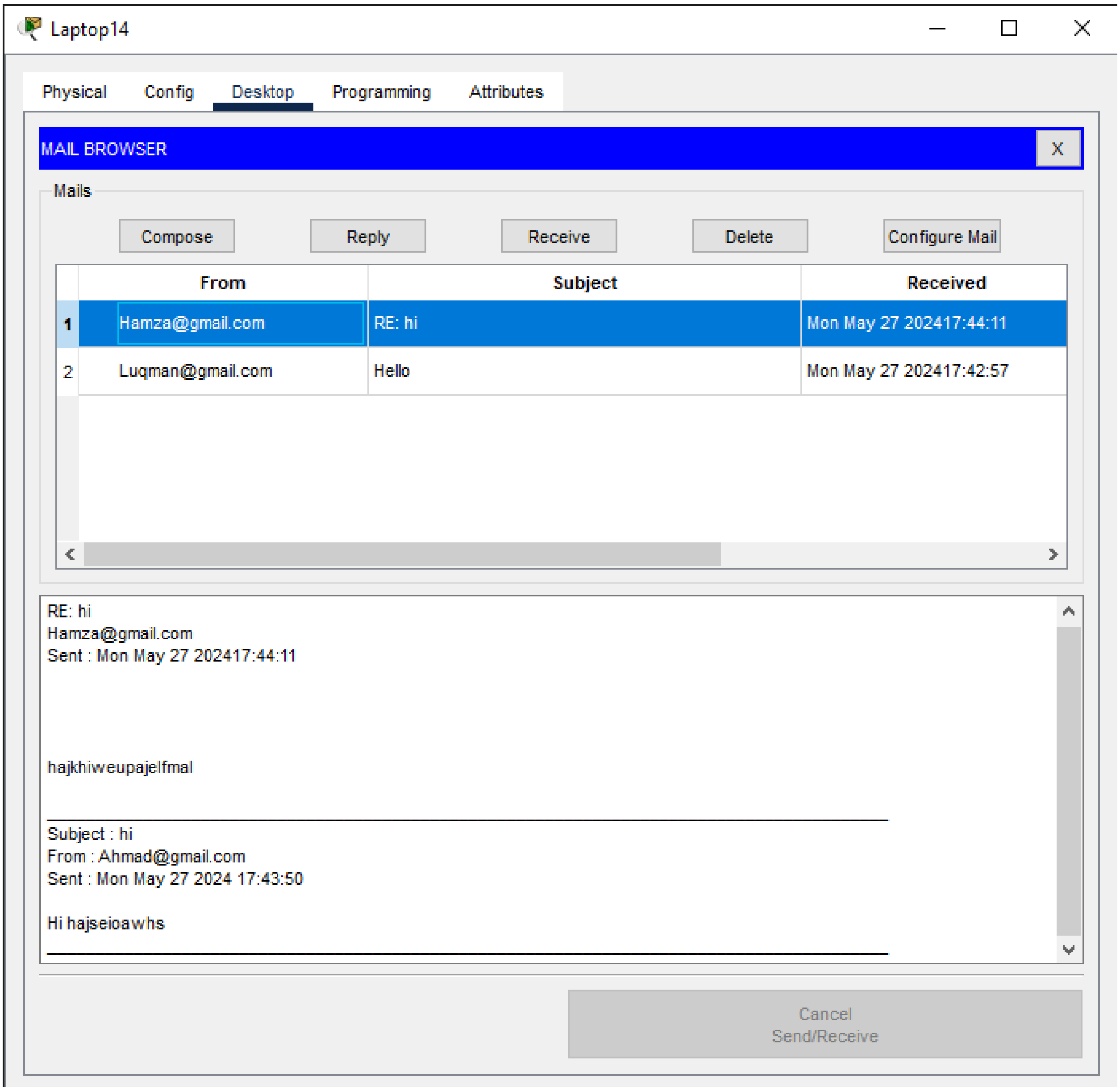
Evaluation:

1. Network Performance Evaluation: Analyzes test results to identify bottlenecks and areas for improvement.
2. Network Security Evaluation: Assesses the effectiveness of security controls and identifies potential risks.
3. Network Reliability Evaluation: Evaluates the network's ability to withstand failures and recover from outages.
4. Return on Investment (ROI) Evaluation: Assesses the cost-effectiveness of network upgrades or new implementations.

Best Practices:

1. Test Early and Often: Test throughout the network design and implementation process.
2. Use Realistic Test Scenarios: Reflect real-world network usage and traffic patterns.
3. Evaluate Multiple Scenarios: Consider various network configurations and scenarios.
4. Document Results: Maintain detailed records of testing and evaluation results.

10.2 Testing the Data Center: Testing the data center to make sure that every server can work and respond properly to the users and meet the required standards, are reliable and perform optimally.



	From	Subject	Received
1	Hamza@gmail.com	RE: hi	Mon May 27 202417:44:11
2	Luqman@gmail.com	Hello	Mon May 27 202417:42:57

RE: hi
Hamza@gmail.com
Sent : Mon May 27 202417:44:11

hajkhiweupajelfmal

Subject : hi
From : Ahmad@gmail.com
Sent : Mon May 27 2024 17:43:50

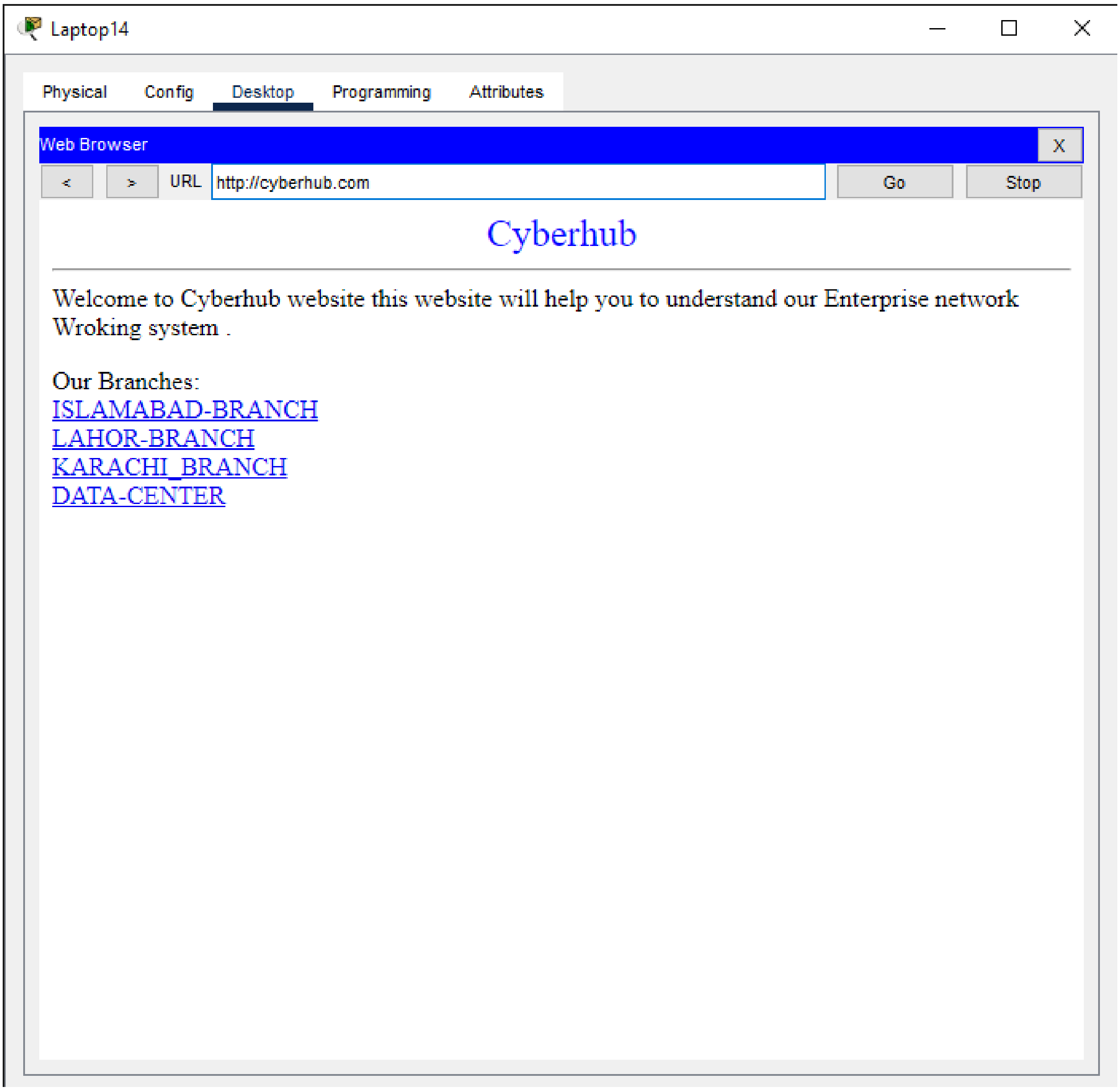
Hi hajseioawhs

Figure 10.1

Let’s test the **Email server**

In the above figure the email server are properly respond and work correctly by sending and receiving emails from client sides.

Now let’s confirm the testing of Web server and DNS server. If the IP address of webserver are resolve properly and using web the website are access using the domain name then it’s mean that both of the servers are working properly and meet the data center requirement’s.



http://cyberhub.com

Cyberhub

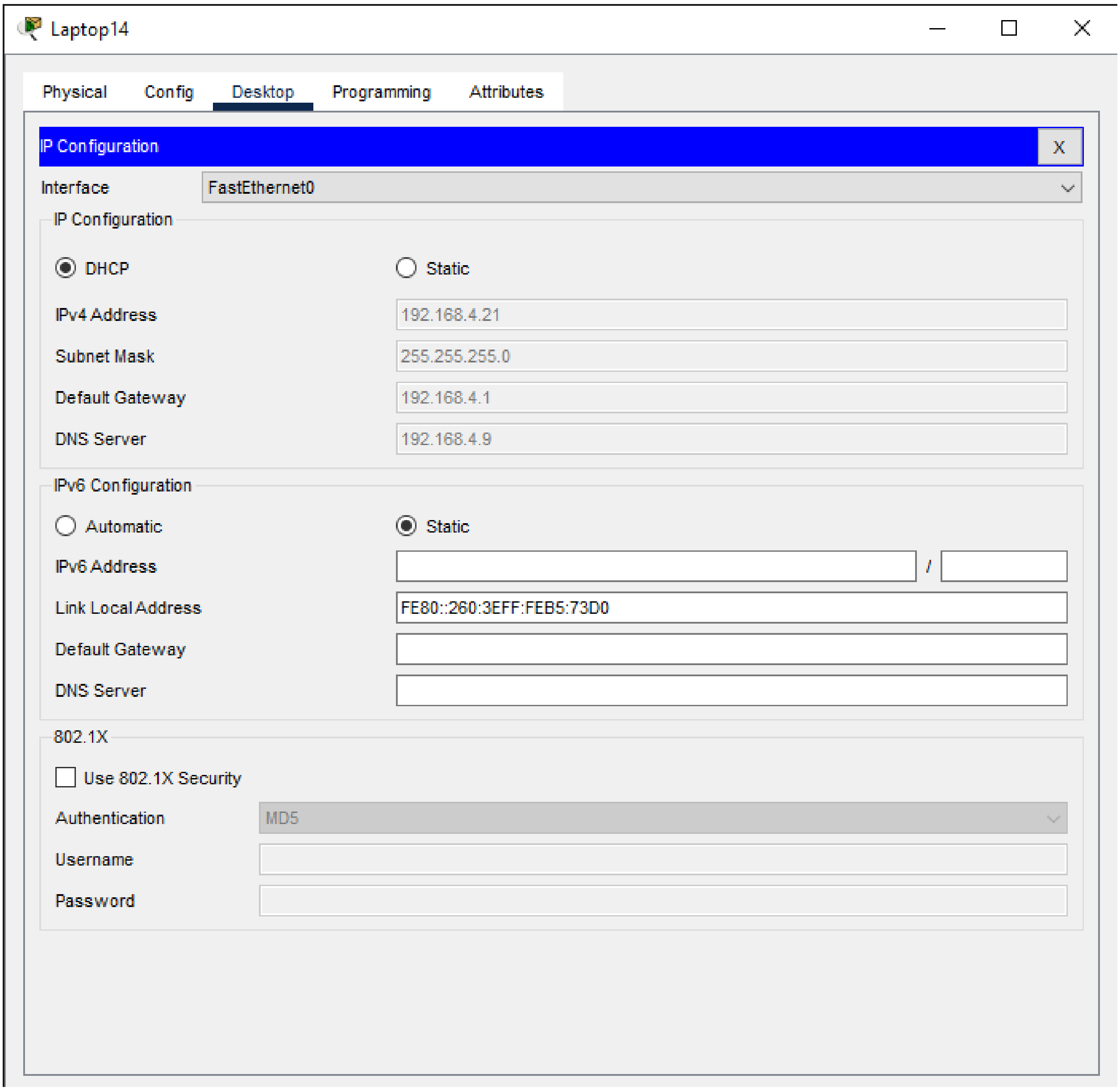
Welcome to Cyberhub website this website will help you to understand our Enterprise network Wroking system .

Our Branches:
ISLAMABAD-BRANCH
LAHOR-BRANCH
KARACHI_BRANCH
DATA-CENTER

Figure 10.2

In the above figure the web server are successfully accessed by the domain name and working properly. As shown in the figure.

Now let’s test the DHCP Server if the DHCP server provide dynamic IP address allocation



Laptop14

IP Configuration

Interface: FastEthernet0

IP Configuration

● DHCP ○ Static

IPv4 Address: 192.168.4.21

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.4.1

DNS Server: 192.168.4.9

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::260:3EFF:FEB5:73D0

Default Gateway:

DNS Server:

802.1X

□ Use 802.1X Security

Authentication: MD5

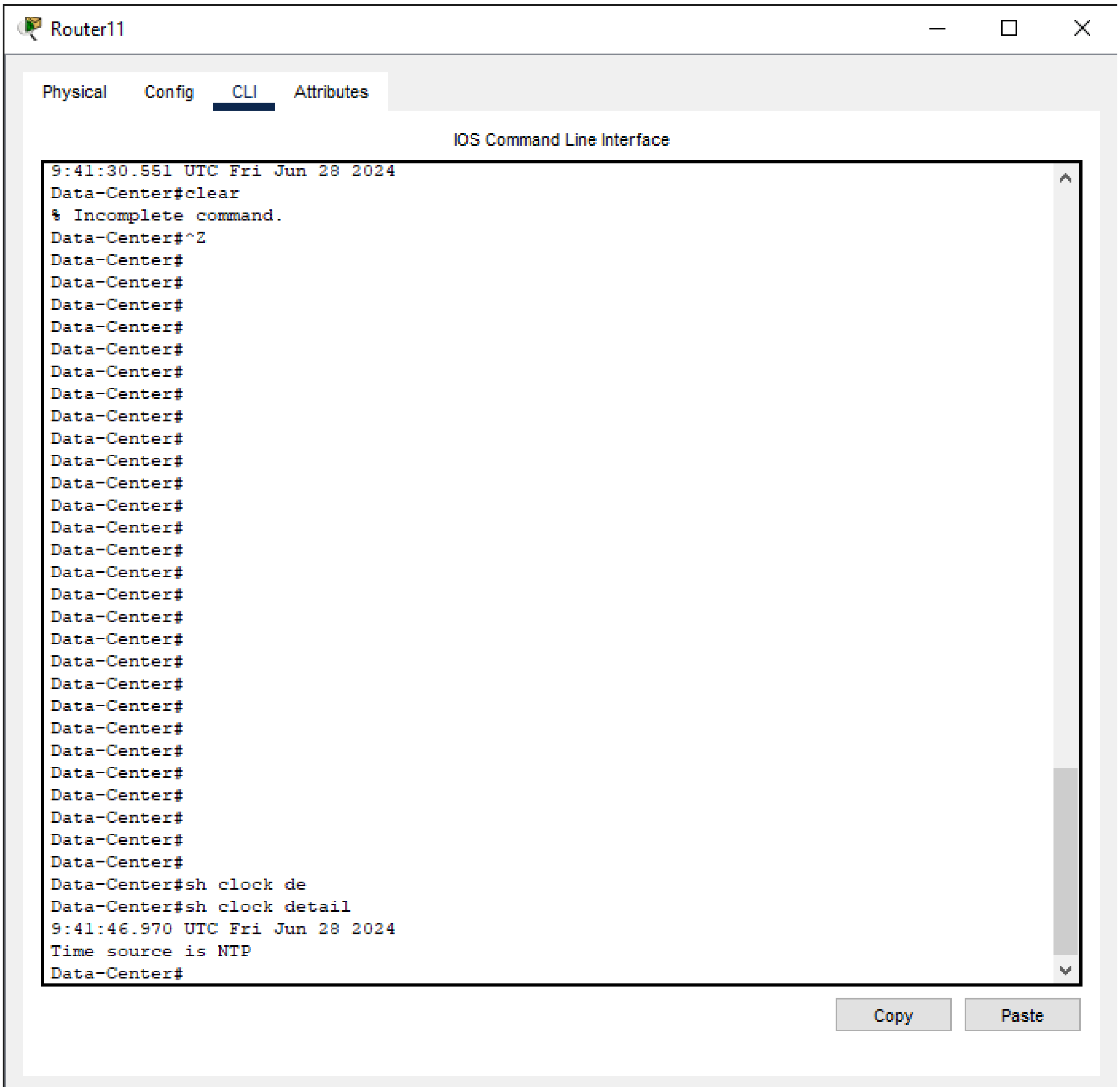
Username:

Password:

Figure 10.3

Across the network it mean that DHCP server are also working properly so let’s test.

In the above figure the DHCP server successfully assign the IP address to PC and working properly also the gateway and DNS server IP are correct according to the configuration.

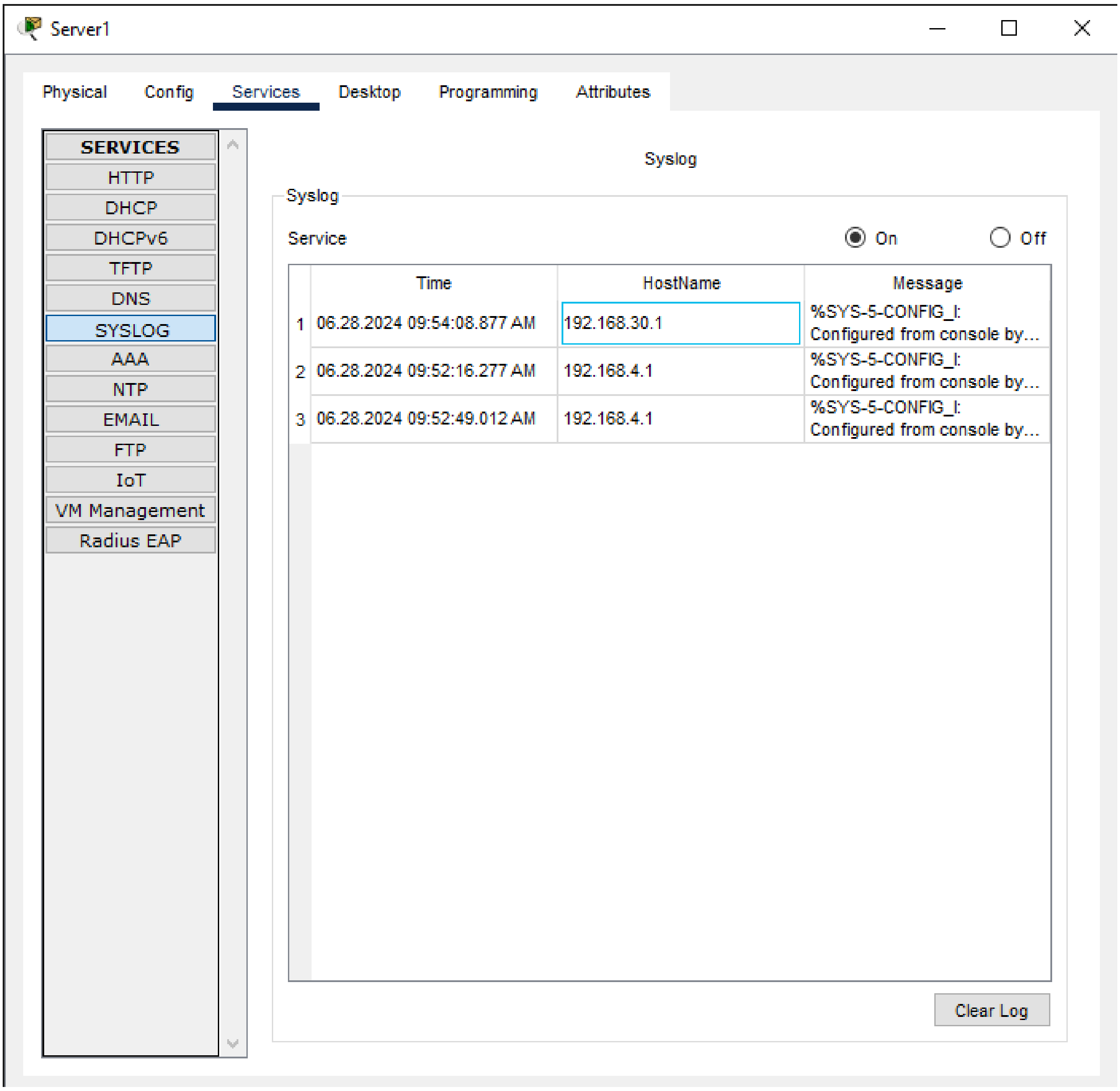


```
9:41:30.551 UTC Fri Jun 28 2024
Data-Center#clear
% Incomplete command.
Data-Center#^Z
Data-Center#
Data-Center#
Data-Center#
Data-Center#
Data-Center#
Data-Center#
Data-Center#
Data-Center#
Data-Center#
Data-Center#
Data-Center#
Data-Center#
Data-Center#
Data-Center#
Data-Center#
Data-Center#
Data-Center#
Data-Center#
Data-Center#
Data-Center#
Data-Center#
Data-Center#
Data-Center#
Data-Center#
Data-Center#
Data-Center#
Data-Center#
Data-Center#
Data-Center#sh clock de
Data-Center#sh clock detail
9:41:46.970 UTC Fri Jun 28 2024
Time source is NTP
Data-Center#
```

Figure 10.4

Now let’s the NTP server to correctly provide the timestamp to every device on the network. In the above figure the NTP server provide the correct timestamp to Routers and working properly.

So let check the syslog server that it capture the logs or not



Syslog

Service ● On ○ Off

	Time	HostName	Message
1	06.28.2024 09:54:08.877 AM	192.168.30.1	%SYS-5-CONFIG_I: Configured from console by...
2	06.28.2024 09:52:16.277 AM	192.168.4.1	%SYS-5-CONFIG_I: Configured from console by...
3	06.28.2024 09:52:49.012 AM	192.168.4.1	%SYS-5-CONFIG_I: Configured from console by...

Figure 10.5

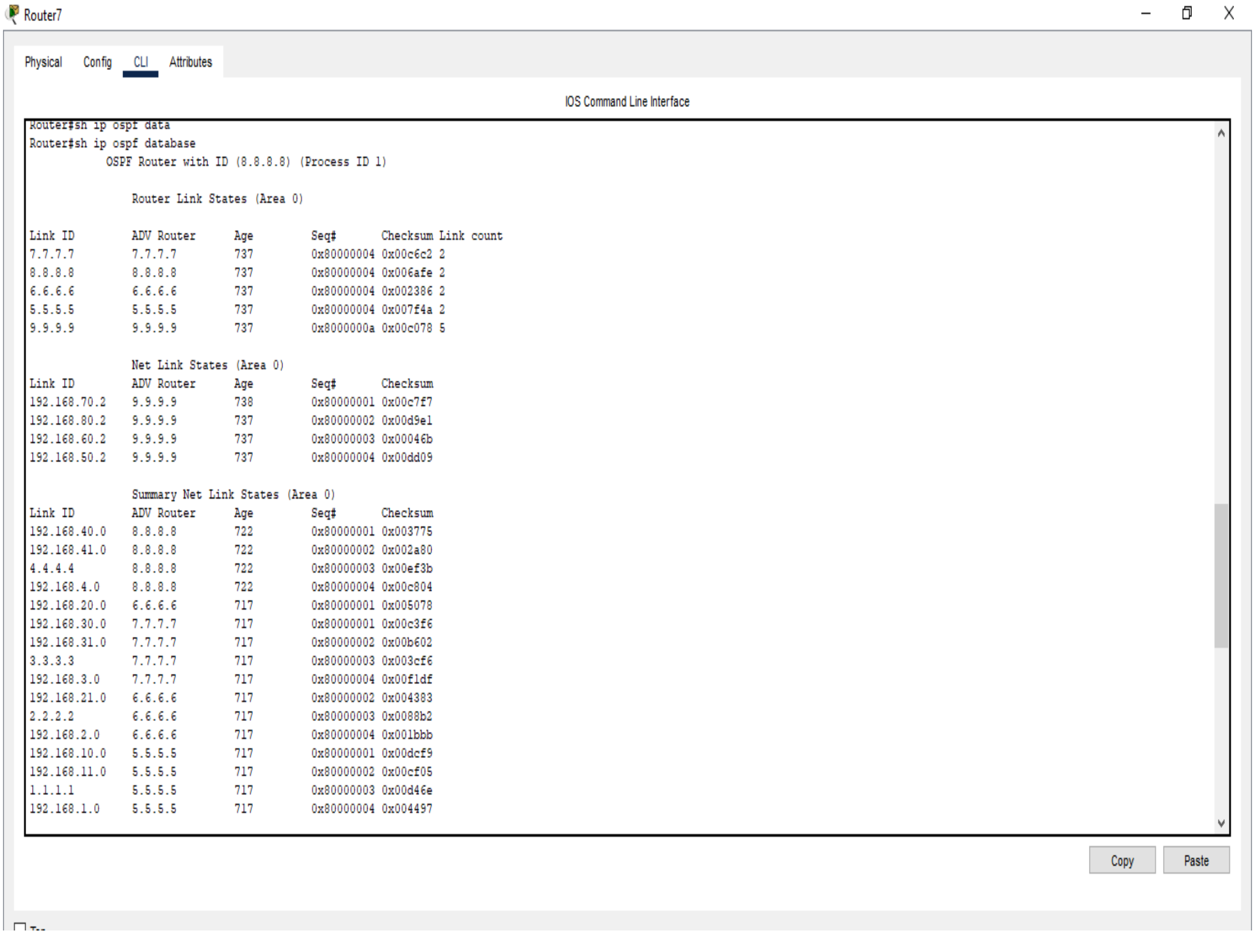
In the above figure we can see that logs are properly stored in syslog server. It mean that syslog server also working properly.

9.3 Testing the OSPF:

OSPF Neighbor State Testing

In a successful formation of OSPF adjacency, OSPF neighbors attain the FULL neighbor state. This is a crucial aspect of OSPF testing, and it's important to verify the connectivity between routers using tools like ping to ensure the proper functioning of OSPF adjacency [**1**].

MTU Testing in OSPF



```
Router#sh ip ospf data
Router#sh ip ospf database
            OSPF Router with ID (8.8.8.8) (Process ID 1)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
7.7.7.7         7.7.7.7         737         0x80000004 0x00c6c2 2
8.8.8.8         8.8.8.8         737         0x80000004 0x006afe 2
6.6.6.6         6.6.6.6         737         0x80000004 0x002386 2
5.5.5.5         5.5.5.5         737         0x80000004 0x007f4a 2
9.9.9.9         9.9.9.9         737         0x8000000a 0x00c078 5

                Net Link States (Area 0)
Link ID         ADV Router      Age         Seq#       Checksum
192.168.70.2    9.9.9.9         738         0x80000001 0x00c7f7
192.168.80.2    9.9.9.9         737         0x80000002 0x00d9e1
192.168.60.2    9.9.9.9         737         0x80000003 0x00046b
192.168.50.2    9.9.9.9         737         0x80000004 0x00dd09

                Summary Net Link States (Area 0)
Link ID         ADV Router      Age         Seq#       Checksum
192.168.40.0    8.8.8.8         722         0x80000001 0x003775
192.168.41.0    8.8.8.8         722         0x80000002 0x002a80
4.4.4.4         8.8.8.8         722         0x80000003 0x00ef3b
192.168.4.0     8.8.8.8         722         0x80000004 0x00c804
192.168.20.0    6.6.6.6         717         0x80000001 0x005078
192.168.30.0    7.7.7.7         717         0x80000001 0x00c3f6
192.168.31.0    7.7.7.7         717         0x80000002 0x00b602
3.3.3.3         7.7.7.7         717         0x80000003 0x003cf6
192.168.3.0     7.7.7.7         717         0x80000004 0x00f1df
192.168.21.0    6.6.6.6         717         0x80000002 0x004383
2.2.2.2         6.6.6.6         717         0x80000003 0x0088b2
192.168.2.0     6.6.6.6         717         0x80000004 0x001bbb
192.168.10.0    5.5.5.5         717         0x80000001 0x00dcf9
192.168.11.0    5.5.5.5         717         0x80000002 0x00cf05
1.1.1.1         5.5.5.5         717         0x80000003 0x00d46e
192.168.1.0     5.5.5.5         717         0x80000004 0x004497
```

Figure 10.6

MTU (Maximum Transmission Unit) configuration is also an important aspect of OSPF testing. It's crucial to ensure that there are no issues with fragmentation and that the MTU settings are compatible to avoid potential problems such as MTU mismatch, which can lead to OSPF flapping issues.

Verifying OSPF Configuration

Verifying and monitoring OSPF configuration is essential for ensuring that OSPF is running on the desired interfaces and in the correct areas. This can be done using commands like show ospf interface from the CLI to verify the OSPF status on specific interfaces

In the above figure the OSPF database contains all the routes and devices can successfully communicate with each other’s.

9.4 Testing the Connectivity: testing connectivity is a fundamental aspect of network configuration and troubleshooting. Here are some common methods for testing connectivity within the Packet Tracer environment:

Using Ping and Telnet

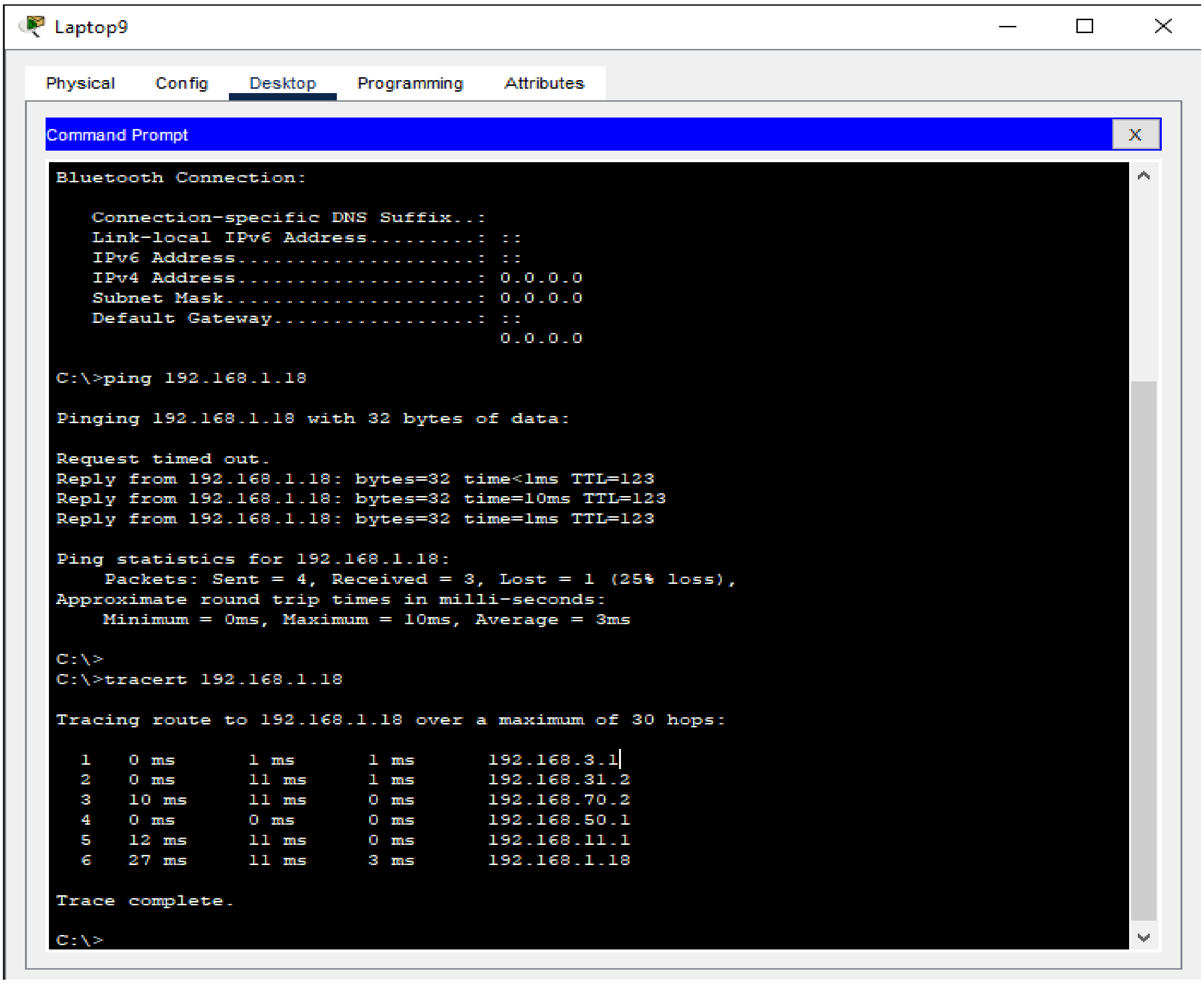
It is a good practice to test connectivity through ping and Telnet in Packet Tracer. These tools allow you to verify the reachability and accessibility of network devices and services.

Real-time Mode and Command Prompt

In Real-time mode, you can open a command prompt from the PC desktop in Packet Tracer and issue a ping command to verify connectivity.

Traceroute Command

In the above figure the ping and tracert command show us that connectivity between Islamabad and Karachi branch is pingable and can successfully communicate with each other with route.



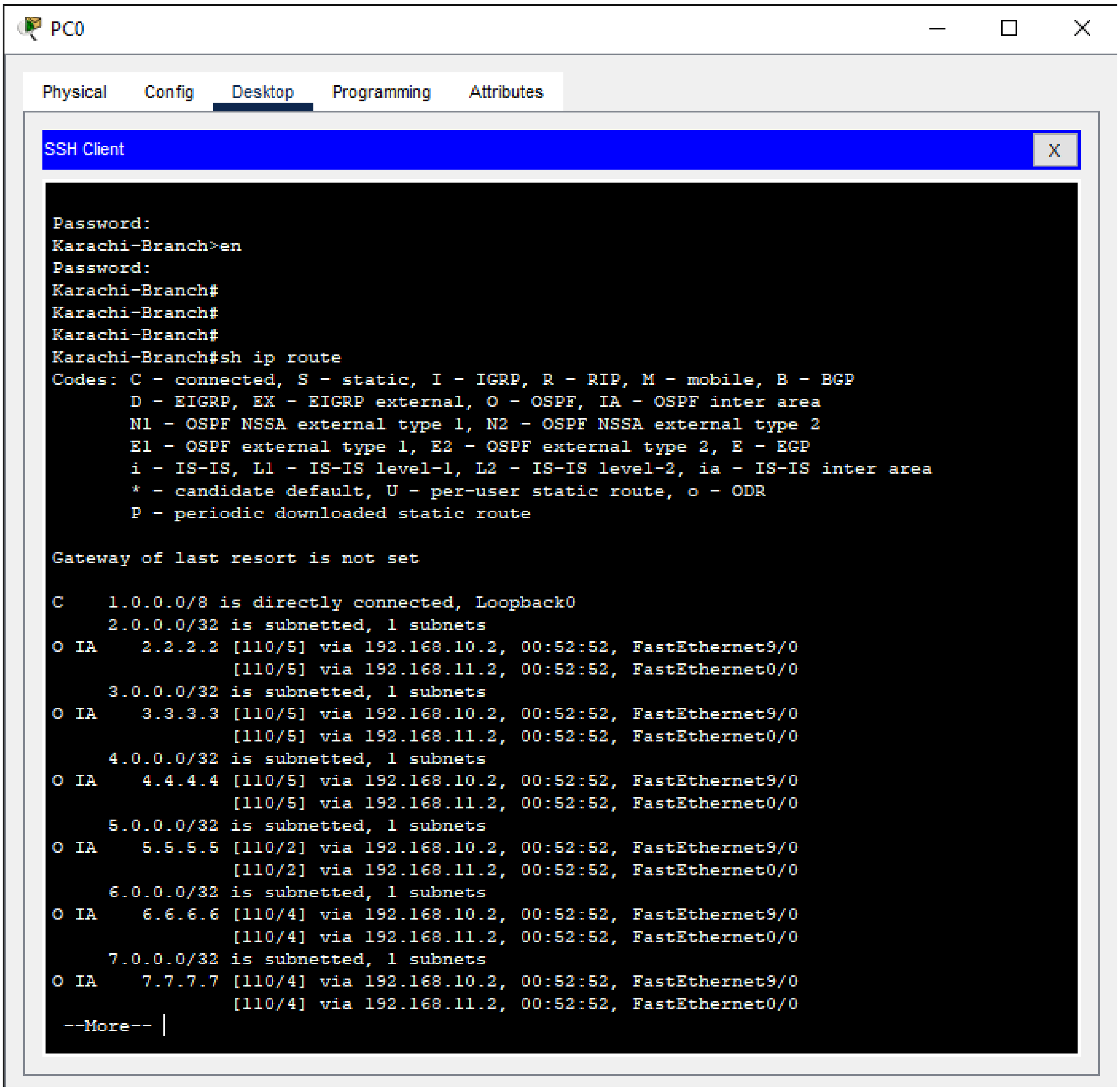
```
Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: ::
   IPv6 Address....................: ::
   IPv4 Address....................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: ::
                                     0.0.0.0

C:\>ping 192.168.1.18

Pinging 192.168.1.18 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.18: bytes=32 time<1ms TTL=123
Reply from 192.168.1.18: bytes=32 time=10ms TTL=123
Reply from 192.168.1.18: bytes=32 time=1ms TTL=123

Ping statistics for 192.168.1.18:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 3ms

C:\>
C:\>tracert 192.168.1.18

Tracing route to 192.168.1.18 over a maximum of 30 hops:

  1   0 ms      1 ms      1 ms      192.168.3.1
  2   0 ms      11 ms     1 ms      192.168.31.2
  3   10 ms     11 ms     0 ms      192.168.70.2
  4   0 ms      0 ms      0 ms      192.168.50.1
  5   12 ms     11 ms     0 ms      192.168.11.1
  6   27 ms     11 ms     3 ms      192.168.1.18

Trace complete.

C:\>
```

Figure 10.7

Packet Tracer also supports the use of the tracert command to test end-to-end connectivity.

This involves sending a ping from one end of the network to the other end and analyzing the results.

9.5 Testing Remote Access on Routers: In remote testing we can able to remotely access the device form anywhere by enabling SSH on routers for secure access. So let's check that SSH is working or not?



```
Password:
Karachi-Branch>en
Password:
Karachi-Branch#
Karachi-Branch#
Karachi-Branch#
Karachi-Branch#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    1.0.0.0/8 is directly connected, Loopback0
     2.0.0.0/32 is subnetted, 1 subnets
O IA    2.2.2.2 [110/5] via 192.168.10.2, 00:52:52, FastEthernet9/0
                [110/5] via 192.168.11.2, 00:52:52, FastEthernet0/0
     3.0.0.0/32 is subnetted, 1 subnets
O IA    3.3.3.3 [110/5] via 192.168.10.2, 00:52:52, FastEthernet9/0
                [110/5] via 192.168.11.2, 00:52:52, FastEthernet0/0
     4.0.0.0/32 is subnetted, 1 subnets
O IA    4.4.4.4 [110/5] via 192.168.10.2, 00:52:52, FastEthernet9/0
                [110/5] via 192.168.11.2, 00:52:52, FastEthernet0/0
     5.0.0.0/32 is subnetted, 1 subnets
O IA    5.5.5.5 [110/2] via 192.168.10.2, 00:52:52, FastEthernet9/0
                [110/2] via 192.168.11.2, 00:52:52, FastEthernet0/0
     6.0.0.0/32 is subnetted, 1 subnets
O IA    6.6.6.6 [110/4] via 192.168.10.2, 00:52:52, FastEthernet9/0
                [110/4] via 192.168.11.2, 00:52:52, FastEthernet0/0
     7.0.0.0/32 is subnetted, 1 subnets
O IA    7.7.7.7 [110/4] via 192.168.10.2, 00:52:52, FastEthernet9/0
                [110/4] via 192.168.11.2, 00:52:52, FastEthernet0/0
 --More--
```

Figure 10.8

In the above figure we can see that we are successfully access the router using SSH.

9.6 Testing WLANs: Testing WLAN (Wireless Local Area Network) connectivity is essential for ensuring the proper functioning of wireless networks within simulated environments. Here are some methods for testing WLAN connectivity in Packet Tracer:

Using Ping and Telnet

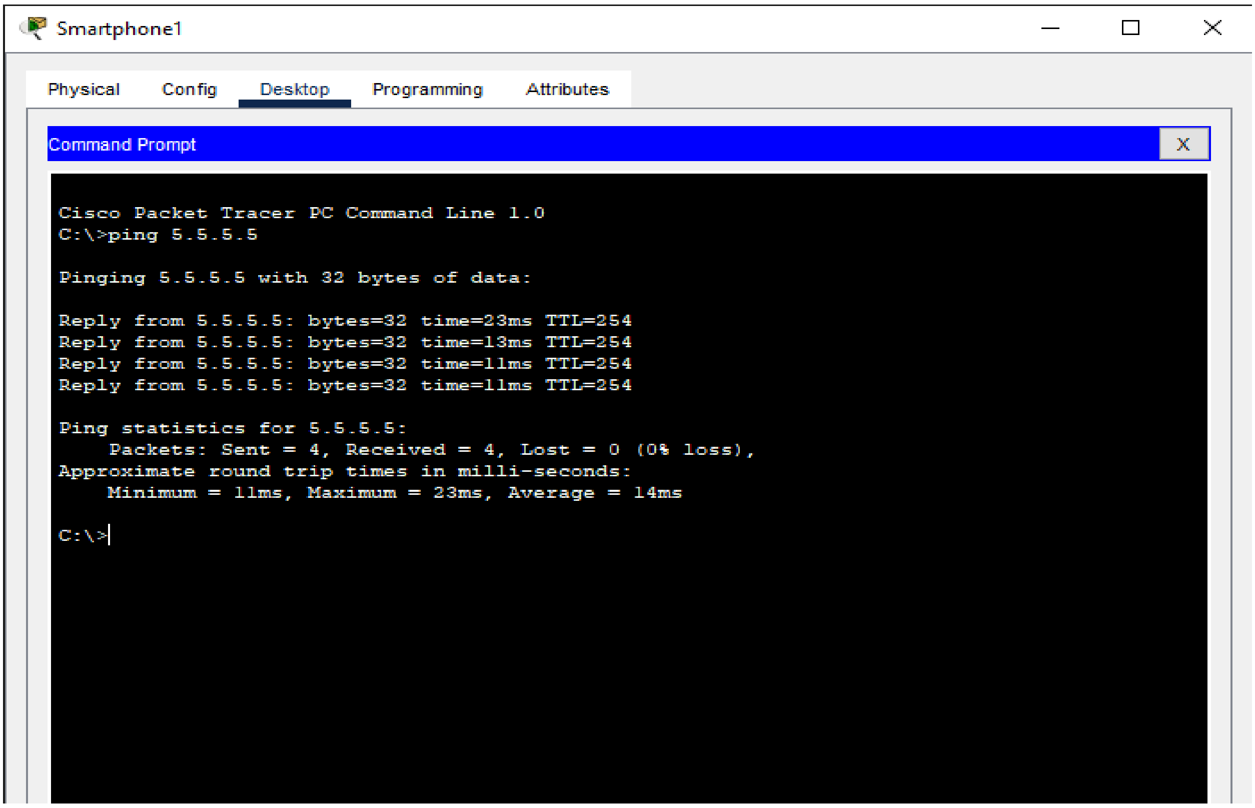
Similar to testing wired network connectivity, you can use the ping and Telnet commands to verify the reachability and accessibility of wireless devices and services within the WLAN.

Simulating Internet Connectivity

To test Internet connectivity within the WLAN, you can simulate the presence of the Internet using the PT-Cloud feature in Packet Tracer. By configuring PT-Cloud and adding the necessary routes, you can simulate the flow of traffic to and from the Internet, allowing you to test the WLAN's ability to access external resources.

Testing Wireless Throughput

If you need to validate the wireless throughput of an access point within the WLAN, you can follow specific procedures for testing 802.11ax wireless throughput. This involves focusing on troubleshooting and validating the wireless throughput of the access point, which can be crucial for assessing the performance of the WLAN.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 5.5.5.5

Pinging 5.5.5.5 with 32 bytes of data:

Reply from 5.5.5.5: bytes=32 time=23ms TTL=254
Reply from 5.5.5.5: bytes=32 time=13ms TTL=254
Reply from 5.5.5.5: bytes=32 time=11ms TTL=254
Reply from 5.5.5.5: bytes=32 time=11ms TTL=254

Ping statistics for 5.5.5.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 11ms, Maximum = 23ms, Average = 14ms

C:\>
```

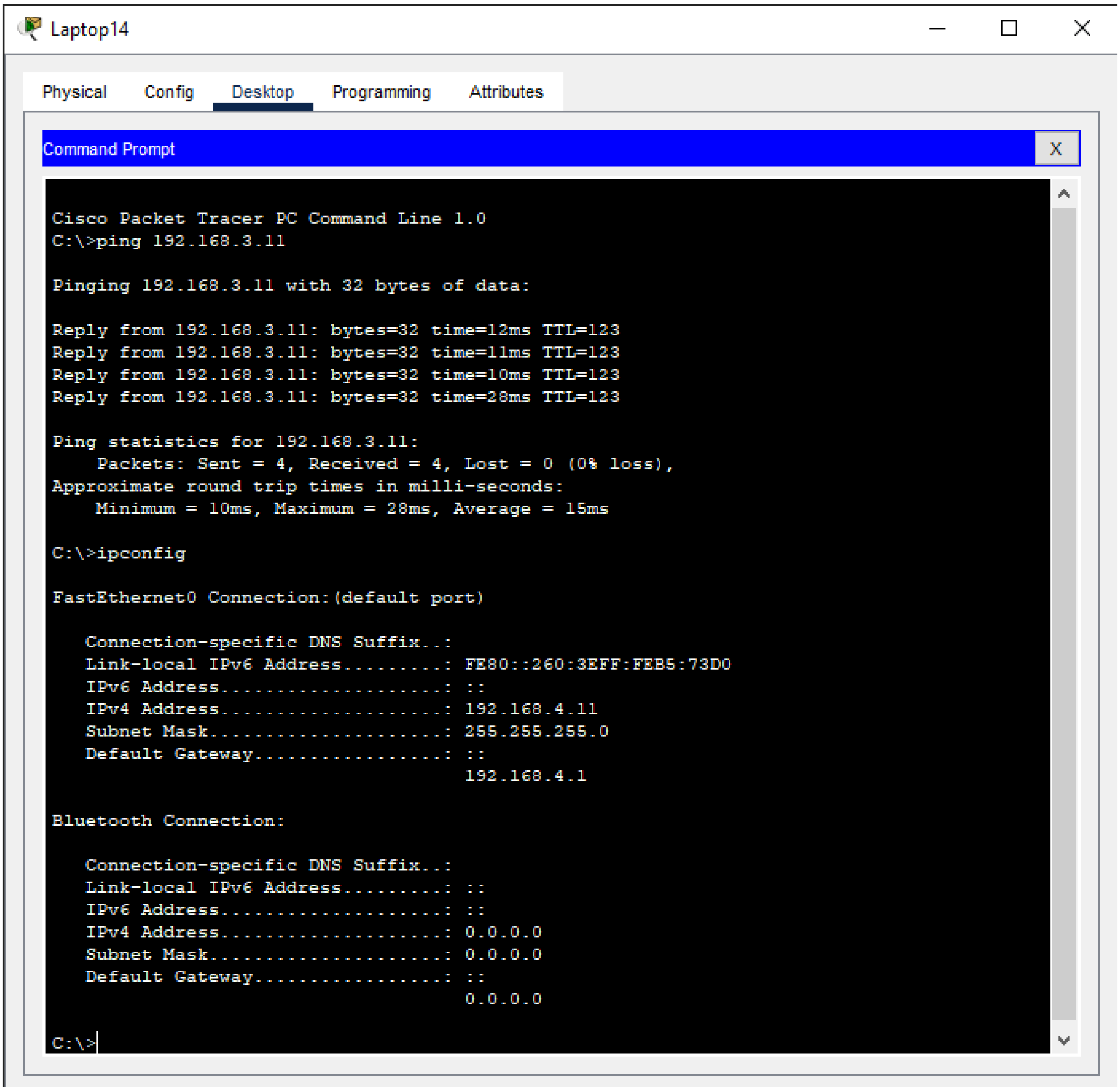
Figure 10.9

In the above figure the smart phone can communicate to ISP router and also can communicate with host of the network.

.

9.7 Testing Connectivity among the Branches:

Now let’s test the connectivity among the branches by pinging each computer form one network to another network.

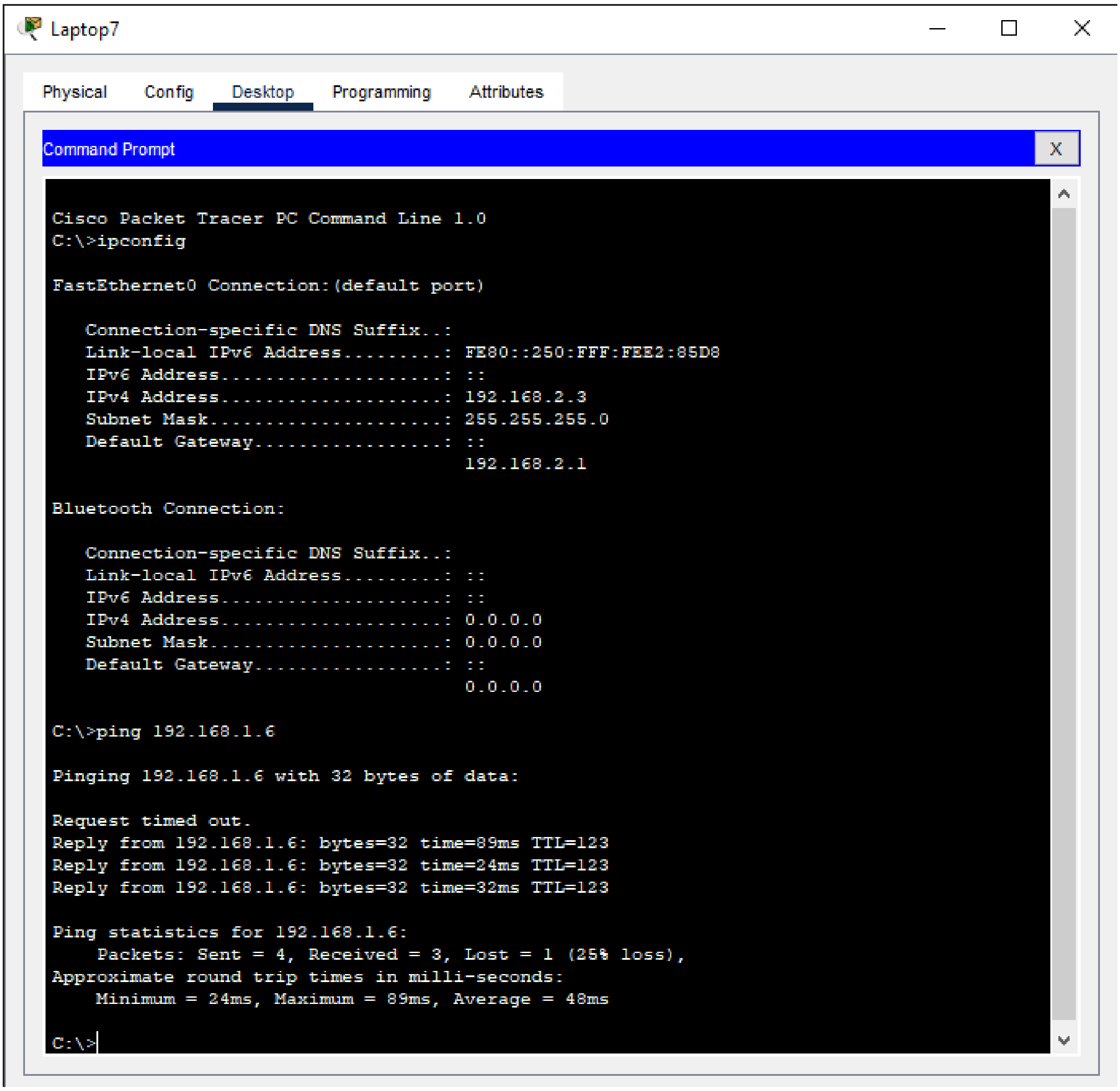


```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.3.11

Pinging 192.168.3.11 with 32 bytes of data:

Reply from 192.168.3.11: bytes=32 time=12ms TTL=123
Reply from 192.168.3.11: bytes=32 time=11ms TTL=123
Reply from 192.168.3.11: bytes=32 time=10ms TTL=123
Reply from 192.168.3.11: bytes=32 time=28ms TTL=123

Ping statistics for 192.168.3.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 28ms, Average = 15ms

C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: FE80::260:3EFF:FEB5:73D0
   IPv6 Address....................: ::
   IPv4 Address....................: 192.168.4.11
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: ::
                                     192.168.4.1

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: ::
   IPv6 Address....................: ::
   IPv4 Address....................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: ::
                                     0.0.0.0

C:\>
```

Figure 10.10

In the above figure shown that data center can successfully connect to the Lahor Branch.

Now let’s test the Karachi branch to Islamabad



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

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: FE80::250:FFF:FEE2:85D8
   IPv6 Address....................: ::
   IPv4 Address....................: 192.168.2.3
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: ::
                                     192.168.2.1

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: ::
   IPv6 Address....................: ::
   IPv4 Address....................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: ::
                                     0.0.0.0

C:\>ping 192.168.1.6

Pinging 192.168.1.6 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.6: bytes=32 time=89ms TTL=123
Reply from 192.168.1.6: bytes=32 time=24ms TTL=123
Reply from 192.168.1.6: bytes=32 time=32ms TTL=123

Ping statistics for 192.168.1.6:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 24ms, Maximum = 89ms, Average = 48ms

C:\>
```

Figure 10.11

In the above figure shown that both branches are communicating each other’s, and the connectivity is stable.

CHAPTER XII

CONCLUSION AND FUTURE WORK

11.1 Conclusion: In conclusion, this project demonstrates a comprehensive enterprise network design and implementation using Packet Tracer, showcasing the power of OSPF routing protocol in connecting diverse network components. The project successfully integrates routing, switching, WLAN, data center, and branch connectivity, ensuring seamless communication and data exchange across the network. Through this project, we have simulated a real-world network environment, highlighting the importance of careful planning, configuration, and troubleshooting in ensuring network reliability, scalability, and security. This project serves as a testament to the versatility and complexity of modern networking and paves the way for further exploration and innovation in the field.

11.2 Achievements: By doing this great project we get the following Achievements.

1. Successful Implementation of OSPF Routing Protocol: Demonstrated expertise in configuring and troubleshooting OSPF, ensuring efficient network routing and convergence.
2. Robust Network Design: Designed a comprehensive enterprise network infrastructure, incorporating routing, switching, WLAN, data center, and branch connectivity.
3. Seamless Network Connectivity: Ensured reliable communication and data exchange across the network, meeting the needs of various users and devices.
4. Network Scalability and Flexibility: Created a scalable network architecture, allowing for easy expansion and adaptation to future growth and changing network requirements.
5. Enhanced Network Security: Implemented security best practices, safeguarding the network from potential threats and vulnerabilities.
6. Development of Troubleshooting Skills: Gained hands-on experience in identifying and resolving network issues, enhancing problem-solving skills and expertise.
7. Practical Application of Networking Concepts: Successfully applied theoretical knowledge in a real-world simulation, reinforcing understanding of networking principles and concepts.
8. Improved Network Performance: Optimized network configuration, resulting in improved network performance, speed, and reliability.

11.3 Future Recommendations:

1. Multi-Protocol Integration: Explore integrating additional routing protocols, such as EIGRP or BGP, to enhance network resilience and scalability.

2. Network Automation: Investigate implementing automation tools, like Python scripting or Ansible, to streamline network configuration and management.

3. Cybersecurity Enhancements: Consider integrating advanced security measures, such as intrusion detection systems or VPNs, to bolster network defenses.

4. Network Virtualization: Explore implementing network virtualization technologies, like VLANs or SDN, to improve network segmentation and resource allocation.

5. Wireless Network Expansion: Plan for future wireless network expansions, incorporating advanced Wi-Fi technologies and mesh networking.

6. Network Performance Optimization: Conduct regular network performance analyses to identify areas for optimization and improvement.

7. Disaster Recovery Planning: Develop a comprehensive disaster recovery plan to ensure business continuity in the event of network failures or outages.

8. Regular Security Audits: Schedule regular security audits to identify vulnerabilities and ensure ongoing network security.

REFRENCES

1. CCNA 200-301 Technology workbook "IP Specialist" written by Nauman Ahmad khan, Abubakar Saeed, Uzair ahmad, Muhammad Yousaf and Afreen Moin
2. The Art of Network Architecture Business Driven Technology written by Russ White and Denis Donohue
3. CISCO CCNA Lab Guidance written by Neil Anderson