A REPORT OF SIX WEEK INDUSTRIAL TRAINING

At

SOLITAIRE INFOSYS PRIVATE LIMITED

ON

DESIGN AND IMPLEMENTATION OF HOSPITAL SYSTEM NETWORK

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE AWARD OF THE DEGREE OF

BACHELOR OF TECHNOLOGY

(Electronics and Computer Engineering)

JUNE - JULY 2024

SUBMITTED BY:

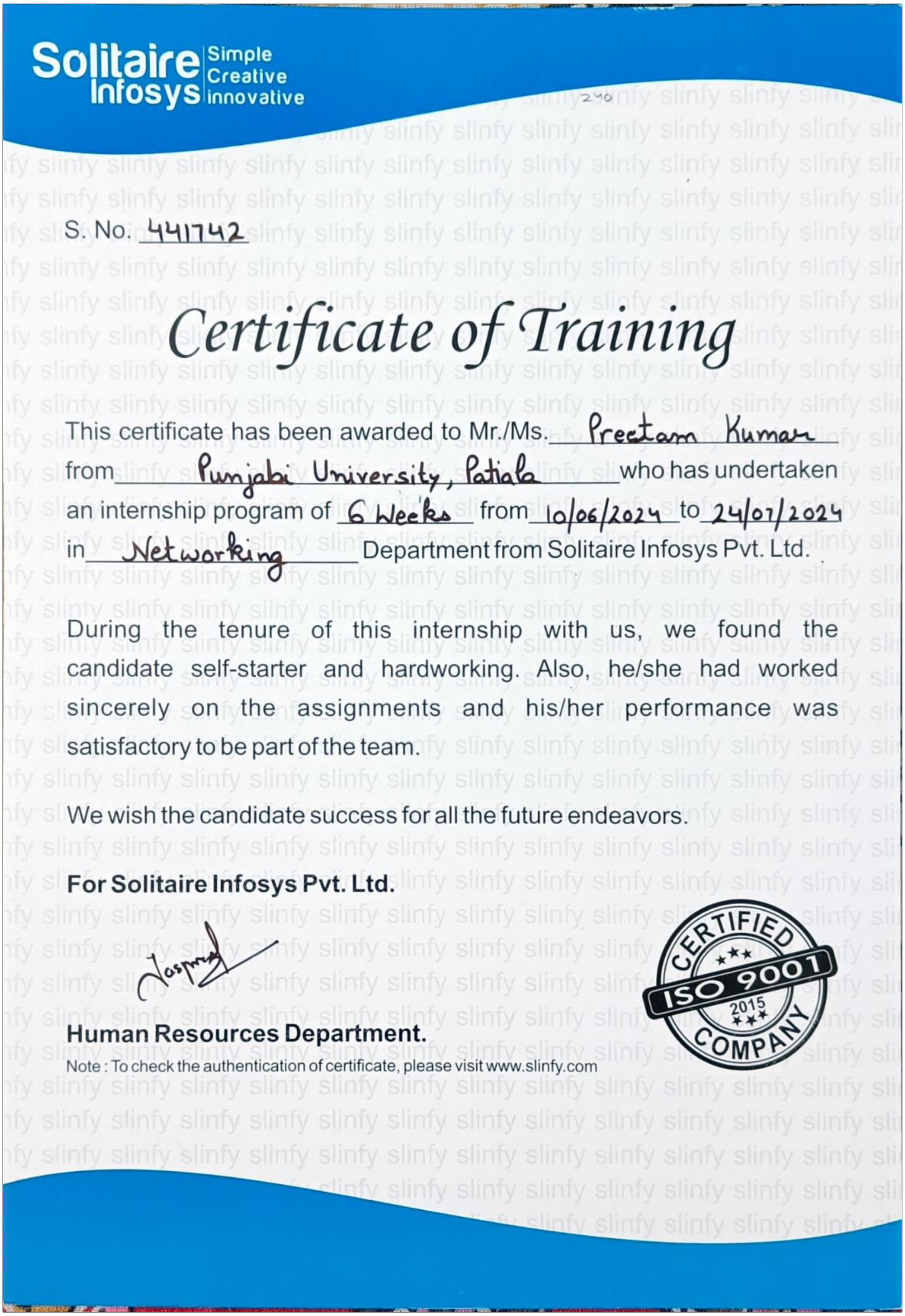
PREETAM KUMAR

12205038

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

PUNJABI UNIVERSITY, PATIALA

CERTIFICATE



Solitaire Infosys | Simple Creative innovative

290

S. No. 441742

Certificate of Training

This certificate has been awarded to Mr./Ms. Preetam Kumar from Punjabi University, Patiala who has undertaken an internship program of 6 Weeks from 10/06/2024 to 24/07/2024 in Networking Department from Solitaire Infosys Pvt. Ltd.

During the tenure of this internship with us, we found the candidate self-starter and hardworking. Also, he/she had worked sincerely on the assignments and his/her performance was satisfactory to be part of the team.

We wish the candidate success for all the future endeavors.

For Solitaire Infosys Pvt. Ltd.

Human Resources Department.

Note : To check the authentication of certificate, please visit www.slinfy.com

CERTIFIED ★★★ ISO 9001 2015 ★★★ COMPANY

CANDIDATE'S DECLARATION

I "Preetam Kumar" hereby declare that I have completed my summer training at "SOLITAIRE INFOSYS PRIVATE LIMITED" during a period from June to July under the guidance of **Ms Tamandeep.** I certify that the work which is being presented in the project entitled, Hospital System Network is an authentic record of my own work. I declare that I have worked with full dedication during these six weeks of training and my learning outcomes fulfil the requirements of training for the award of the degree of B.Tech (Electronics and Computer Engineering), Punjabi University, Patiala.

Preetam kumar

Signature of the Student

The summer training Viva-Voce Examination of___________________________________

____has been held on

____________________________________and accepted.

Signature of the Examiner

ACKNOWLEDGRMENT

"Success is a sweet fruit to which everyone strives to taste."

Regardless of how trivial or difficult a task may seem, it cannot be completed without the assistance of others. I would like to take this opportunity to express my gratitude to the people who helped me accomplish this project.

Every step of this project was a learning experience for me. In addition, it has given me the confidence to work in a professional environment. During project development, I gained experience that will serve me well in the future.

I am very happy to be a part of the training program offered by SOLITAIRE INFOSYS PRIVATE LIMITED. I sincerely thank my teacher, Ms Tamandeep, who is the trainer at Solitaire Infosys Pvt. Ltd. For his guidance, help, and motivation.

I am grateful to HOD, Electronics and Communication, Punjabi University for pursuing this training in a smooth and organized manner.

Last but not least, I would like to thank my family and the All Mighty God.

Thanks

INDEX

PART -1 INDUSTRIAL TRAINING REPORT

SOLITAIRE INFOSYS PVT. LTD.

SCO38 1ST FLOOR, SECTOR-20C, CHANDIGARH,
PUNJAB - 160020

CHAPTER 1

1.1 INTRODUCTION TO ORGANIZATION

COMPANY PROFILE

Solitaire
infosystems
Simple
Creative
innovative

The best IT service provider across the globe is SOLITAIRE INFOSYS PRIVATE LIMITED. Solitaire Infosys Pvt. Ltd. was established as a company in Mohali in 2011. Solitaire Infosys Private Limited is a Private incorporated on 06 June 2011. It is classified as Non-government Company and is registered at Registrar of Companies, Chandigarh. Solitaire Infosys Private Limited's Corporate Identification Number is (CIN) U72900CH2011PTC033013 and its registration number is 33013.Its Email address is adityajain1@gmail.com and its registered address is SCO38 FIRST FLOOR, SECTOR- 20-C CHANDIGARH CH 160020 INDIA.

Development office of Company showed as above situated at C-110, Industrial Area, Phase-VII, Mohall India. Company is limited by the shares. It is private company. Company has corporate offices in USA and India. In USA, office is situated at 24981 Owens Lake CIR Lake Forest, CA 92630-2522, USA. In Canada, the office of company is situated at Suite 208, 3474-93 Street NW, Edmonton, Alberta-T6E 6A4, Canada.

MANAGEMENT

Directors of Solitaire Infosys Private Limited are Joginder Singh and Rajesh Sharma.

VISION

Company is working for the internet generation with company's simple, creative and innovative ideas. Company visualizes becoming the most trusted and respected IT service provider across the globe with our vibrant, dynamic, and value-based IT solutions that revolve around our clients, team,and international standards.

MISSION

The mission of company is curiously strong quality of Solitaire Infosys. It prevents the sinking the feeling. It eclipses the competition.

CORE VALUES

Core values are all blue sky thinking and a raft of measures. Company aim to becomes more assiduous, zealous and value based IT service provider.

COMPANY DETAILS

Company Status	ACTIVE
R o C	R o C-Chandigarh
Registration Number	33013
Company Category	Company limited by Shares
Company Sub Category	Non-govt company
Class of Company	Private
Date of Incorporation	06 June 2011

OBJECTIVES:

Solitaire Infosys Pvt. Ltd. was established with an aim of becoming skills every single day to deliver high-quality results to clients to enhance their business, sales, leads, and ultimately, profits.

Solitaire Infosys helps enterprises, whether established or Start-up, to build and grow customer-centric digital products for mobile and web. Clients of company trust our experience of over a decade and company’s expertise that we have gained after numerous successful deliveries in various fields. Company delivers satisfactory services to our clients with an aim of helping their business in growing and reaching their organizational goals.

BUSINESS OF COMPANY

Solitaire Infosys Pvt. Ltd. is an acclaimed IT service provider contributing its part in the development of many businesses around the globe. It socializes with clients to get a superior cognizance of their business and requirements and help them in fabricating websites and applications for their business. Founded in 2011 by a dynamic duo with the same aim and zeal, it has come a long way in satisfying our clients.

Company serves clients with the world-class services for more than seven years now. The clients are delivered with the best IT solutions after we have developed a great understanding of their business and requirements. Team works on the client projects like its own and that is the reason why company holds the edge in the league.

With every project that company deliver, company deliver our respect, creativity, quality, transparency, and teamwork to our clients. Company has the experience, expertise, and capabilities to enable organizations to accelerate their service processes in every possible way. Company is known for our excellent customer satisfaction, cost-effectiveness, and innovative skills that are unparalleled.

PERFORMANCE

Company provides the UX& UI designs to clients. It has structured maintenance process to ensure enhanced performance of mobile applications. Company has support system that helps the clients with its innovative operational ideas. Company provides web development solutions. Team of company's expert professionals is proficient enough to develop every type of website for customers. Proficient app developers help clients generate return on investment and meet their business goals with highly efficient applications. It creates fresh Digital Marketing plan that will prove to be beneficial for business in generating more traffic, sales and leads. Solitaire Infosys provides processes, personnel and global expertise in application maintenance and support including best practices that enhance the value of application portfolio. Company has accomplished more than 10299 Projects, dealing with more than 1257 clients and better relation with more 980 clients. Business of company spreads around more than 24 countries.

1.2 BASIC OF NETWORKING

1.2.1 What is networking?

Networking is the practice of connecting computers and other devices to share resources and information. It is a fundamental aspect of modern computing, enabling communication and data transfer across local and global distances. This report provides an overview of networking concepts, types, topologies, devices, protocols, IP addressing, and security.

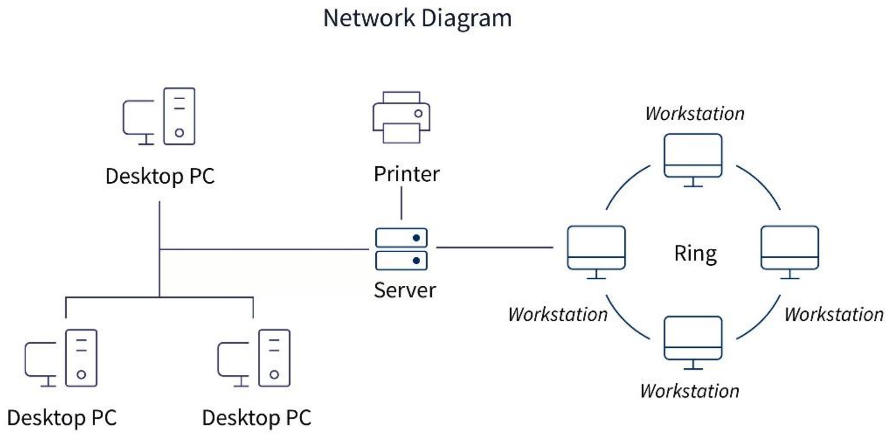


Figure 1.1 Networking

1.2.2 Types of Networks

1. Personal Area Network (PAN)
2. Local Area Network (LAN)
3. Metropolitan Area Network (MAN)
4. Wide Area Network (WAN)

1. Personal Area Network (PAN)

PAN is the most basic type of computer network. It is a type of network designed to connect devices within a short range, typically around one person. It allows your personal devices, like smartphones, tablets, laptops, and wearables, to communicate and share data with each other. PAN offers a network range of 1 to 100 meters from person to device providing communication. Its transmission speed is very high with very easy maintenance and very low cost. Examples of PAN are USB, computer, phone, tablet, printer, PDA, etc.

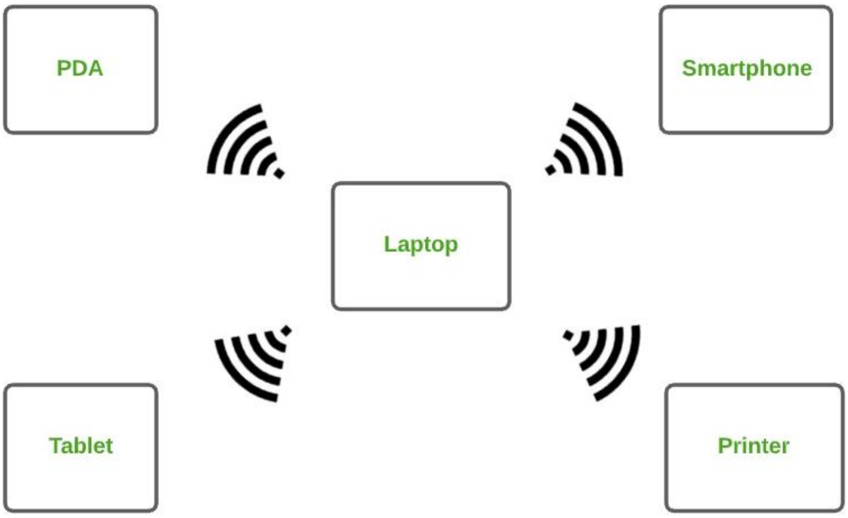


Figure 1.2 Personal Area Network

2. Local Area Network (LAN)

LAN is the most frequently used network. A LAN is a computer network that connects computers through a common communication path, contained within a limited area, that is, locally. A LAN encompasses two or more computers connected over a server. The two important technologies involved in this network are Ethernet and Wi-Fi. It ranges up to 2km & transmission speed is very high with easy maintenance and low cost. Examples of LAN are networking in a home, school, library, laboratory, college, office, etc.

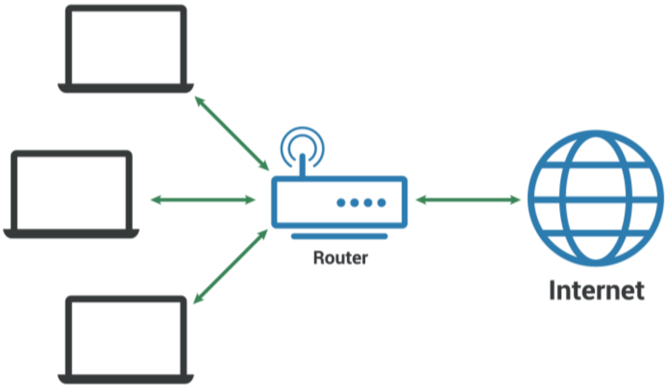


Figure 1.3 Local Area Network

3. Metropolitan Area Network (MAN)

A MAN is larger than a LAN but smaller than a WAN. This is the type of computer network that connects computers over a geographical distance through a shared communication path over a city, town, or metropolitan area. This network mainly uses FDDI, CDDI, and ATM as the technology with a range from 5km to 50km. Its transmission speed is average. It is difficult to maintain and it comes with a high cost. Examples of MAN are networking in towns, cities, a single large city, a large area within multiple buildings, etc.

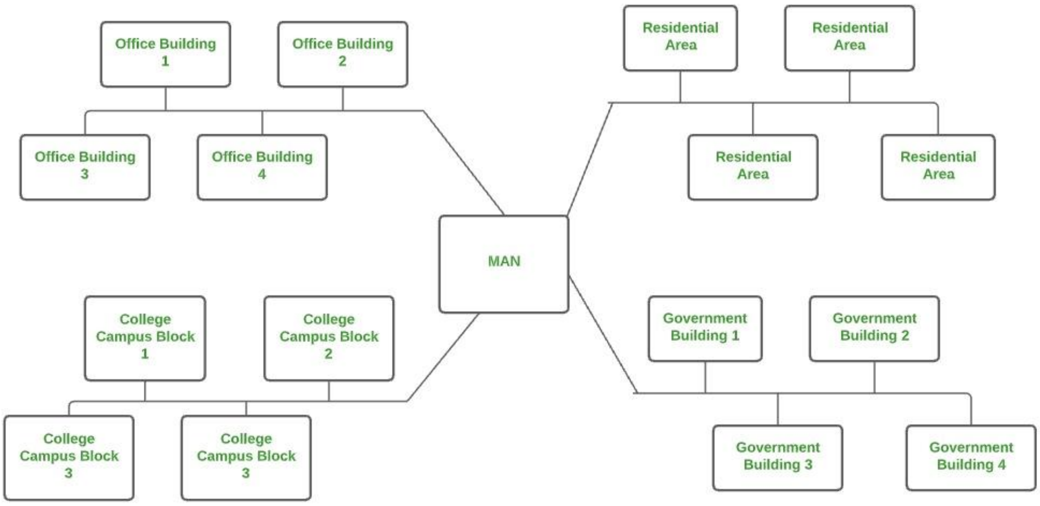


Figure 1.4 Metropolitan Area Network

4. Wide Area Network (WAN)

WAN is a type of computer network that connects computers over a large geographical distance through a shared communication path. It is not restrained to a single location but extends over many locations. WAN can also be defined as a group of local area networks that communicate with each other with a range above 50km. Here we use Leased-Line & Dial-up technology. Its transmission speed is very low and it comes with very high maintenance and very high cost. The most common example of WAN is the Internet.

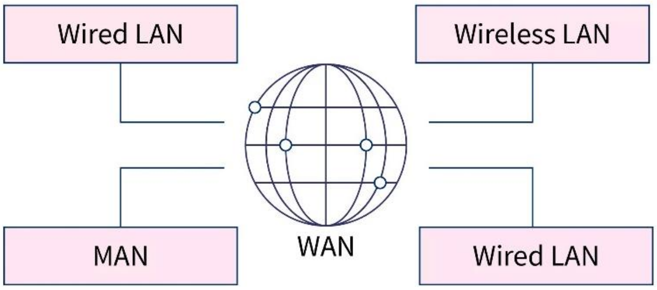


Figure 1.5 Wide Area Network

1.2.3 Network Devices

Hardware devices that are used to connect computers, printers, fax machines and other electronic devices to a network are called network devices. These devices transfer data in a fast, secure and correct way over same or different networks.

– HUB

A hub is a basic networking device that connects multiple Ethernet devices, making them act as a single network segment. Hubs transmit data to all connected devices, regardless of the destination, which can lead to data collisions. Hubs operate at the physical layer (Layer 1) of the OSI model and do not differentiate between the source and destination of data packets. Because of their simplicity and the potential for collisions, hubs are largely obsolete and have been replaced by switches in modern networks. However, they can still be found in small, simple networks where network performance is not a critical concern.

Figure 1.6 Hub

– SWITCHES

A switch is a device that connects network devices and manages node-to-node communication across a network, making sure that data packets reach their intended destination. Unlike routers, which send information between networks, switches send information between nodes within a network. Switches operate at the data link layer (Layer 2) of the OSI model and use MAC addresses to forward data to the correct destination.

Figure 1.7 Switch

– ROUTERS

A router is a physical or virtual device that sends data “packets” between networks. Routers analyse the data within packets to determine the best transmission path and use sophisticated routing algorithms to forward data packets until they reach their destination node. Routers operate at the network layer (Layer 3) of the OSI model, making decisions based on IP addresses.

Figure 1.8 Router

– GATEWAYS

A gateway is a network node that connects two different networks, often with different protocols, and translates data formats, ensuring compatibility and communication between them. Gateways are critical for integrating diverse networks and systems. They operate at various layers of the OSI model, depending on the functionality required, and can perform tasks such as protocol conversion, data encapsulation, and network address translation.

Figure 1.9 Gateway

– Access Points (AP)

An access point is a device that allows wireless devices to connect to a wired network using Wi-Fi. Access points extend the range of a wireless network, enabling more devices to connect without the need for additional cabling.

Figure 1.10 Access Point

1.2.4 Key components

- **Ports:**
  Ports are logical endpoints used by networking protocols to distinguish different types of traffic sent to a device. Each port is associated with a specific protocol or application, identified by a port number ranging from 0 to 65535. For example, HTTP uses port 80, while HTTPS uses port 443.

- **Nodes**
- A node is a network connection point that can receive, send, create, or store data. It’s essentially any network device—computers, printers, modems, bridges, or switches—that can recognize, process, and transmit information to another network node. Each node requires some form of identification (such as an IP or MAC address) to receive access to the network.

- **Ping**
  Ping is a network utility used to test the reachability of a host on an IP network and measure the round-trip time for messages sent from the source to the destination.

- **Protocols**
  Protocols are rules that define how computers interact with each other in a network to exchange data. Examples includes TCP/IP, HTTP, SMTP, and DNS.

- **DNS (Domain Name System)**
  DNS is a system that translates human-readable domain names (e.g., www.example.com) into IP addresses that computers use to identify each other on the network.

- **Network Topologies**
  Network topologies refer to the layout or structure of the network. Common topologies Include star, ring, bus, mesh, and hybrid topologies.

- **Internet**
  The internet is a global network of interconnected networks, providing access to information, services, and communication worldwide.

1.2.5 IP Address

An IP address is a unique identifier assigned to each device connected to a network, enabling them to communicate with each other. There are two versions of IP addresses:

- **IPv4:** Composed of four sets of numbers separated by periods (e.g., 192.168.1.1). It uses 32-bit addresses, allowing for about 4.3 billion unique addresses.

- **IPv6:** Composed of eight groups of hexadecimal numbers separated by colons (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334). It uses 128-bit addresses, allowing for a vastly larger number of unique addresses.

1.2.6 IP address classes

Class	From	To
A	0.0.0.0	127.255.255.255
B	128.0.0.0	191.255.255.255
C	192.0.0.0	223.255.255.255
D	224.0.0.0	239.255.255.255
E	240.0.0.0	255.255.255.255

Table 1.1 IP address class

1.2.7 Subnet Mask

A subnet mask is a 32-bit number created by setting hosts bits to all 0s and setting network bits to all 1s.

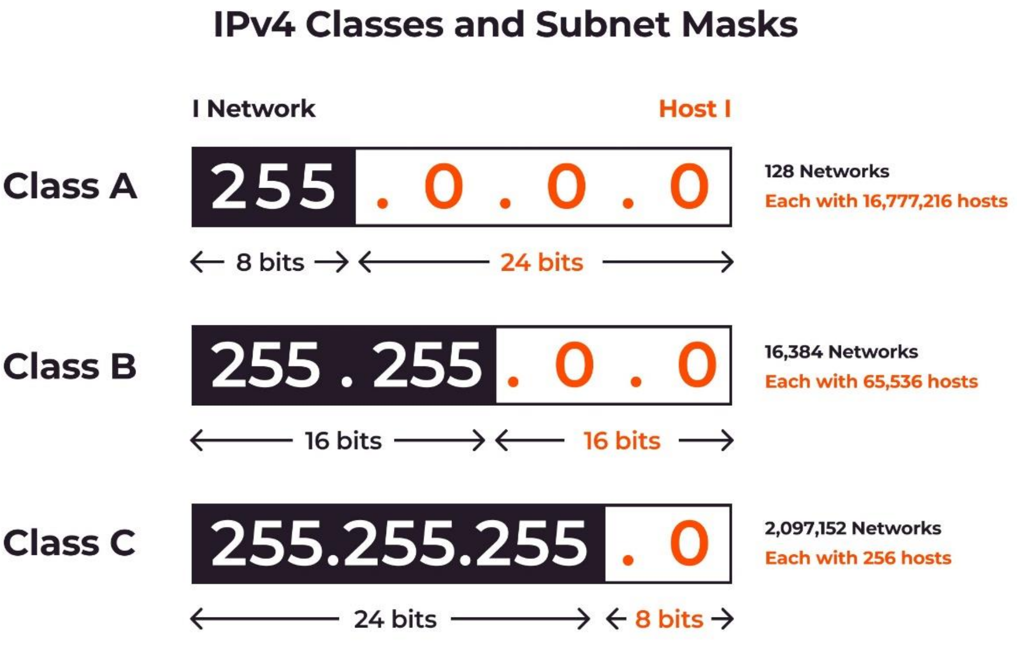


Figure 1.11

1.2.8 OSI Reference Model

The **Open Systems Interconnection (OSI) model** was developed by the **International Organization for Standardization (ISO),** and formalized in 1984. It provided the first framework governing how information should be sent across a network.

The OSI model consists of seven layers, each corresponding to a specific network function:

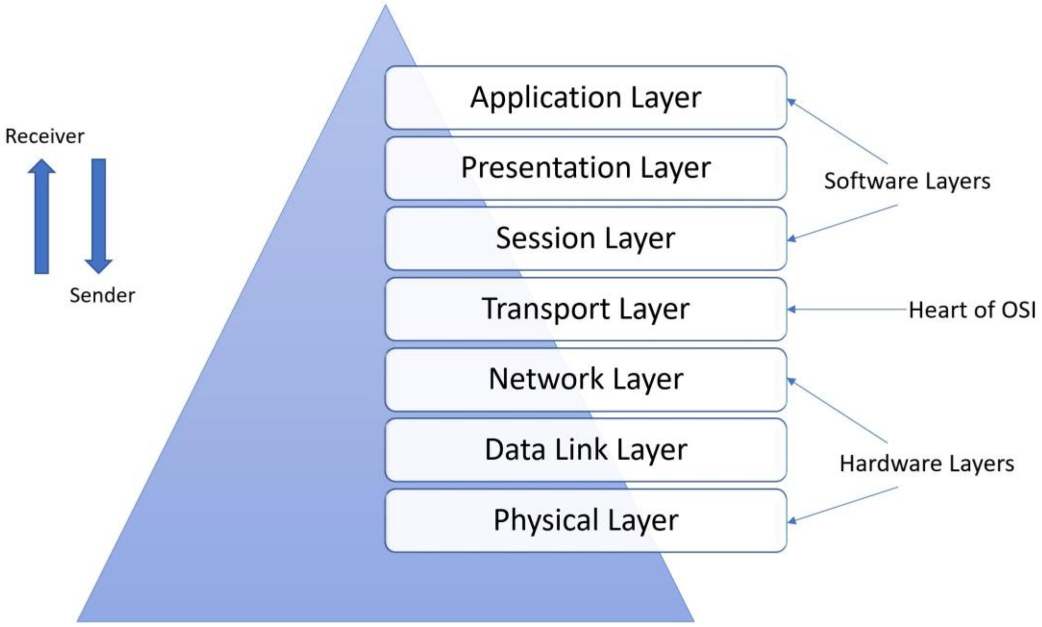


Figure 1.12 OSI Model

OSI Model - The Upper Layers

The top three layers of the OSI model are often referred to as the **upper layers:**

- Layer-7 - **Application** layer
- Layer-6 - **Presentation** layer
- Layer-5 - **Session** layer

Protocols that operate at these layers manage application-level functions, and are generally implemented in *software.*

The function of the upper layers of the OSI model can be difficult to visualize. Upper layer protocols do not always fit perfectly within a layer, and often function across multiple layers.

OSI Model - The Application Layer

The Application layer (Layer-7) provides the interface between the user application and the network. A web browser and an email client are examples of user applications.

The user application itself *does not* reside at the Application layer – the *protocol* does. The user interacts with the application, which in turn interacts with the application protocol.

Examples of Application layer protocols include:

- **FTP**, via an FTP client
- **HTTP**, via a web browser
- **POP3** and **SMTP**, via an email client
- **Telnet**

The Application layer provides a variety of functions:

- Identifies communication partners
- Determines resource availability
- Synchronizes communication

The Application layer interacts with the Presentation layer below it. As it is the top-most layer, it does not interact with any layers above it.

OSI Model - The Presentation Layer

The Presentation layer (Layer-6) controls the *formatting* and *syntax* of user data for the application layer. This ensures that data from the *sending* application can be understood by the *receiving* application.

Standards have been developed for the formatting of data types, such as text, images, audio, and video. Examples of Presentation layer formats include:

- **Text** - RTF, ASCII, EBCDIC
- **Images** - GIF, JPG, TIF
- **Audio** - MIDI, MP3, WAV
- **Movies** - MPEG, AVI, MOV

If two devices do not support the same format or syntax, the Presentation layer can provide **conversion** or **translation** services to facilitate communication.

Additionally, the Presentation layer can perform **encryption** and **compression** of data, as required. However, these functions can also be performed at lower layers as well. For example, the Network layer can perform encryption, using IPSec.

OSI Model - The Session Layer

The **Session layer (Layer-5)** is responsible for establishing, maintaining, and ultimately terminating *sessions* between devices. If a session is *broken*, this layer can attempt to recover the session.

Sessions communication falls under one of three categories:

- **Full-Duplex** – simultaneous two-way communication
- **Half-Duplex** – two-way communication, but not simultaneous
- **Simplex** – one-way communication

Many modern protocol suites, such as TCP/IP, do not implement Session layer protocols. Connection management is often controlled by lower layers, such as the Transport layer.

The lack of true Session layer protocols can present challenges for high-availability and failover. Reliance on lower-layer protocols for session management offers less flexibility than a strict adherence to the OSI model.

OSI Model - The Lower Layers

The bottom four layers of the OSI model are often referred to as the **lower layers**:

- Layer-4 – **Transport** layer
- Layer-3 – **Network** layer
- Layer-2 – **Data-Link** layer
- Layer-1 – **Physical** layer

Protocols that operate at these layers control the end-to-end transport of data between devices, and are implemented in both software and hardware.

OSI Model - The Transport Layer

The **Transport layer (Layer-4)** does not actually send data, despite its name. Instead, this layer is responsible for the *reliable* transfer of data, by ensuring that data arrives at its destination error-free and in order.

Transport layer communication falls under two categories:

- **Connection-oriented** – requires that a connection with specific agreed-upon parameters be established before data is sent.
- **Connectionless** – requires no connection before data is sent.

Connection-oriented protocols provide several important services:

- **Segmentation and sequencing** – data is segmented into smaller pieces for transport. Each segment is assigned a *sequence number*, so that the receiving device can reassemble the data on arrival.
- **Connection establishment** – connections are established, maintained, and ultimately terminated between devices.
- **Acknowledgments** – receipt of data is confirmed through the use of *acknowledgments*. Otherwise, data is retransmitted, guaranteeing delivery.
- **Flow control** (or **windowing**) – data transfer rate is negotiated to prevent congestion.

The TCP/IP protocol suite incorporates two Transport layer protocols:

- **Transmission Control Protocol (TCP) –** connection-oriented
- **User Datagram Protocol (UDP) –** connectionless

OSI Model - The Network Layer

The **Network layer (Layer-3)** controls internetwork communication, and has two key responsibilities:

- **Logical addressing –** provides a unique address that identifies both the host, and the network that host exists on.
- **Routing –** determines the best path to a particular destination network, and then routes data accordingly.

Two of the most common Network layer protocols are:

- **Internet Protocol (IP)**
- Novell's **Internetwork Packet Exchange (IPX).**

IPX is almost entirely deprecated. IP version 4 (IPv4) and IP version 6 (IPv6) are covered in nauseating detail in other guides.

OSI Model - The Data-Link Layer

While the Network layer is concerned with transporting data between networks, the **Data-Link layer (Layer-2)** is responsible for transporting data *within* a network.

The Data-Link layer consists of two sublayers:

- **Logical Link Control (LLC)** sublayer
- **Media Access Control (MAC)** sublayer

The LLC sublayer serves as the intermediary between the physical link and all higher layer protocols. It ensures that protocols like IP can function regardless of what type of physical technology is being used.

Additionally, the LLC sublayer can perform flow-control and error checking, though such functions are often provided by Transport layer protocols, such as TCP.

The MAC sublayer controls access to the physical medium, serving as mediator if multiple devices are competing for the same physical link. Datalink layer technologies have various methods of accomplishing this - **Ethernet** uses *Carrier Sense Multiple Access with Collision Detection (CSMA/CD),* and **Token Ring** utilizes a token.

OSI Model - The Physical Layer

The **Physical layer (Layer-1)** controls the signalling and transferring of raw bits onto the physical medium. The Physical layer is closely related to the Data-link layer, as many technologies (such as Ethernet) contain both datalink and physical functions.

The Physical layer provides specifications for a variety of hardware:

- Cabling
- Connectors and transceivers
- Network interface cards (NICs)
- Wireless radios
- Hubs

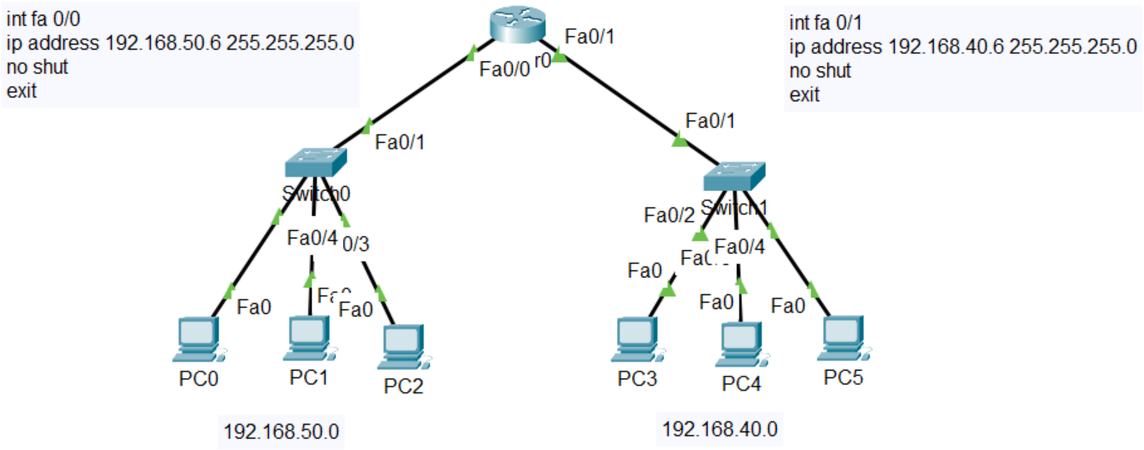
1.3 BASIC CONFIGURATIONS

1.3.1 Router-Switch configuration

To configure router with switch, use a copper-straight-through wire.

Open command-line-interface (CLI) of router and write following commands:-

```
~  enable
~  configure terminal
~  interface fastEthernet 0/0
~  ip address <IP address> <subnet mask>
~  no shutdown
~  exit
```



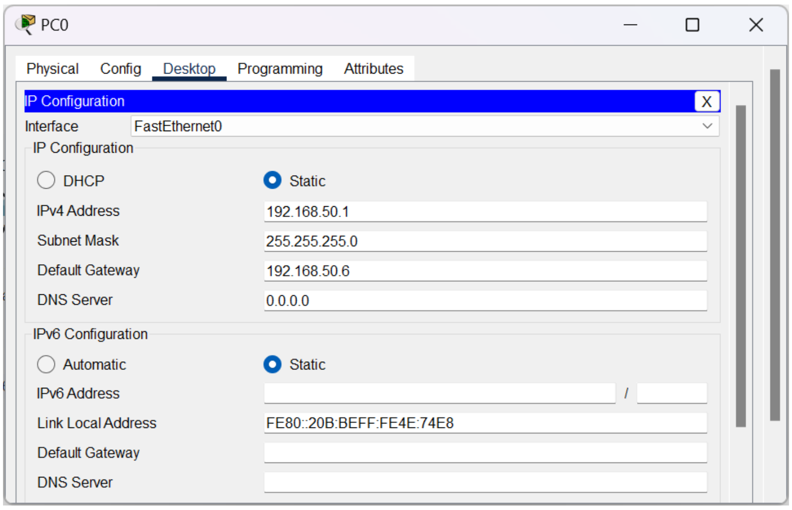
```
int fa 0/0
ip address 192.168.50.6 255.255.255.0
no shut
exit
```

```
int fa 0/1
ip address 192.168.40.6 255.255.255.0
no shut
exit
```

Figure 1.13

1.3.2 How to give IP-address to pc

- Click on PC.
- Go to desktop.
- Click on IP configuration.



Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address: 192.168.50.1

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.50.6

DNS Server: 0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::20B:BEFF:FE4E:74E8

Default Gateway:

DNS Server:

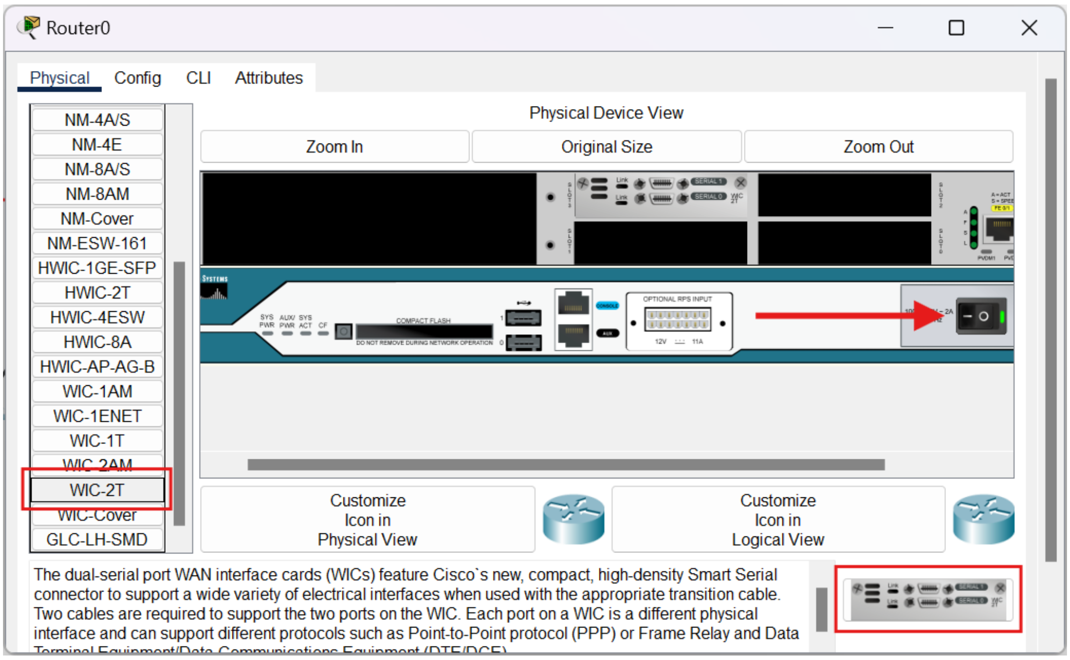
Figure 1.14

1.3.3 Router-Router configuration

- To configure one router to another, use serial DTE wire.
- Before connecting wires, add serial port to the router.

How to add serial port to router?

- Click on router.
- Switch off the router.
- Select WIC-2T from modules panel and add to router.
- Switch on the router.

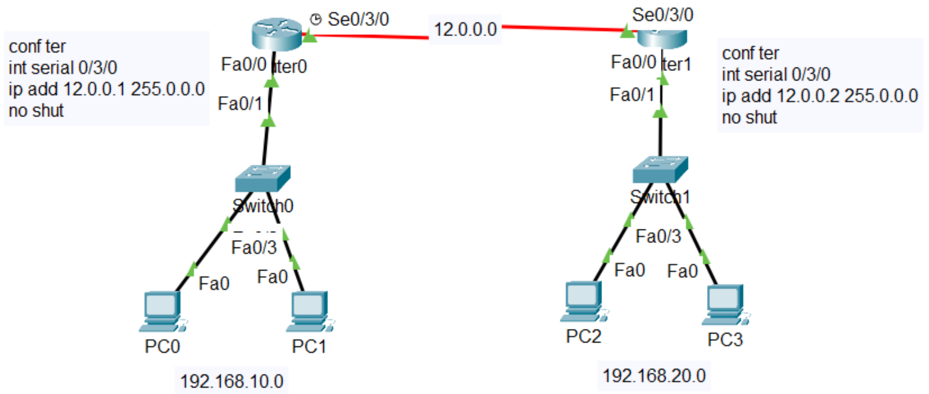


The dual-serial port WAN interface cards (WICs) feature Cisco`s new, compact, high-density Smart Serial connector to support a wide variety of electrical interfaces when used with the appropriate transition cable. Two cables are required to support the two ports on the WIC. Each port on a WIC is a different physical interface and can support different protocols such as Point-to-Point protocol (PPP) or Frame Relay and Data Terminal Equipment/Data Communications Equipment (DTE/DCE)

Figure 1.14

Configuration commands:-

```
~  Enable
~  configure terminal
~  Interface serial 0/3/0
~  ip address <IP address> <subnet mask>
~  no shutdown
```



```
conf ter
int serial 0/3/0
ip add 12.0.0.1 255.0.0.0
no shut
```

```
conf ter
int serial 0/3/0
ip add 12.0.0.2 255.0.0.0
no shut
```

Figure 1.15

1.3.4 Some common commands:-

Write	for saving configuration
Show run	to check the configuration
Show ip interface brief	to view a summary of router interfaces
Note :- ▪ If router is in configuration mode, use ‘do’ before these commands. ▪ For removing/deleting any command use ‘no’ before commands.	

1.3.5 Password on Router

– **Commands**

```
~  conf ter
~  enable password <password>
```

1.3.6 Hostname

– **Commands**

```
~  conf ter
~  hostname <name>
```

1.4 ROUTING FUNDAMENTALS

1.4.1 IP Routing: Default, Static, and Dynamic Routing

Introduction

IP routing is the process by which data packets are forwarded from one network to another to reach their destination. It's the backbone of the internet, ensuring seamless communication between devices across the globe. This chapter explores the fundamental routing types: default, static, and dynamic, as well as the role of routing protocols.

1.4.1.1 Default Routing

- **Definition:** Default routing involves configuring a single route on a router to send all packets destined for networks not explicitly defined in the routing table. This route is often referred to as the "default gateway."
- **Purpose:** Simplifies router configuration, providing a fallback route for unknown destinations.
- **Usage:** Commonly used in small networks or as a temporary solution.
- **Limitations:** Offers minimal control over traffic flow, potentially impacting performance and security if not used judiciously.

1.4.1.2 Static Routing

- **Definition:** Static routing requires manual configuration of routes by a network administrator. Specific routes to destination networks are defined within the router's configuration.
- **Purpose:** Provides precise control over traffic flow, often used in small, stable networks or for critical links.
- **Advantages:** Predictable traffic flow, increased security.
- **Disadvantages:** Time-consuming configuration, scalability challenges in large networks, requires manual updates for network changes.

1.4.1.3 Dynamic Routing

- **Definition:** Dynamic routing protocols allow routers to automatically learn and exchange network topology information with neighbouring routers. Routing tables are updated dynamically based on network changes.
- **Purpose:** Simplifies network management, enhances scalability, and provides adaptability to network changes.
- **Types:**
  - **Interior Gateway Protocols (IGPs):** Used within an autonomous system. Examples include RIP, IGRP, OSPF, and EIGRP.
  - **Exterior Gateway Protocols (EGPs):** Used between autonomous systems. The most prominent example is BGP.
- **Advantages:** Scalability, adaptability, reduced administrative overhead.

- **Disadvantages:** Increased network complexity, potential for routing loops or convergence issues.

1.4.2 Routing Protocols

Routing protocols are essential for dynamic routing, enabling routers to automatically learn about network topology changes and update their routing tables accordingly.

1.4.2.1 Static Routing

– **Configuring Static Route**

~
```
ip route <Destination Network ID> <Destination Subnet Mask> <Next-hop IP address
>
```

– **Practical**

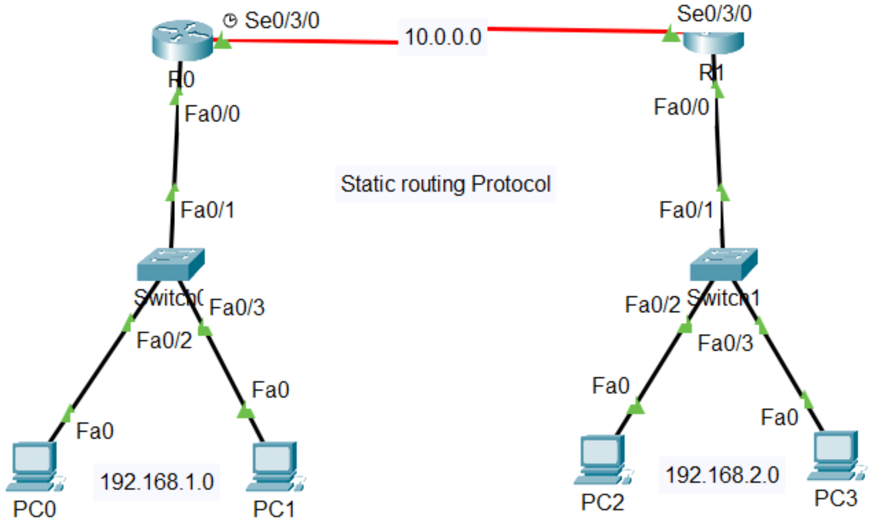


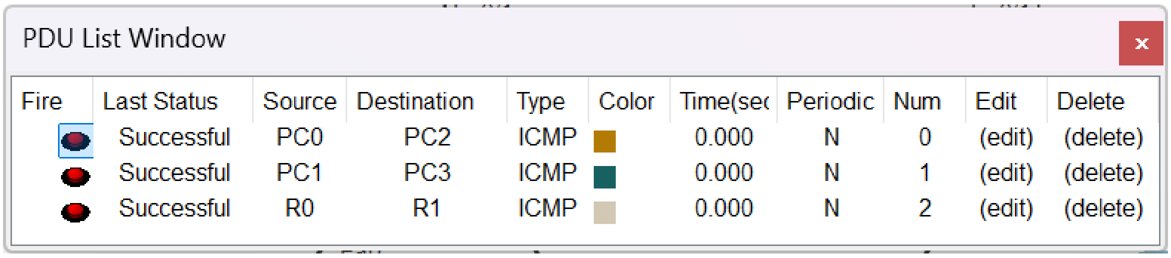
Figure 1.16

Configuring static route on R0

```
R0(config)# ip route 192.168.2.0 255.255.255.0 10.0.0.2
```

Configuring static route on R1

```
R1(config)# ip route 192.168.1.0 255.255.255.0 10.0.0.1
```



Fire	Last Status	Source	Destination	Type	Color	Time(sec	Periodic	Num	Edit	Delete
●	Successful	PC0	PC2	ICMP	🟫	0.000	N	0	(edit)	(delete)
●	Successful	PC1	PC3	ICMP	🟩	0.000	N	1	(edit)	(delete)
●	Successful	R0	R1	ICMP	⬜	0.000	N	2	(edit)	(delete)

Figure 1.17

1.4.2.2 RIP (Routing Information Protocol)

RIP stands for **Routing Information Protocol**, which is a specific type of *dynamic routing protocol* used in networking. It's designed to exchange routing information between routers within an autonomous system. Max Hop counts: 15

However, there are different *versions* of RIP:

- **RIPv1:** The original version, which is classful and has limitations like lack of subnet mask support.
- **RIPv2:** An improved version that is classless and supports subnet masks, VLSM, and authentication.

– **Configuring RIP v1**

```
~ Router(config)# router rip
~ Router(config-router)# network <Network ID>
```

– **Configuring RIP v2**

```
~ Router(config)# router rip
~ Router(config-router)# network <Network ID>
~ Router(config-router)# version 2
```

Loopback?

You use the loopback interface to identify the device. While you can use any interface address to determine if the device is online, the loopback address is the preferred method.

– **Configuring loopback**

```
~ Router(config)# int loopback <0-2147483647>
~ Router(config-router)# ip address <IP address> <subnet mask>
```

– **Practical**

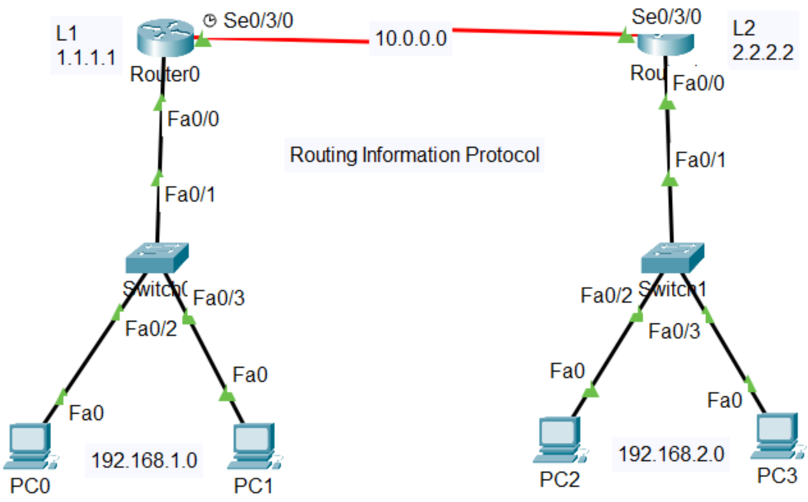


Figure 1.18

Configuring ripv1 on R0

```
~  Router(config)#router rip
~  Router(config-router)#net 1.1.1.1
~  Router(config-router)#net 10.0.0.0
~  Router(config-router)#net 192.168.1.0
```

Configuring ripv1 on R1

```
~  Router(config)#router rip
~  Router(config-router)#net 2.2.2.2
~  Router(config-router)#net 10.0.0.0
~  Router(config-router)#net 192.168.2.0
```

Configuring ripv2 on R0

```
~  Router(config)#router rip
~  Router(config-router)#version 2
~  Router(config-router)#net 1.1.1.1
~  Router(config-router)#net 10.0.0.0
~  Router(config-router)#net 192.168.1.0
```

Configuring ripv2 on R1

```
~  Router(config)#router rip
~  Router(config-router)#version 2
~  Router(config-router)#net 2.2.2.2
~  Router(config-router)#net 10.0.0.0
~  Router(config-router)#net 192.168.2.0
```

1.4.2.3 EIGRP: Enhanced Interior Gateway Routing Protocol

EIGRP is a hybrid routing protocol, combining elements of both distance-vector and link-state protocols. It's known for its efficiency, scalability, and rapid convergence. Max Hop count is 255 (100 by default).

- **Configuring EIGRP**

```
~  Router(config)# router eigrp <as no>
~  Router(config-router)# network <Network ID>
```

- **Practical**

Configuring EIGRP on all routers

***On Router1**

```
~  Router(config)# router eigrp 10
~  Router(config-router)# net 16.0.0.0
```

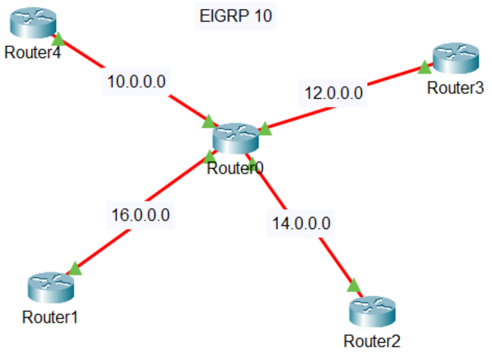


Figure 1.19

***On Router2**

```
~  Router(config)# router eigrp 10
~  Router(config-router)# net 14.0.0.0
```

***On Router3**

```
~  Router(config)# router eigrp 10
~  Router(config-router)# net 12.0.0.0
```

***On Router4**

```
~  Router(config)# router eigrp 10
~  Router(config-router)# net 10.0.0.0
```

***On Router0**

```
~  Router(config)# router eigrp 10
~  Router(config-router)# net 10.0.0.0
~  Router(config-router)# net 12.0.0.0
~  Router(config-router)# net 14.0.0.0
~  Router(config-router)# net 16.0.0.0
```

1.4.2.4 OSPF: Open Shortest Path First

OSPF is a link-state routing protocol primarily used for IP networks. It's considered one of the most robust and scalable Interior Gateway Protocols (IGPs).

– **Configuring OSPF**

```
~  Router(config)# router ospf <process - id>
~  Router(config-router)# network <Network ID> <wildcard mask>
   area <area id>
```

Wildcard mask

A wildcard mask is a 32-bit binary number used to specify a range of IP addresses. It's essentially an inverted subnet mask.

Example	
Subnet Mask	Wildcard Mask
255.255.255.0	0.0.0.255
255.255.0.0	0.0.255.255
255.255.252.0	0.0.3.255
255.240.0.0	0.15.255.255

Table 1.2

➢ OSPF with different areas

– **Practical**

Configuring OSPF on all routers

***On Router1**

```
~  Router(config)# router ospf 10
~  Router(config-router)# net 10.0.0.0 0.255.255.255 area 1
~  Router(config-router)# net 11.0.0.0 0.255.255.255 area 0
```

*On Router3

```
~  Router(config)# router ospf 10
~  Router(config-router)# net 10.0.0.0 0.255.255.255 area 1
```

*On Router2

```
~  Router(config)# router ospf 10
~  Router(config-router)# net 13.0.0.0 0.255.255.255 area 2
~  Router(config-router)# net 12.0.0.0 0.255.255.255 area 0
```

*On Router4

```
~  Router(config)# router ospf 10
~  Router(config-router)# net 13.0.0.0 0.255.255.255 area 2
```

*On Router0

```
~  Router(config)# router ospf 10
~  Router(config-router)# net 11.0.0.0 0.255.255.255 area 0
~  Router(config-router)# net 12.0.0.0 0.255.255.255 area 0
```

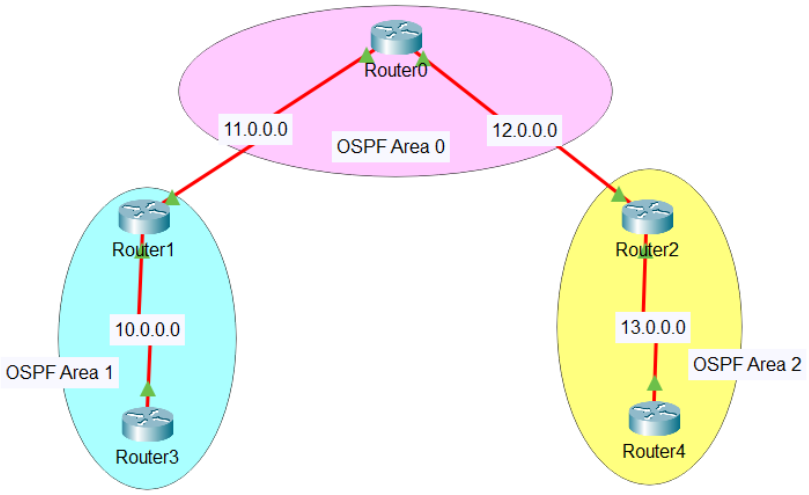
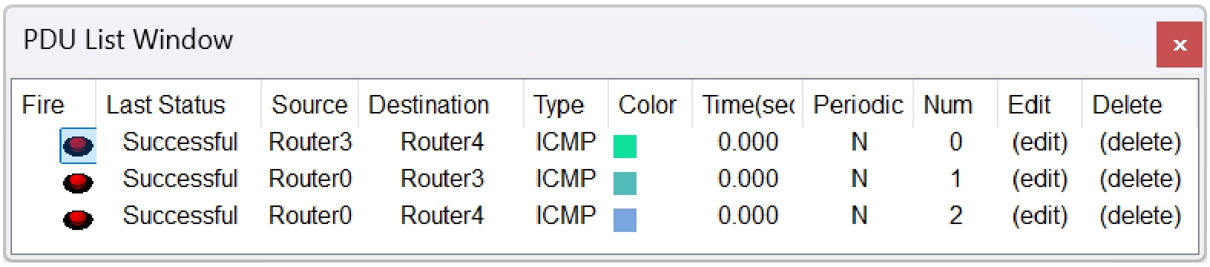


Figure 1.20



PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec	Periodic	Num	Edit	Delete
●	Successful	Router3	Router4	ICMP	🟩	0.000	N	0	(edit)	(delete)
●	Successful	Router0	Router3	ICMP	🟩	0.000	N	1	(edit)	(delete)
●	Successful	Router0	Router4	ICMP	🟦	0.000	N	2	(edit)	(delete)

Figure 1.21

1.4.3 Redistribution

Redistribution is the process of sharing routing information between different routing protocols. This allows routers running multiple protocols to exchange route information, creating a unified routing domain.

- **Commands**

```
~ Router(config)# router <routing protocol>
~ Router(config-router)# redistribute ?
```

Note: - with '?', you know what to do next and every protocol has a different command.

1.4.3.1 Rip – Eigrp

- **Configuration on Router0**

```
~ Router(config)# router rip
~ Router(config-router)# redistribute eigrp 10 metric 1
~ exit
~ Router(config)# router eigrp 10
~ Router(config-router)# redistribute rip metric 1000 1 255 1
  1000
```

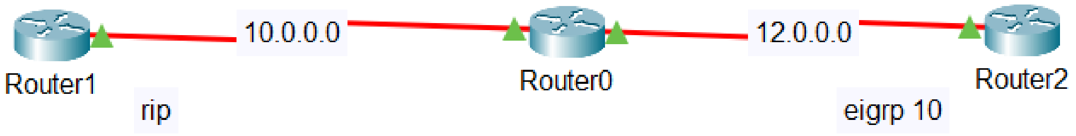


Figure 1.22

1.4.3.2 Rip – OSPF

- **Configuration on Router0**

```
~ Router(config)# router rip
~ Router(config-router)# redistribute ospf 10 metric 1
~ exit
~ Router(config)# router ospf 10
~ Router(config-router)# redistribute rip metric 1000 subnets
```

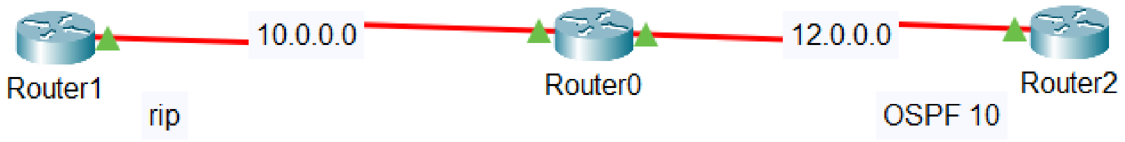


Figure 1.23

1.4.3.3 Eigrp – OSPF

- **Configuration on Router0**

```
~ Router(config)# router ospf 10
~ Router(config-router)# redistribute eigrp 10 subnets
~ exit
~ Router(config)# router eigrp 10
~ Router(config-router)# redistribute ospf 10 metric 1000 1 255
  1 1000
```

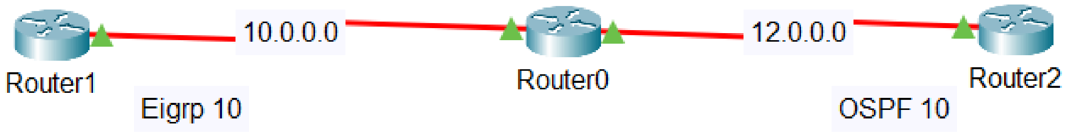


Figure 1.24

1.5 SWITCHING

1.5.1 What is switching

Switching is a fundamental concept in computer networks that allows for efficient data transfer between devices. Unlike hubs, which simply broadcast data packets to all connected devices, switches use Media Access Control (MAC) addresses to intelligently forward packets only to the intended recipient.

1.5.2 Trunking

Trunking, also known as link aggregation, is a networking technology that combines multiple physical links into a single logical link. This technique increases bandwidth, improves fault tolerance, and provides redundancy for critical network connections.

- Switch to switch configuration

```
~ Switch(config)# int fa <port no.>
~ Switch(config-if)# switchport mode trunk
```

1.5.3 VLAN: Virtual Local Area Network

A Virtual Local Area Network (VLAN) is a logical grouping of devices on a physical network that functions as if they were on a separate network segment. VLANs segment a network based on logical criteria like department, function, or security needs, rather than physical location.

- **Commands**

```
~ Switch(config)# vlan <1-4094>
~ Switch(config-vlan)# name <name>
~ Switch(config-vlan)# ex
~ Switch(config)# int fa <port no.>
~ Switch(config-if)# switchport access vlan <1-4094>
```

- **Practical**

  ***On Switch0 & Switch1**

```
~ Switch(config)# vlan 10
~ Switch(config-vlan)# name IT
~ Switch(config-vlan)# ex
~ Switch(config)# int fa 0/2
~ Switch(config-if)# switchport access vlan 10
~ Switch(config-if)# ex

~ Switch(config)# vlan 20
~ Switch(config-vlan)# name CSE
~  Switch(config-vlan)# ex
~  Switch(config)# int fa 0/3
~  Switch(config-if)# switchport access vlan 20
```

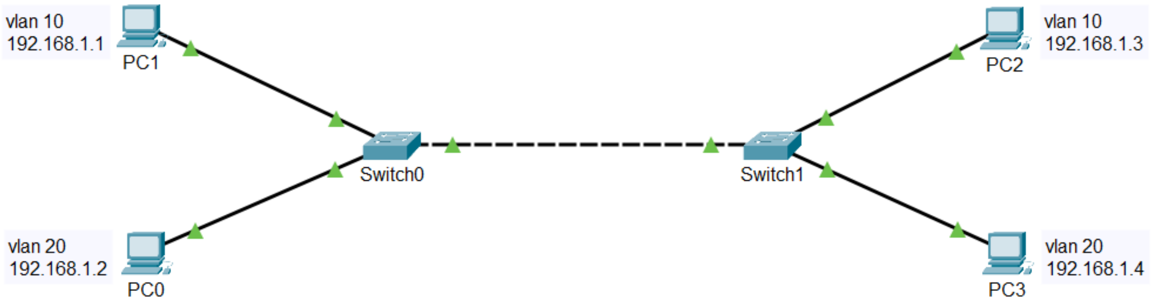


Figure 1.25

1.5.4 Inter-VLAN

Inter-VLAN, refers to the process of enabling controlled communication between devices residing in separate VLANs (Virtual Local Area Networks) on a network.

– **Practical**

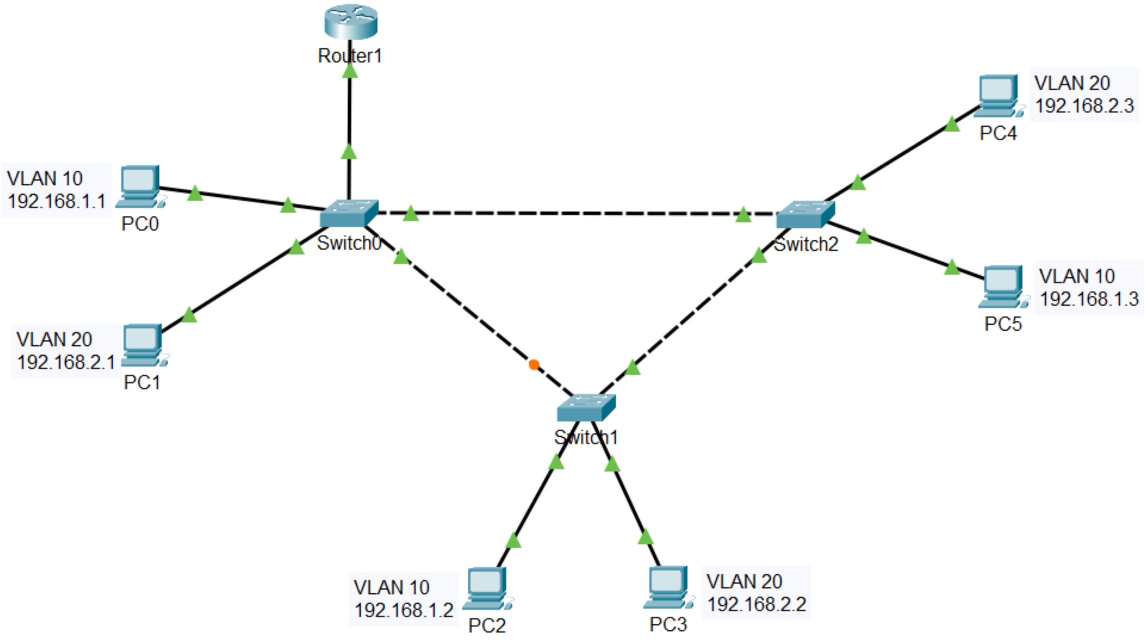


Figure 1.26

- **Step 1:** Apply VLAN on all Switches.
- **Step 2:** Configuration on Router1

```
~  Router(config)# int gig 0/0
~  Router(config-if)# no shut
~  Router(config-if)# ex
~  Router(config)# int gig 0/0.10
~  Router(config-subif)# encapsulation dot1Q 10
~  Router(config-subif)# ip address 192.168.1.10 255.255.255.0
~  Router(config-subif)# ex

~  Router(config)# int gig 0/0.20
~  Router(config-subif)# encapsulation dot1Q 20
~  Router(config-subif)# ip address 192.168.2.10 255.255.255.0
~  Router(config-subif)# ex
```

1.5.5 HSRP: Hot Standby Router Protocol

HSRP (Hot Standby Router Protocol) is a Cisco proprietary routing protocol designed to provide fault tolerance and redundancy for the default gateway in a Local Area Network (LAN). It ensures that there's minimal disruption to network traffic if the primary router fails.

– **Practical**

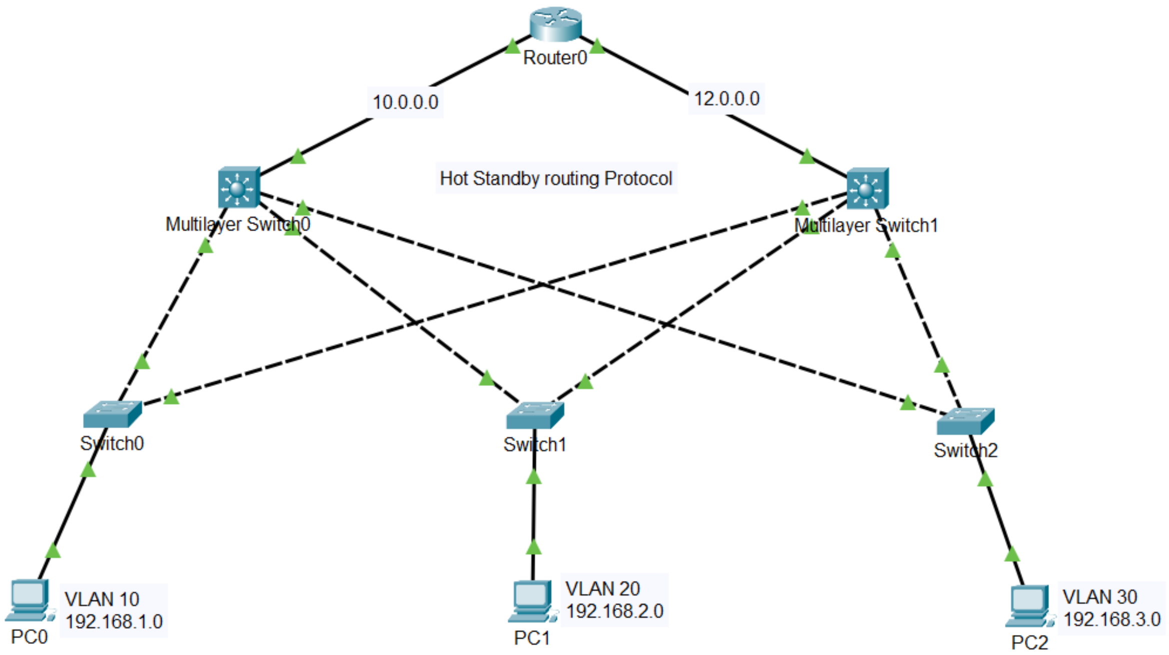


Figure 1.27

- **Step 1:** Configure OSPF 10 with area 1 on Router0.
- **Step 2:** Apply VLAN 10, VLAN 20, and VLAN 30 on SW1, SW2, and SW3 respectively.
- **Step 3:** Configuration on MS0

```
~  MS0(config)# int gig 1/0/1
~  MS0(config-if)# no switchport
~  MS0(config-if)# ip address 10.0.0.2 255.0.0.0
~  MS0(config-if)# no shutdown
~  MS0(config-if)# exit

~  MS0(config)#int range gig 1/0/2-4
~  MS0(config-if-range)# switchport mode trunk
~  MS0(config-if-range)# exit

~  MS0(config)# vlan 10
~  MS0(config-vlan)# name IT
~  MS0(config-vlan)# exit
~  MS0(config)# vlan 20
~  MS0(config-vlan)# name CSE
~  MS0(config-vlan)# exit
~  MS0(config)# vlan 30
~  MS0(config-vlan)# name ECE
~  MS0(config-vlan)# exit

~  MS0(config)# int Vlan10
~  MS0(config-if)# ip address 192.168.1.3 255.255.255.0
~  MS0(config-if)# standby 10 priority 100
~  MS0(config-if)# standby 10 ip 192.168.1.1
~  MS0(config-if)# exit

~  MS0(config)# int Vlan20
~  MS0(config-if)# ip address 192.168.2.3 255.255.255.0
~  MS0(config-if)# standby 20 priority 100
~  MS0(config-if)# standby 20 ip 192.168.2.1
~  MS0(config-if)# exit

~  MS0(config)# int Vlan30
~  MS0(config-if)# ip address 192.168.3.3 255.255.255.0
~  MS0(config-if)# standby 30 priority 100
~  MS0(config-if)# standby 30 ip 192.168.3.1
~  MS0(config-if)# exit

~  MS0(config)# ip routing
~  MS0(config)# router ospf 10
~  MS0(config-router)# router-id 2.2.2.2
~  MS0(config-router)# network 192.168.1.0 0.0.0.255 area 1
~  MS0(config-router)# network 10.0.0.0 0.255.255.255 area 1
~  MS0(config-router)# network 192.168.2.0 0.0.0.255 area 1
~  MS0(config-router)# network 192.168.3.0 0.0.0.255 area 1
```

- **Step 4:** Configuration on MS1
  Repeat previous commands with some modification.

1.6 OTHERS

1.6.1 IP Access Control Lists (ACLs)

An IP Access Control List (ACL) is a list of rules that specifies which users or systems are granted or denied access to a particular object or system resource.

- **Standard Access Lists**
  ~ Range (1-99)
- **Extended Access Lists**
  ~ Range (100-199)

– **Practical**
Here we are denying the access of PC0 from Router2.

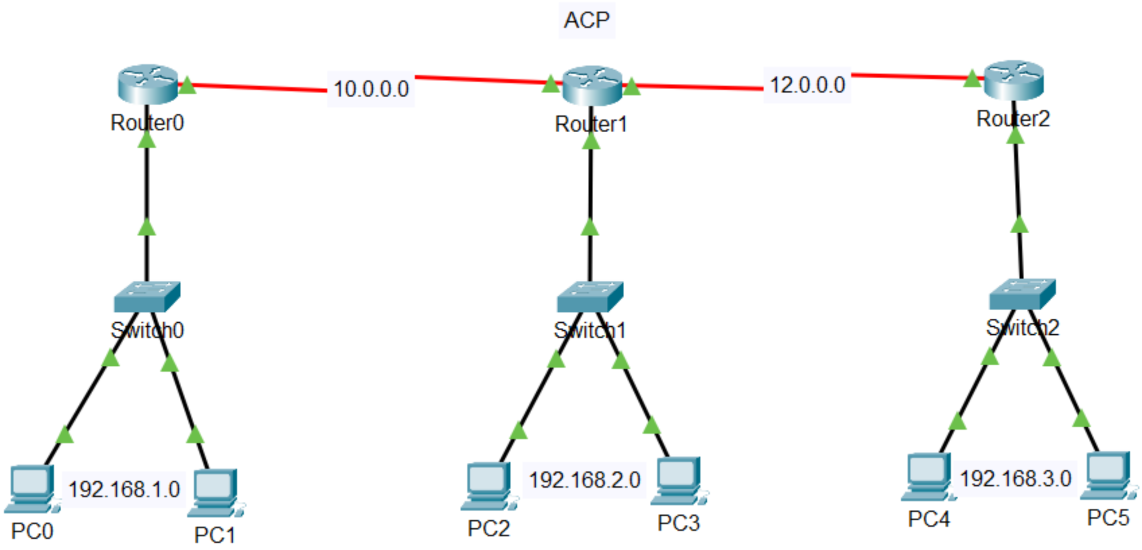


Figure 1.28

– **Commands** *On Router2

```
~  Router(config)# access-list 10 deny host 192.168.1.1
~  Router(config)# access-list 10 permit any

~  Router(config)# int serial 0/3/0
~  Router(config-if)# ip access-group 10 in
```

1.6.2 Point-to-Point Protocol (PPP)

Point-to-Point Protocol (PPP) is a communication protocol used to establish and manage connections between two network devices over a physical link.

– **Practical**

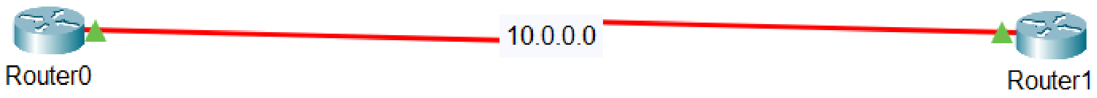


Figure 1.29

– **Configuration on R0 & R1**

```
~  Router# conf ter
~  Router(config)# int serial 0/3/0
~  Router(config-if)# encapsulation ppp
```

1.6.3 VPN using Tunnel

A tunnel refers to a logical connection established between two devices or networks. It acts like a virtual pathway that allows data to travel securely even though it's physically traversing another network, often the public internet.

– **Practical**

Creating a tunnel from Router0 to Router1.

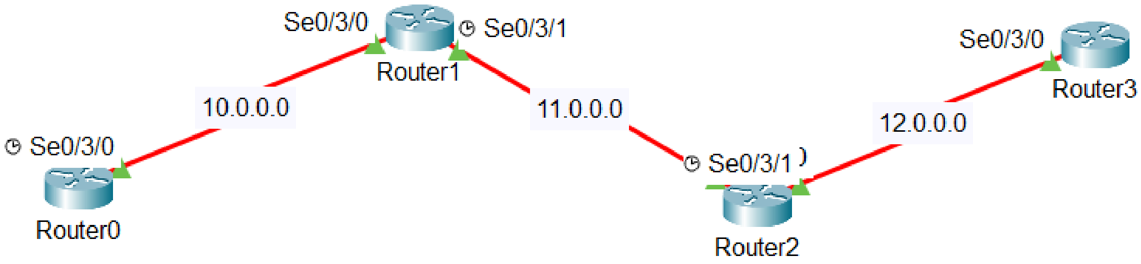


Figure 1.30

– **Configuration**

*On Router0

```
~  Router(config)# interface Tunnel 47
~  Router(config-if)# ip address 172.0.0.1 255.255.0.0
~  Router(config-if)# tunnel source Serial0/3/0
~  Router(config-if)# tunnel destination 12.0.0.2
```

*On Router0

```
~  Router(config)# interface Tunnel 47
~  Router(config-if)# ip address 172.0.0.2 255.255.0.0
~  Router(config-if)# tunnel source Serial0/3/0
~  Router(config-if)# tunnel destination 10.0.0.1
```

PART -2 PROJECT

NAME OF PROJECT

HOSPITAL SYSTEM NETWORK

CHAPTER 2

2.1 PROJECT DETAILS

2.1.1 Introduction to Project

The Hospital System Network Design project aims to create a robust, secure, and efficient network infrastructure for a modern healthcare facility. This network will serve as the backbone for seamless communication, data sharing, and collaboration among various departments and stakeholders within the hospital. The network design will emphasize the delivery of high-quality patient care, quick access to critical medical information, and the ability to support the latest healthcare technologies.

With the advancement of technology in the healthcare sector, hospitals are embracing digital transformation to enhance their services, optimize workflows, and improve patient outcomes. The "Hospital System Network Design" project represents a strategic initiative aimed at revolutionizing the hospital's information infrastructure to meet the growing demands of modern healthcare.

The primary objective of this project is to enable seamless data exchange and collaboration among various departments, medical personnel, and support staff. By developing an interconnected network that seamlessly integrates electronic health records (EHR), medical imaging systems, laboratory information, pharmacy management, and other critical healthcare applications, hospital staff can access real-time patient data whenever and wherever required.

Scalability is another critical aspect of the network design. By anticipating future growth and technological advancements, the project aims to develop a flexible and adaptable network infrastructure. This will allow the hospital to seamlessly integrate new medical devices, accommodate increased data volumes, and adapt to evolving healthcare standards and protocols.

The project will also focus on redundancy and disaster recovery mechanisms to ensure high availability and continuous access to essential systems. In the event of unforeseen disruptions, such as hardware failures or natural disasters, the hospital's critical operations will remain functional, minimizing downtime and ensuring uninterrupted patient care.

Moreover, network performance optimization will be a key consideration throughout the project. By reducing latency, enhancing data transfer rates, and improving overall network responsiveness, medical personnel can efficiently retrieve and exchange information, enabling quicker diagnosis and more effective treatment plans.

Interoperability with external healthcare providers and systems is yet another vital component of the network design. By adhering to industry standards and protocols, the hospital can foster seamless information exchange with external partners, ensuring a more comprehensive and coordinated approach to patient care.

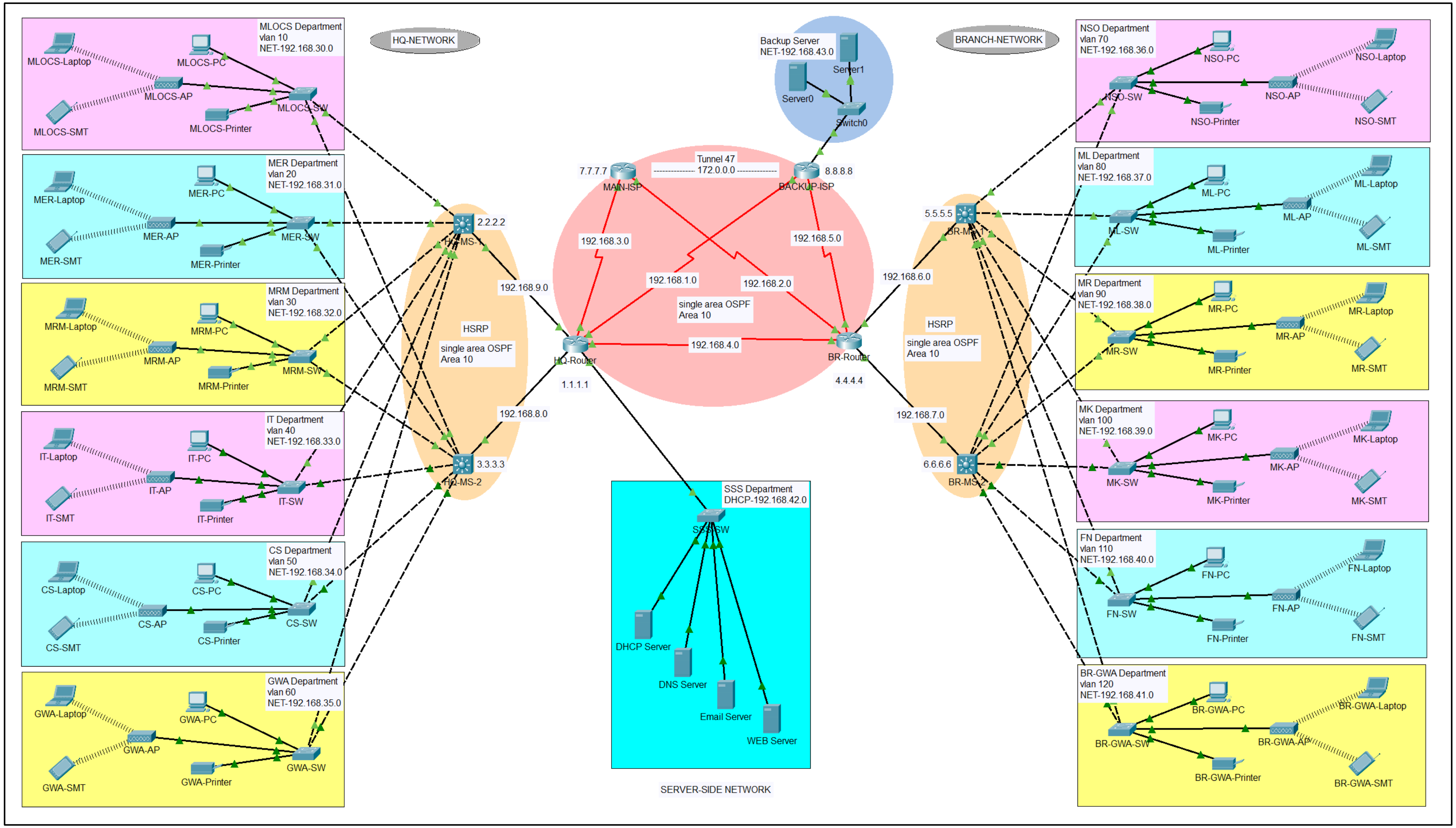

MLOCS Department
vlan 10
NET-192.168.30.0
MLOCS-Laptop
MLOCS-PC
MLOCS-AP
MLOCS-SW
MLOCS-SMT
MLOCS-Printer
MER Department
vlan 20
NET-192.168.31.0
MER-Laptop
MER-PC
MER-AP
MER-SW
MER-SMT
MER-Printer
MRM Department
vlan 30
NET-192.168.32.0
MRM-Laptop
MRM-PC
MRM-AP
MRM-SW
MRM-SMT
MRM-Printer
IT Department
vlan 40
NET-192.168.33.0
IT-Laptop
IT-PC
IT-AP
IT-SW
IT-SMT
IT-Printer
CS Department
vlan 50
NET-192.168.34.0
CS-Laptop
CS-PC
CS-AP
CS-SW
CS-SMT
CS-Printer
GWA Department
vlan 60
NET-192.168.35.0
GWA-Laptop
GWA-PC
GWA-AP
GWA-SW
GWA-SMT
GWA-Printer
HQ-NETWORK
2.2.2.2
HQ-MS-1
HSRP
single area OSPF
Area 10
3.3.3.3
HQ-MS-2
192.168.9.0
192.168.8.0
HQ-Router
1.1.1.1
7.7.7.7
MAIN-ISP
Tunnel 47
172.0.0.0
8.8.8.8
BACKUP-ISP
192.168.3.0
192.168.5.0
192.168.1.0
192.168.2.0
single area OSPF
Area 10
192.168.4.0
BR-Router
4.4.4.4
Backup Server
NET-192.168.43.0
Server1
Server0
Switch0
SSS Department
DHCP-192.168.42.0
SSS-SW
DHCP Server
DNS Server
Email Server
WEB Server
SERVER-SIDE NETWORK
BRANCH-NETWORK
5.5.5.5
BR-MS-1
192.168.6.0
HSRP
single area OSPF
Area 10
192.168.7.0
6.6.6.6
BR-MS-2
NSO Department
vlan 70
NET-192.168.36.0
NSO-PC
NSO-Laptop
NSO-SW
NSO-AP
NSO-Printer
NSO-SMT
ML Department
vlan 80
NET-192.168.37.0
ML-PC
ML-Laptop
ML-AP
ML-SW
ML-Printer
ML-SMT
MR Department
vlan 90
NET-192.168.38.0
MR-PC
MR-Laptop
MR-AP
MR-SW
MR-Printer
MR-SMT
MK Department
vlan 100
NET-192.168.39.0
MK-PC
MK-Laptop
MK-AP
MK-SW
MK-Printer
MK-SMT
FN Department
vlan 110
NET-192.168.40.0
FN-PC
FN-Laptop
FN-SW
FN-AP
FN-Printer
FN-SMT
BR-GWA Department
vlan 120
NET-192.168.41.0
BR-GWA-PC
BR-GWA-Laptop
BR-GWA-SW
BR-GWA-AP
BR-GWA-Printer
BR-GWA-SMT

Figure 2.1

2.1.2 Software Requirements

- Operating System: Windows7 ultimate, Windows 10
- Software: Cisco Packet Tracer, GNS 3 (any one)

2.1.3 Cisco Packet Tracer

Cisco Packet Tracer is a comprehensive, networking technology teaching and learning program that offers a unique combination of realistic simulation and visualization experiences, assessment and activity authoring capabilities, and opportunities for multiuser collaboration and competition. The innovative features of Packet Tracer help students and teachers collaborate, solve problems, and learn concepts in an engaging and dynamic social environment.

Some of the benefits of Packet Tracer are:

- Provides a realistic simulation and visualization learning environment that supplements classroom equipment, including the ability to see internal processes in real-time that are normally hidden on real devices.
- Enables multi-user, real-time collaboration and competition for dynamic learning.
- Enables authoring and localization of structured learning activities such as labs, demonstrations, quizzes, exams, and games.
- Empowers students to explore concepts, conduct experiments, and test their understanding of network building.
- Allows students and teachers to design, build, configure, and troubleshoot complex networks using virtual equipment.
- Supports a variety of teaching and learning opportunities such as lectures, group, and individual labs, homework, games, and competitions.

Supports feature expansion through external applications using an API to enhance the functionality of Cisco Packet Tracer in areas such as curriculum and assessment delivery, games, accessibility, and interfacing with real equipment.

Key Features:

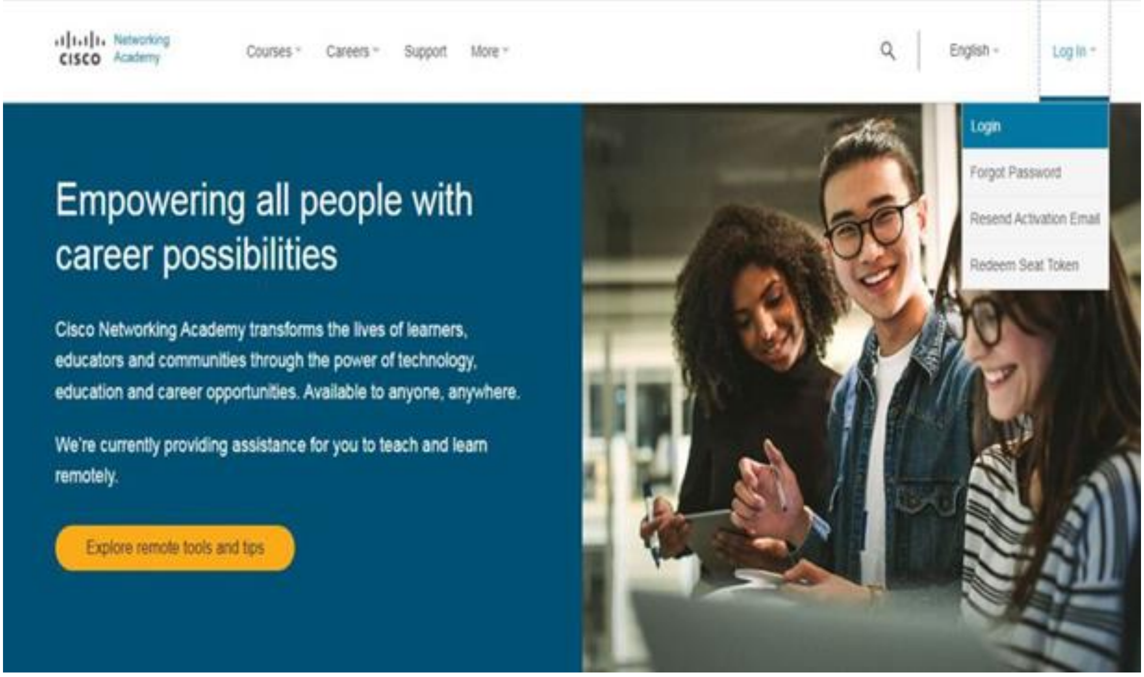
- Unlimited devices
- E-learning
- Customize single/multi user activities
- Interactive Environment
- Visualizing Networks
- Real-time mode and Simulation mode
- Self-paced
- Supports majority of networking protocols
- International language support

- Cross platform compatibility

2.1.3.1 Installation

<u>Follow the below steps to install Packet Tracer</u>

Step - 1. Visit the official website of https://www.netacad.com/ using any web browser.



Empowering all people with career possibilities

Cisco Networking Academy transforms the lives of learners, educators and communities through the power of technology, education and career opportunities. Available to anyone, anywhere.

We're currently providing assistance for you to teach and learn remotely.

Figure 2.2

Step - 2. Press the login button and select log in option.

Step - 3. Now the login screen appears again so fill in the Email id. Enter the password and press the Login button.

Step - 4. After Login, dashboard will initialize, now click on Resources and choose Download Packet Tracer Option.

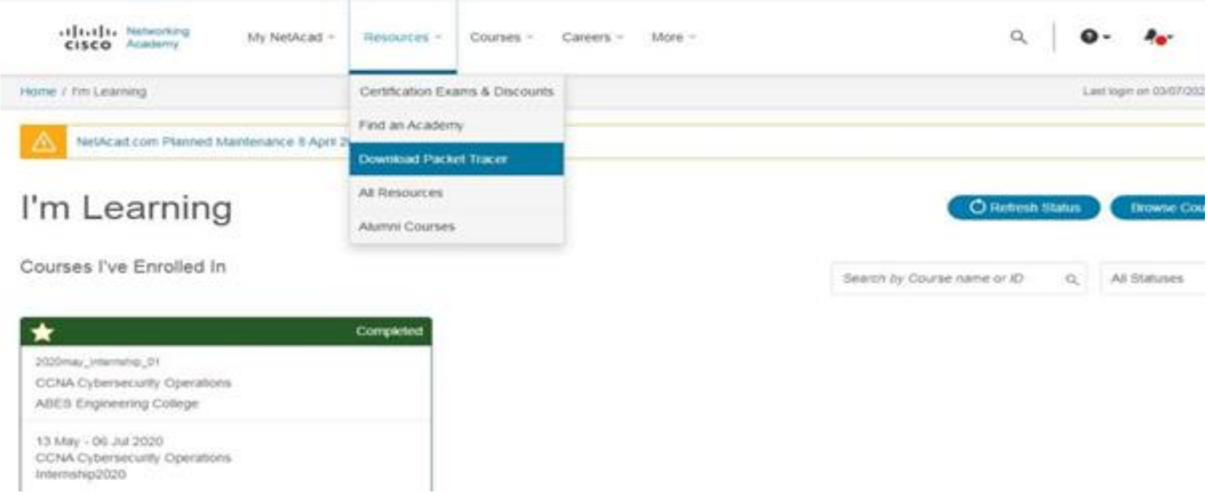


Figure 2.3

Step - 5. Choose the latest version according to the operating system to download the packet tracer. Downloading will start automatically.

Step - 6. Check for the executable file in your system and run it.

Step - 7. Follow the download instructions appearing on the screen.

Step - 8. Once the download is complete, double-click on the installer file to begin the installation process

Step - 9. Follow the on-screen instructions to complete the installation.

<u>Interface is initialized and the software is ready to use.</u>

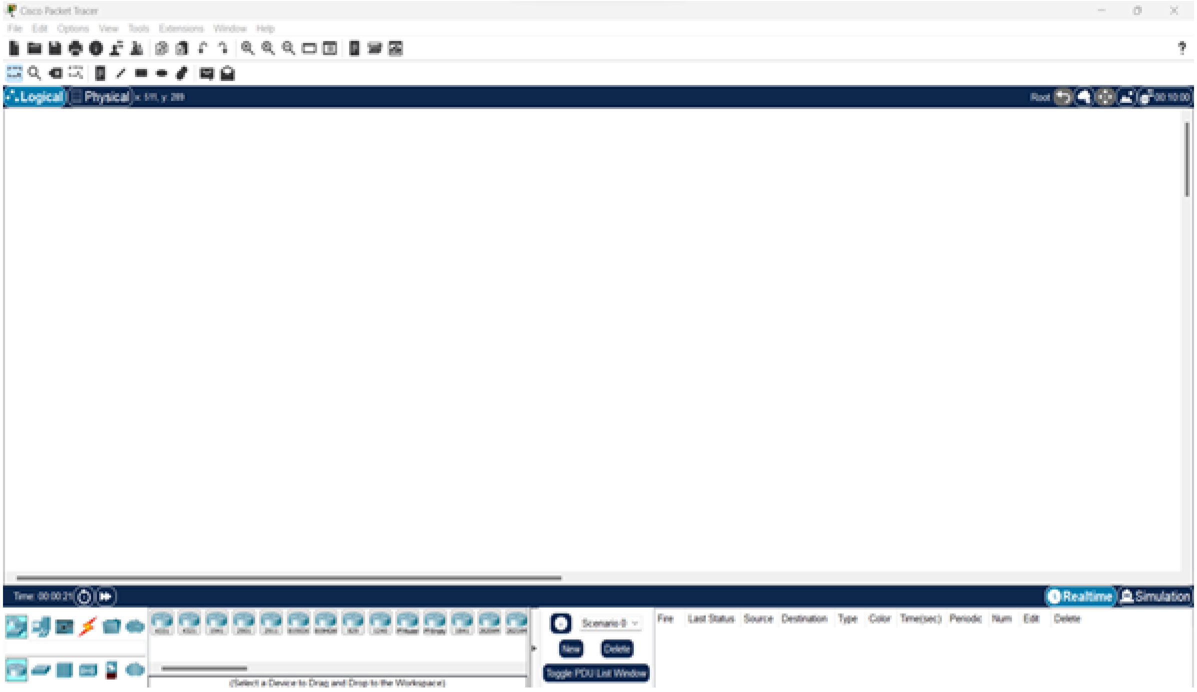

Cisco Packet Tracer
File Edit Options View Tools Extensions Window Help
Logical
Physical
x: 511, y: 289
Root
00:10:00
Time: 00:00:21
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color Time(sec) Periodic Num Edit Delete
(Select a Device to Drag and Drop to the Workspace)

Figure 2.4

2.2 IMPLEMENTATION

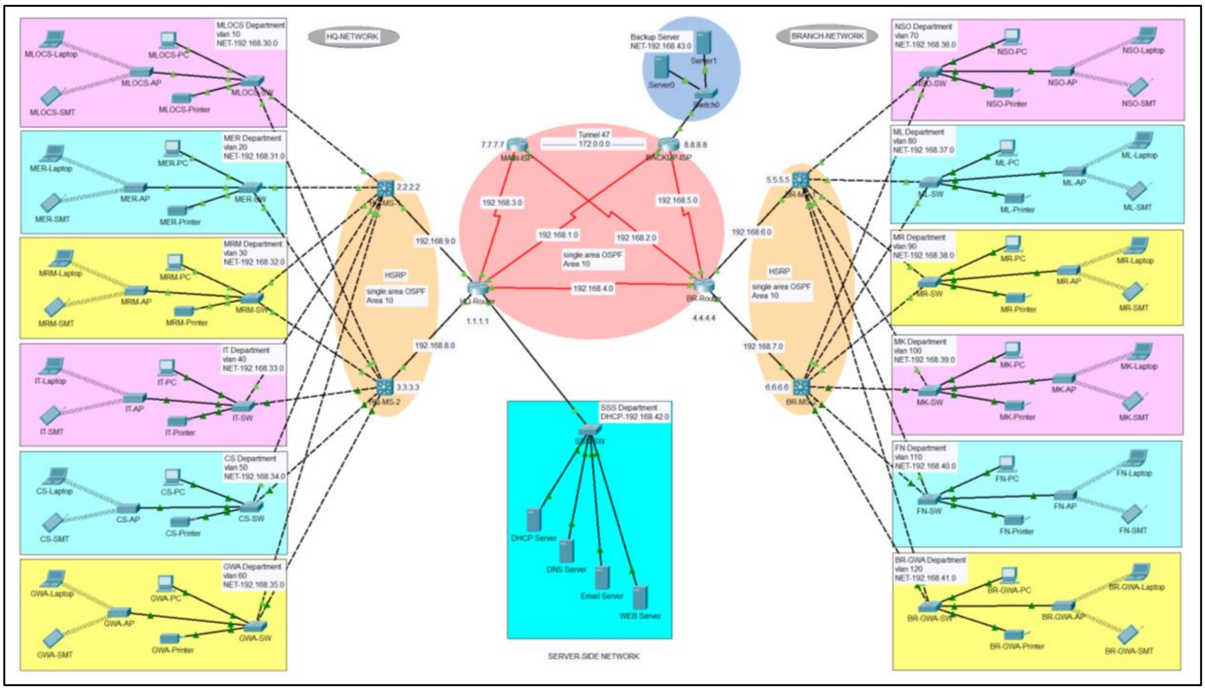


Figure 2.5

2.2.1 Departmental details

HQ Network			Branch Network		
Department	**VLAN**	**NET**	**Department**	**VLAN**	**NET**
MLOCS	10	192.168.30.0	NSO	70	192.168.36.0
MER	20	192.168.31.0	ML	80	192.168.37.0
MRM	30	192.168.32.0	MR	90	192.168.38.0
IT	40	192.168.33.0	MK	100	192.168.39.0
CS	50	192.168.34.0	FN	110	192.168.40.0
GWA	60	192.168.35.0	BR-GWA	120	192.168.41.0

Server Side Network	
Department	**DHCP**
SSS	192.168.42.0

Table 2.1

2.2.2 Connecting Wires

– **Copper Straight-Through Cable:**

- **Function:** Used to connect devices that operate at different layers of the network model.
- **Wiring:** The wires in the RJ45 connector have the **same order** at both ends (pins 1-8 on one end match pins 1-8 on the other end). Straight through cable use one wiring standard: both ends use T568A wiring standard or both ends use T568B wiring standard. The following figure shows a straight through cable of which both ends are wired as the T568B standard.

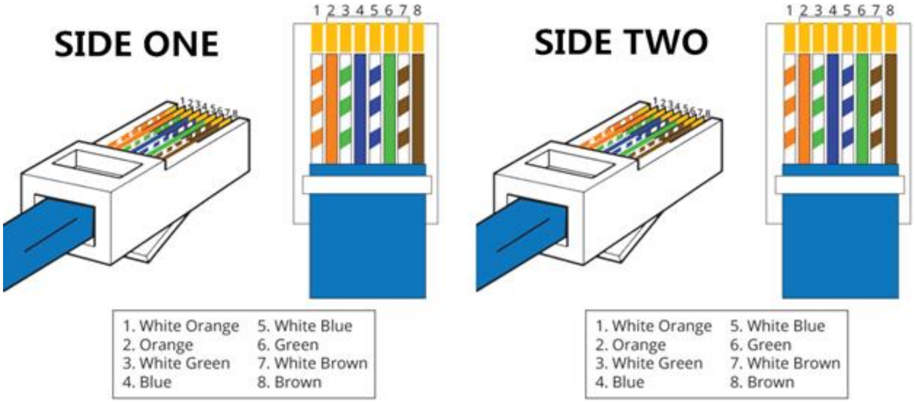


Figure 2.6

- **Applications:** Common use cases include connecting a computer to a router, a switch to a router, or any combination where one device sends data and the other receives it.

– **Copper Cross-Over Cable:**

- **Function:** Used to connect devices that operate at the same layer of the network model.
- **Wiring:** Unlike straight through cable, the RJ45 crossover cable uses two different wiring standards: one end uses the T568A wiring standard, and the other end uses the T568B wiring standard.

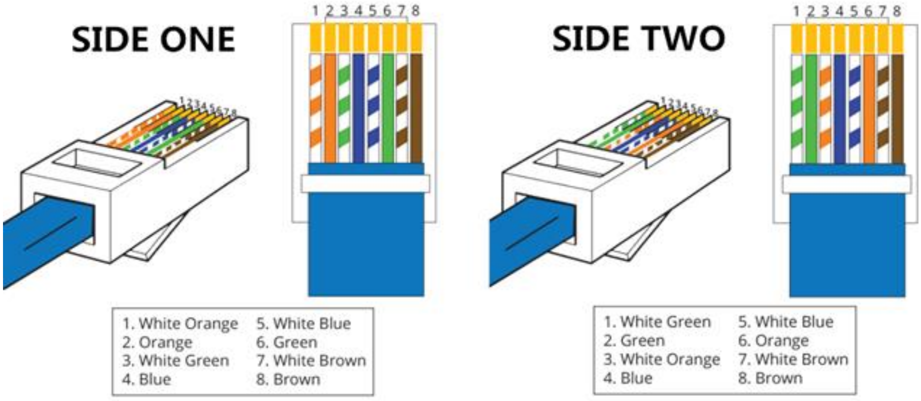


Figure 2.7

- **Applications:** You can use a copper crossover cable to connect two devices of the same type directly together, such as two computers, two switches, or two routers.

– **Serial DTE (Data Terminal Equipment):**

- **Function:** Used to connect end devices like computers, printers, or terminals that generate or consume data within a network.
- **Wiring:** The wiring for Serial DTE typically follows the RS-232 standard, which specifies the pin configuration and electrical characteristics. The pins include transmit data (TXD), receive data (RXD), signal ground (SG), and control signals such as RTS (Request to Send) and CTS (Clear to Send).
- **Applications:** Common use cases include connecting a computer to a modem, connecting terminals to a mainframe, or interfacing with other DCE (Data Circuit-terminating Equipment) devices like routers or communication switches.

2.2.3 Operations performed

1. IP configuration
2. Router-Switch configuration
3. DHCP
4. VLAN
5. HSRP
6. OSPF
7. VPN
8. Wireless connection

– IP configuration

Assign IP addresses to END Devices like PC, Laptop, Printer, Server etc. according to their Departments. Each department has different network Id's.

- **HQ NETWORK**

  It consists of SIX different Departments having network Id's from 192.168.30.0 to 192.168.35.0

  <u>For example:</u>

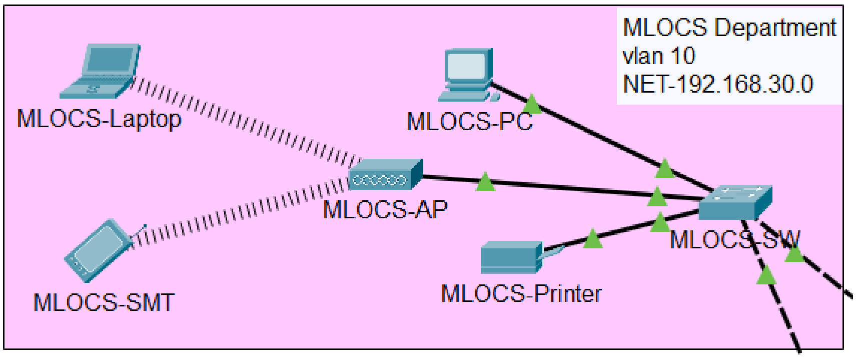


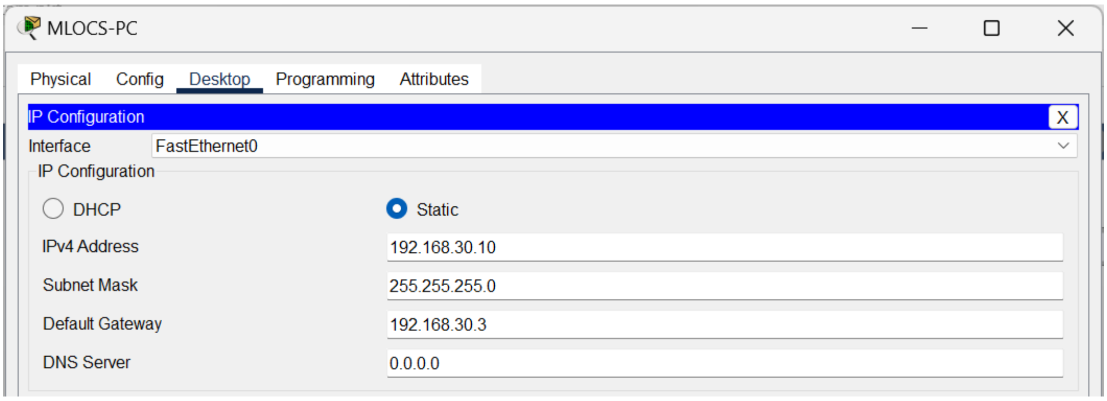
Figure 2.8

MLOCS Department		
Devices	**IP Address**	**Default Gateway**
PC	192.168.30.10	192.168.30.3
Printer	192.168.30.11	192.168.30.3
Laptop	192.168.30.12	192.168.30.3
Smartphone	192.168.30.13	192.168.30.3

Table 2.2

Steps:

1. Click on any END Device.
2. Click on Desktop.
3. Click on IP Configuration.


MLOCS-PC

Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address: 192.168.30.10

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.30.3

DNS Server: 0.0.0.0

Figure 2.9

- **BRANCH NETWORK**

  It consists of SIX different Departments having network Id's from 192.168.36.0 to 192.168.41.0

  For example:

NSO Department		
Devices	**IP Address**	**Default Gateway**
PC	192.168.36.10	192.168.36.3
Printer	192.168.36.11	192.168.36.3
Laptop	192.168.36.12	192.168.36.3
Smartphone	192.168.36.13	192.168.36.3

Table 2.3

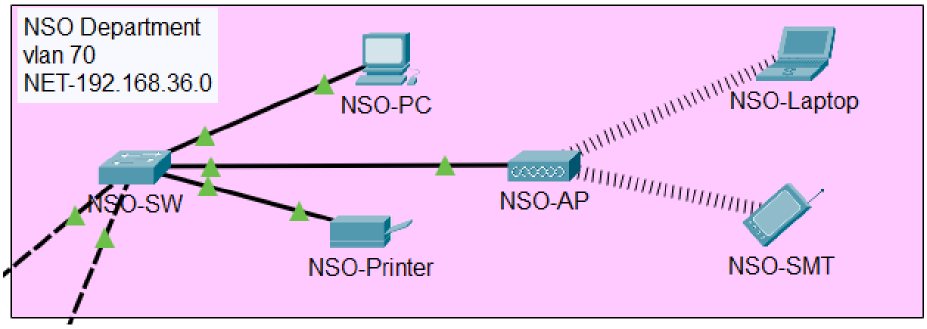


Figure 2.10

- **Backup Server**

Devices	IP Address	Default Gateway
Server0	192.168.43.1	192.168.43.5
Server1	192.168.43.2	192.168.43.5

Table 2.4

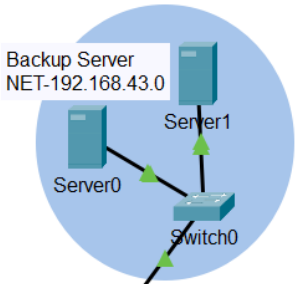


Figure 2.11

– Router-Switch configuration

It has four routers and four multi-switch having network Id's from 192.168.1.0 to 192.168.9.0

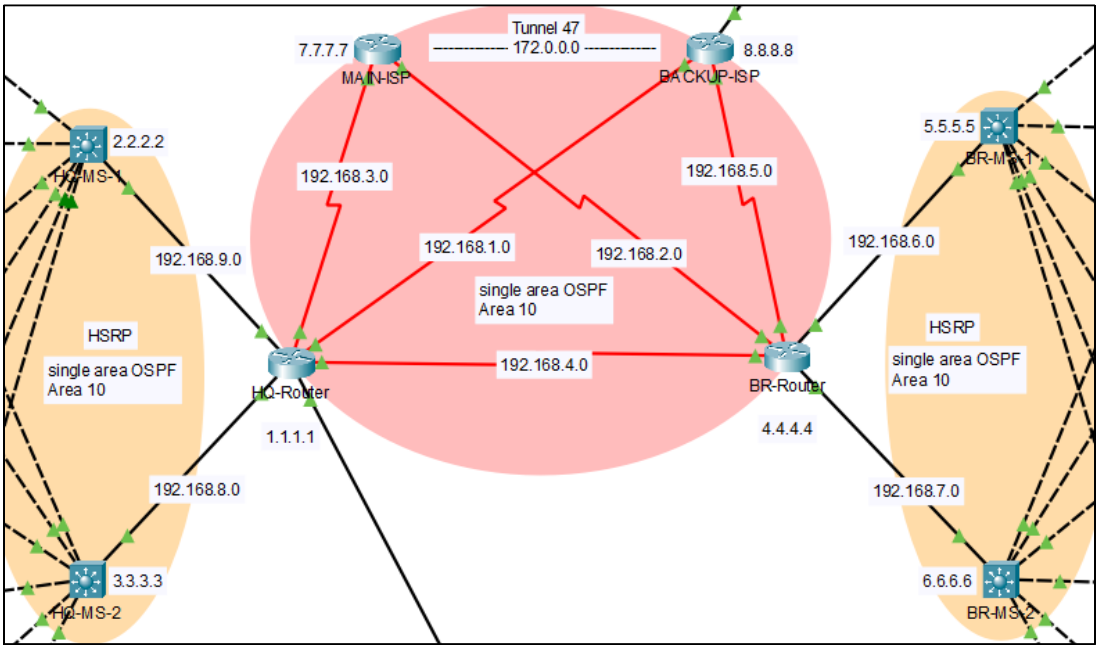


Figure 2.12

- HQ-Router

```
~  int se 0/2/1
~  ip address 192.168.1.1 255.255.255.0

~  int se 0/2/0
~  ip address 192.168.3.1 255.255.255.0

~  int se 0/1/0
~  ip address 192.168.4.1 255.255.255.0

~  int gig 0/1
~  ip address 192.168.8.1 255.255.255.0

~  int gig 0/0
~  ip address 192.168.9.1 255.255.255.0
```

- BR-Router

```
~  int se 0/2/1
~  ip address 192.168.2.1 255.255.255.0

~  int se 0/1/0
~  ip address 192.168.4.2 255.255.255.0

~  int se 0/2/0
~  ip address 192.168.5.1 255.255.255.0

~  int gig 0/0
~  ip address 192.168.6.1 255.255.255.0

~  int gig 0/1
~  ip address 192.168.7.1 255.255.255.0
```

- Main-ISP-Router

```
~  int se 0/3/1
~  ip address 192.168.2.2 255.255.255.0

~  int se 0/3/0
~  ip address 192.168.3.2 255.255.255.0
```

- Backup-ISP-Router

```
~  int se 0/3/1
~  ip address 192.168.1.2 255.255.255.0
~  int se 0/3/0
~  ip address 192.168.5.2 255.255.255.0
~  int fa 0/0
~  ip address 192.168.43.5 255.255.255.0
```

- HQ-MS1

```
~  int gig 1/0/1
~  no switchport
~  ip address 192.168.9.2 255.255.255.0
```

- HQ-MS2

```
~  int gig 1/0/1
~  no switchport
~  ip address 192.168.8.2 255.255.255.0
```

- BR-MS1

```
~  int gig 1/0/1
~  no switchport
~  ip address 192.168.6.2 255.255.255.0
```

- BR-MS2

```
~  int gig 1/0/1
~  no switchport
~  ip address 192.168.7.2 255.255.255.0
```

– DHCP

Dynamic Host Configuration Protocol (DHCP) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway.

- **Server-Side Network**

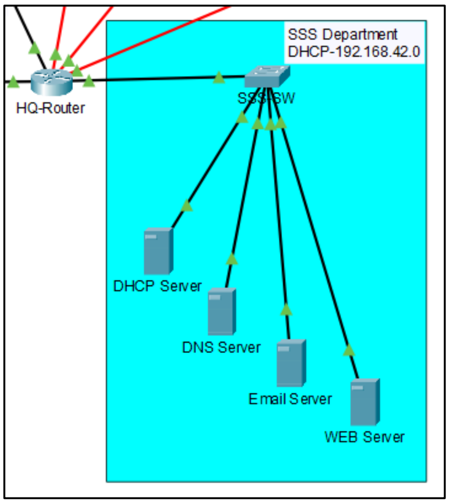


Figure 2.13

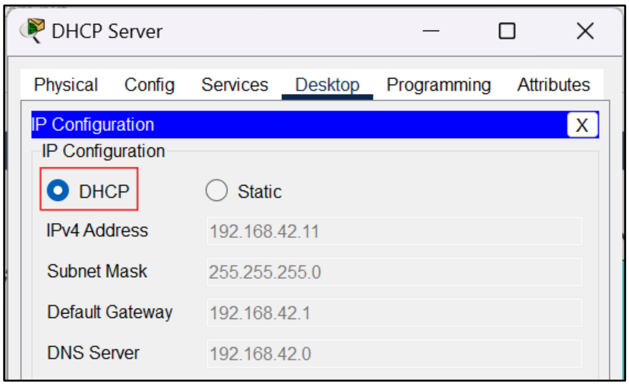
Step 1.

Configuration *On HQ-Router

```
~  ip dhcp pool slinf
~  default-router 192.168.42.1
~  dns-server 192.168.42.0
~  exit
~  ip dhcp excluded-address
   192.168.42.1 192.168.42.10
```

Step 2.

1) Click on server, go to desktop.
2) Click on IP configuration.
3) Click on DHCP.



IP Configuration

● DHCP ○ Static

IPv4 Address 192.168.42.11

Subnet Mask 255.255.255.0

Default Gateway 192.168.42.1

DNS Server 192.168.42.0

Figure 2.14

SSS Department		
Server	**IP Address**	**Default Gateway**
DHCP	192.168.42.11	192.168.42.1
DNS	192.168.42.14	192.168.42.1
Email	192.168.42.12	192.168.42.1
WEB	192.168.42.13	192.168.42.1

Table 2.5

– VLAN

HQ-NETWORK			BRANCH-NETWORK		
SWITCH	**VLAN**	**NAME**	**SWITCH**	**VLAN**	**NAME**
MLOCCS-SW	vlan 10	MLOCS	NSO-SW	vlan 70	NSO
MER-SW	vlan 20	MER	ML-SW	vlan 80	ML
MRM-SW	vlan 30	MRM	MR-SW	vlan 90	MR
IT-SW	vlan 40	IT	MK-SW	vlan 100	MK
CS-SW	vlan 50	CS	FN-SW	vlan 110	FN
GWA-SW	vlan 60	GWA	BR-GWA-SW	vlan 120	BR-GWA

Table 2.6

<u>For example:</u>

*on CS-SW

```
~  conf t
~  vlan 50
~  name CS
~  exit
~  int range fa 0/3-5
~  switchport access vlan 50
~  switchport mode access
~  exit

~  int range fa 0/1-2
~  switchport mode trunk
```

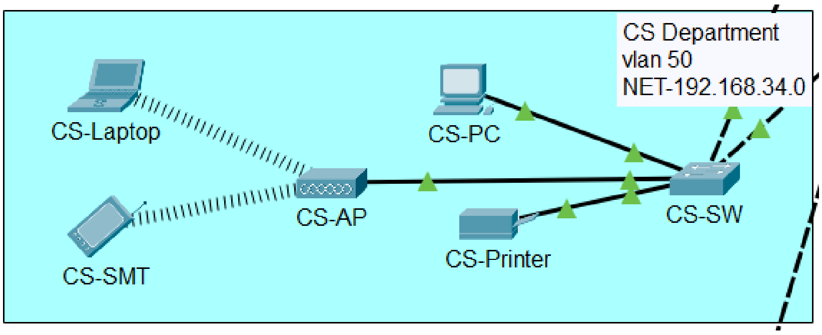


Figure 2.15

*on MK-SW

```
~  conf t
~  vlan 100
~  name MK
~  exit
~  int range fa 0/3-5
~  switchport access vlan 100
~  switchport mode access
~  exit

~  int range fa 0/1-2
~  switchport mode trunk
```

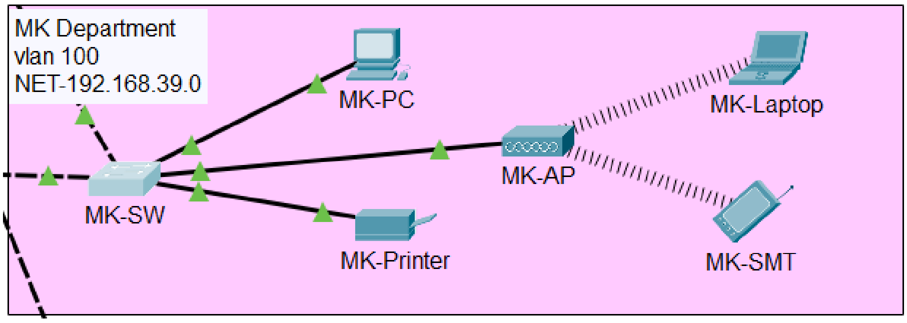


Figure 2.16

– HSRP

Before applying HSRP, we have to do trunking and assigning all the VLAN's to Multi-switch. Here we have four Multi-switch, two in HQ network and two in Branch network.

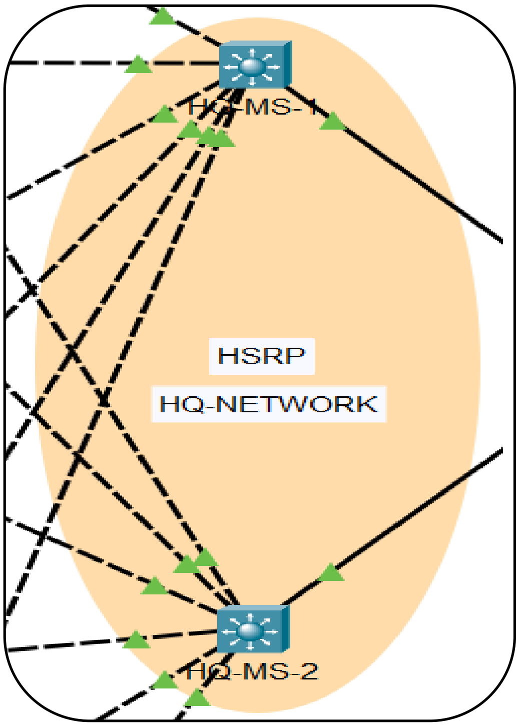


Figure 2.17

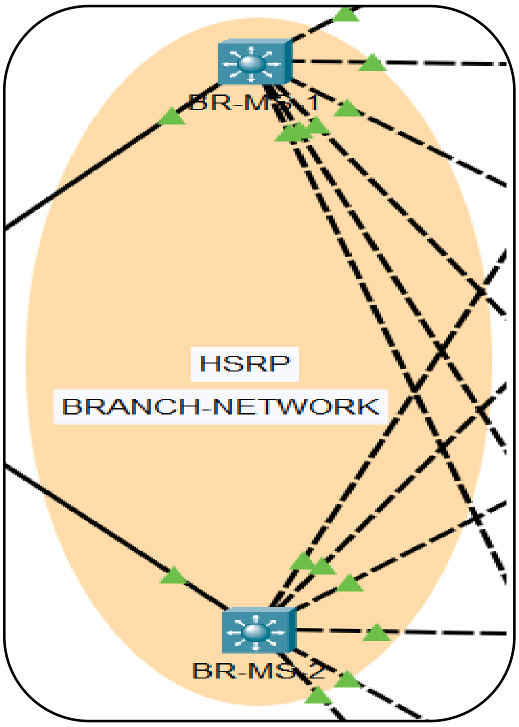


Figure 2.18

- **HQ-MS-1**

```
~  int range gig 1/0/2-7
~  switchport mode trunk
~  ex

~  vlan 10
~  name MLOCS
~  ex
~  vlan 20
~  name MER
~  ex
~  vlan 30
~  name MRM
~  ex
~  vlan 40
~  name IT
~  ex
~  vlan 50
~  name CS
~  ex
~  vlan 60
~  name GWA
~  ex

~  int vlan 10
~  ip address 192.168.30.3 255.255.255.0
~  standby 10 priority 100
~  standby 10 ip 192.168.30.1
~  ex

~  int vlan 20
~  ip address 192.168.31.3 255.255.255.0
~  standby 20 priority 100
~  standby 20 ip 192.168.31.1
~  ex

~  int vlan 30
~  ip address 192.168.32.3 255.255.255.0
~  standby 30 priority 100
~  standby 30 ip 192.168.32.1
~  ex

~  int vlan 40
~  ip address 192.168.33.3 255.255.255.0
~  standby 40 priority 100
~  standby 40 ip 192.168.33.1
~  ex

~  int vlan 50
~  ip address 192.168.34.3 255.255.255.0
~  standby 50 priority 100
~  standby 50 ip 192.168.34.1
~  ex

~  int vlan 60
~  ip address 192.168.35.3 255.255.255.0
~  standby 60 priority 100
~  standby 60 ip 192.168.35.1
~  ex
```

- **HQ-MS-2**

```
~  int range gig 1/0/2-7
~  switchport mode trunk
~  ex

~  vlan 10
~  name MLOCS
~  ex
~  vlan 20
~  name MER
~  ex
~  vlan 30
~  name MRM
~  ex
~  vlan 40
~  name IT
~  ex
~  vlan 50
~  name CS
~  ex
~  vlan 60
~  name GWA
~  ex

~  int vlan 10
~  ip address 192.168.30.3 255.255.255.0
~  standby 10 priority 90
~  standby 10 ip 192.168.30.1
~  ex
~  int vlan 20
~  ip address 192.168.31.3 255.255.255.0
~  standby 20 priority 90
~  standby 20 ip 192.168.31.1
~  ex

~  int vlan 30
~  ip address 192.168.32.3 255.255.255.0
~  standby 30 priority 90
~  standby 30 ip 192.168.32.1
~  ex

~  int vlan 40
~  ip address 192.168.33.3 255.255.255.0
~  standby 40 priority 90
~  standby 40 ip 192.168.33.1
~  ex

~  int vlan 50
~  ip address 192.168.34.3 255.255.255.0
~  standby 50 priority 90
~  standby 50 ip 192.168.34.1
~  ex

~  int vlan 60
~  ip address 192.168.35.3 255.255.255.0
~  standby 60 priority 90
~  standby 60 ip 192.168.35.1
~  ex
```

- **BR-MS-1**

```
~  int range gig 1/0/2-7
~  switchport mode trunk
~  ex

~  vlan 70
~  name NSO
~  ex
~  vlan 80
~  name ML
~  ex
~  vlan 90
~  name MR
~  ex
~  vlan 100
~  name MK
~  ex
~  vlan 110
~  name FN
~  ex
~  vlan 120
~  name BR-GWA
~  ex

~  int vlan 70
~  ip address 192.168.36.3 255.255.255.0
~  standby 70 priority 110
~  standby 70 ip 192.168.36.1
~  ex

~  int vlan 80
~  ip address 192.168.37.3 255.255.255.0
~  standby 80 priority 110
~  standby 80 ip 192.168.37.1
~  ex

~  int vlan 90
~  ip address 192.168.38.3 255.255.255.0
~  standby 90 priority 110
~  standby 90 ip 192.168.38.1
~  ex

~  int vlan 100
~  ip address 192.168.39.3 255.255.255.0
~  standby 100 priority 110
~  standby 100 ip 192.168.39.1
~  ex

~  int vlan 110
~  ip address 192.168.40.3 255.255.255.0
~  standby 110 priority 110
~  standby 110 ip 192.168.40.1
~  ex

~  int vlan 120
~  ip address 192.168.41.3 255.255.255.0
~  standby 120 priority 110
~  standby 120 ip 192.168.41.1
~  ex
```

- **BR-MS-2**

```
~  int range gig 1/0/2-7
~  switchport mode trunk
~  ex

~  vlan 70
~  name NSO
~  ex
~  vlan 80
~  name ML
~  ex
~  vlan 90
~  name MR
~  ex
~  vlan 100
~  name MK
~  ex
~  vlan 110
~  name FN
~  ex
~  vlan 120
~  name BR-GWA
~  ex

~  int vlan 70
~  ip address 192.168.36.3 255.255.255.0
~  standby 70 priority 120
~  standby 70 ip 192.168.36.1
~  ex

~  int vlan 80
~  ip address 192.168.37.3 255.255.255.0
~  standby 80 priority 120
~  standby 80 ip 192.168.37.1
~  ex

~  int vlan 90
~  ip address 192.168.38.3 255.255.255.0
~  standby 90 priority 120
~  standby 90 ip 192.168.38.1
~  ex

~  int vlan 100
~  ip address 192.168.39.3 255.255.255.0
~  standby 100 priority 120
~  standby 100 ip 192.168.39.1
~  ex
~  int vlan 110
~  ip address 192.168.40.3 255.255.255.0
~  standby 110 priority 120
~  standby 110 ip 192.168.40.1
~  ex

~  int vlan 120
~  ip address 192.168.41.3 255.255.255.0
~  standby 120 priority 120
~  standby 120 ip 192.168.41.1
~  ex
```

– OSPF

Here we applied single area OSPF with area 10 on all routers and multi-switch along with unique ID’s.

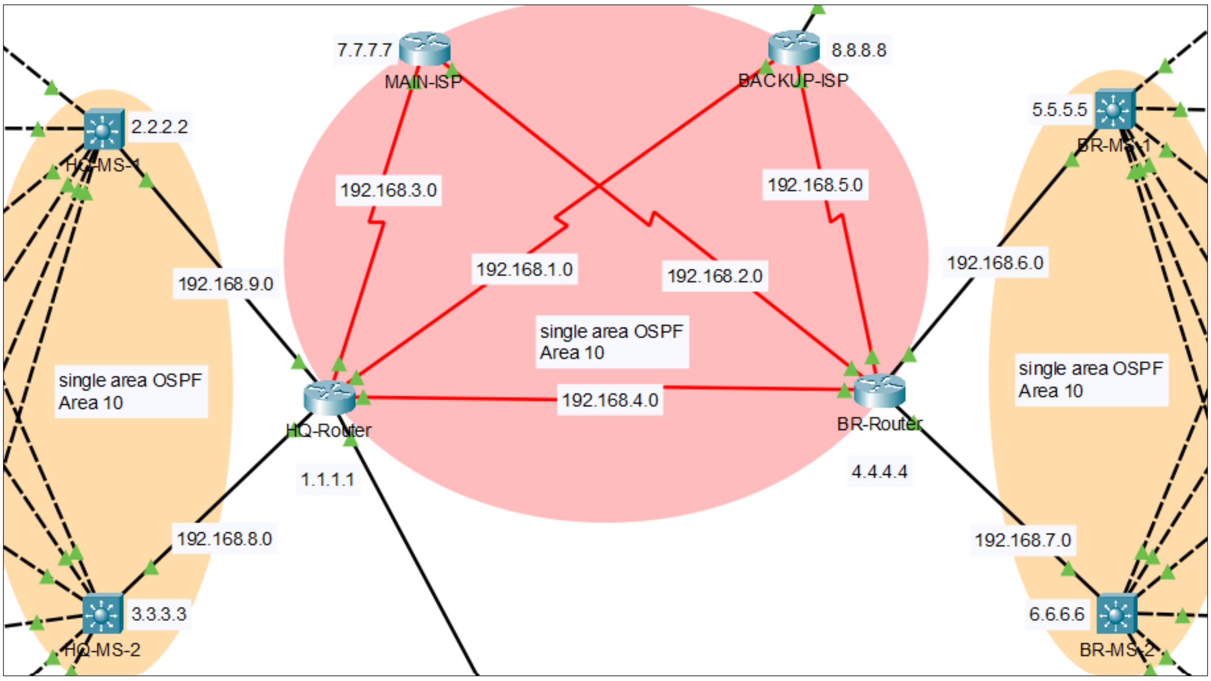


Figure 2.19

- **MAIN-ISP-Router**

```
~  router ospf 10
~  router-id 7.7.7.7
~  network 192.168.3.0 0.0.0.255 area 10
~  network 192.168.2.0 0.0.0.255 area 10
```

- **BACKUP-ISP-Router**

```
~  router ospf 10
~  router-id 8.8.8.8
~  network 192.168.1.0 0.0.0.255 area 10
~  network 192.168.5.0 0.0.0.255 area 10
```

- **HQ-Router**

```
~  router ospf 10
~  router-id 1.1.1.1
~  network 192.168.3.0 0.0.0.255 area 10
~  network 192.168.1.0 0.0.0.255 area 10
~  network 192.168.4.0 0.0.0.255 area 10
~  network 192.168.8.0 0.0.0.255 area 10
~  network 192.168.9.0 0.0.0.255 area 10
~  network 192.168.42.0 0.0.0.255 area 10
```

- **BR-Router**

```
~  router ospf 10
~  router-id 4.4.4.4
~  network 192.168.6.0 0.0.0.255 area 10
~  network 192.168.7.0 0.0.0.255 area 10
~  network 192.168.5.0 0.0.0.255 area 10
~  network 192.168.4.0 0.0.0.255 area 10
~  network 192.168.2.0 0.0.0.255 area 10
```

- **HQ-MS-1**

```
~  ip routing
~  router ospf 10
~  router-id 2.2.2.2
~  network 192.168.9.0 0.0.0.255 area 10
~  network 192.168.30.0 0.0.0.255 area 10
~  network 192.168.31.0 0.0.0.255 area 10
~  network 192.168.32.0 0.0.0.255 area 10
~  network 192.168.33.0 0.0.0.255 area 10
~  network 192.168.34.0 0.0.0.255 area 10
~  network 192.168.35.0 0.0.0.255 area 10
```

- **HQ-MS-2**

```
~  ip routing
~  router ospf 10
~  router-id 3.3.3.3
~  network 192.168.8.0 0.0.0.255 area 10
~  network 192.168.30.0 0.0.0.255 area 10
~  network 192.168.31.0 0.0.0.255 area 10
~  network 192.168.32.0 0.0.0.255 area 10
~  network 192.168.33.0 0.0.0.255 area 10
~  network 192.168.34.0 0.0.0.255 area 10
~  network 192.168.35.0 0.0.0.255 area 10
```

- **BR-MS-1**

```
~  ip routing
~  router ospf 10
~  router-id 5.5.5.5
~  network 192.168.6.0 0.0.0.255 area 10
~  network 192.168.36.0 0.0.0.255 area 10
~  network 192.168.37.0 0.0.0.255 area 10
~  network 192.168.38.0 0.0.0.255 area 10
~  network 192.168.39.0 0.0.0.255 area 10
~  network 192.168.40.0 0.0.0.255 area 10
~  network 192.168.41.0 0.0.0.255 area 10
```

- **BR-MS-2**

```
~  ip routing
~  router ospf 10
~  router-id 6.6.6.6
~  network 192.168.7.0 0.0.0.255 area 10
~  network 192.168.36.0 0.0.0.255 area 10
~  network 192.168.37.0 0.0.0.255 area 10
~  network 192.168.38.0 0.0.0.255 area 10
~  network 192.168.39.0 0.0.0.255 area 10
~  network 192.168.40.0 0.0.0.255 area 10
~  network 192.168.41.0 0.0.0.255 area 10
```

– VPN using tunnel

Creating a tunnel between MAIN-ISP and BACKUP-ISP with network 172.0.0.0

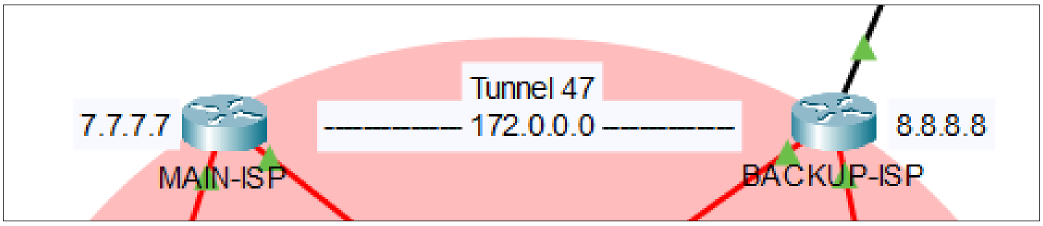


Figure 2.20

- **MAIN-ISP**

```
~  interface Tunnel 47
~  ip address 172.0.0.1 255.255.0.0
~  tunnel source Serial0/3/0
~  tunnel destination 192.168.5.2
```

- **BACKUP-ISP**

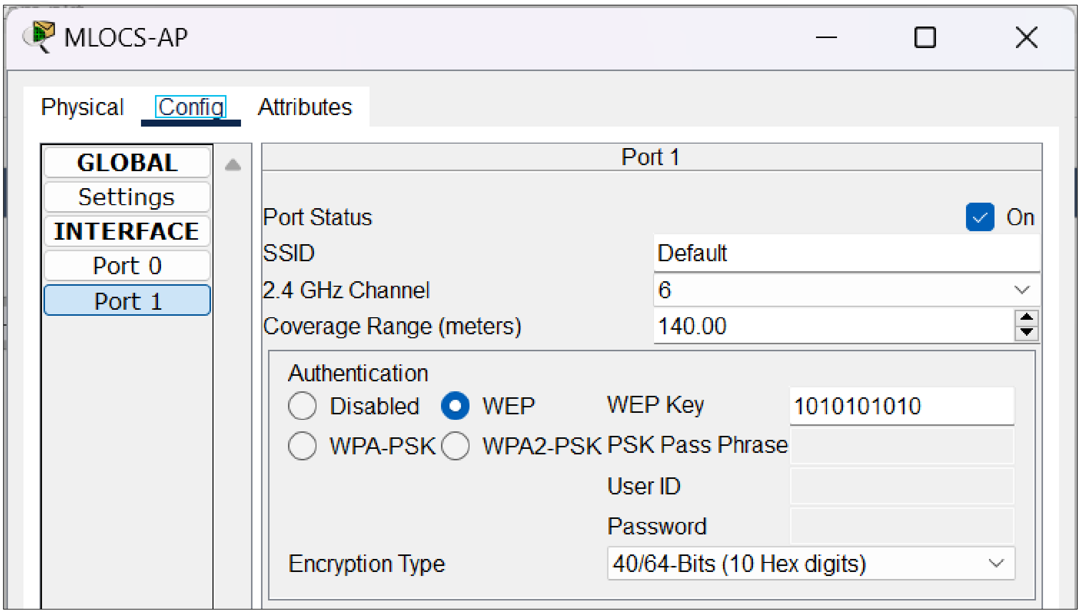
```
~  interface Tunnel 47
~  ip address 172.0.0.2 255.255.0.0
~  tunnel source Serial0/3/0
~  tunnel destination 192.168.3.2
```

– Wireless Connectivity

Access point is used for connecting Laptop and Smartphone to the network with authentication type **WEP.**

Step 1. Creating WEP key

Click on AP device, go to “Config”.
Click on Port 1
Click on WEP and type WEP key of 10 digit.



MLOCS-AP

Port 1

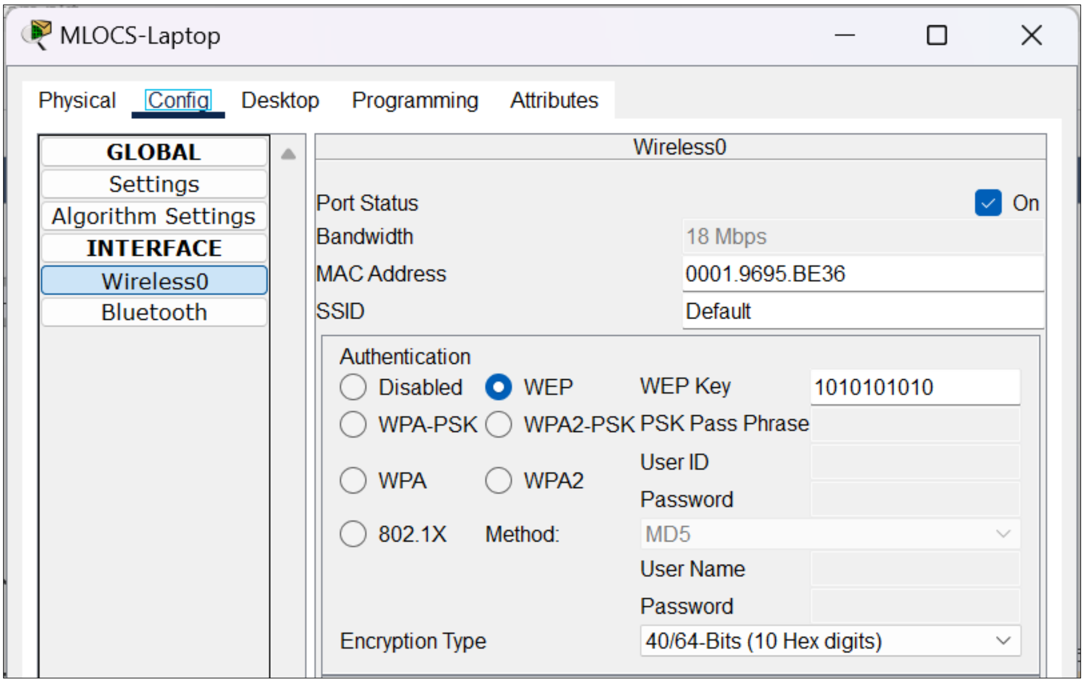
Port Status ☑ On
SSID: Default
2.4 GHz Channel: 6
Coverage Range (meters): 140.00

Authentication
○ Disabled ● WEP WEP Key: 1010101010
○ WPA-PSK ○ WPA2-PSK PSK Pass Phrase:
User ID:
Password:
Encryption Type: 40/64-Bits (10 Hex digits)

Figure 2.21

Step 2. Connecting devices

Click on Laptop/Smartphone, go to “Config”.
Click on Wireless0
Click on WEP and type WEP key.



MLOCS-Laptop

Wireless0

Port Status ☑ On
Bandwidth: 18 Mbps
MAC Address: 0001.9695.BE36
SSID: Default

Authentication
○ Disabled ● WEP WEP Key: 1010101010
○ WPA-PSK ○ WPA2-PSK PSK Pass Phrase:
○ WPA ○ WPA2 User ID:
Password:
○ 802.1X Method: MD5
User Name:
Password:
Encryption Type: 40/64-Bits (10 Hex digits)

Figure 2.22

Apply these steps on all other wireless devices.

REFERENCES

Book: CCNP Routing and Switching ROUTE 300-101 Official Cert Guide

Sources:

- https://www.routeralley.com/guides.html
- https://networklessons.com/cisco/ccna-200-301/introduction-to-ospf
- https://www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/networking-basics.html