# Chapter 1

# About the Institute

### 1.1 Overview

Karnataka German Multi Skill Development Centre (KGMSDC), a Society promoted by Government of India and Government of Karnataka with technical support of German International Services (GIZ-IS) has set up Karnataka German Technical Training Institute (KGTTI) having centres at Bengaluru and Gulbarga. The society was headed by the Chief Secretary of the Karnataka State.

### Vision

To develop KGMSDCs as world class training centres that offer specialized skills training programs in alignment with the Industry requirements in Karnataka and beyond.

### Mission

KGMSDCs will generate high quality skilled manpower in close association with the industry, while operating with operational flexibility and striving financial self-sustainability

### Training

- CNC Manufacturing: strong> CAD/CAM, CNC Programming & Operation, Metrology.
- Electronics Design & Manufacturing: SMT, Wave soldering, Embedded systems, VLSI, Electronics maintenance.
- Industrial Automation: PLC and Drives, Pneumatics, Hydraulics, Man-Machine Interface, Field Instrumentation
- Advanced Welding: MIG, MAG, TIG, Pipe Welding, International Welder.
- IT Hardware and Networking, CCNA, VM Ware
- Volkswagen Group - Service Advisor Talent Program (VG-SATP).
- All programs will follow German vocational standards that are demand oriented and directly imply a close relationship with industry. To provide International Standards and the hands-on training both KGTTI centres has extensive and state-of-art training facilities.

**Facilities**

KGTTI has excellent infrastructure with state-of-the-art facilities and operates within a professional framework, with a dynamic work culture and professional experts, placing special emphasis on result orientation and a thrust on client satisfaction. Using its expertise and facilities, it offers its services to all kinds of Industry. Besides industries it offers its services to Government Departments, to jobseekers and also to weaker section of the society.

**Our Strengths**

- Focus on Technology based services
- State-of the-art training labs and equipment
- Competence based training (CBT)
- Qualified, experienced professionals / experts
- Networking with expert organizations - of national and international repute
- Handling of prestigious Job works for Aeronautical Development Agency.
- Dynamic work culture, professional staff, emphasis on result orientation and thrust on client satisfaction
- Partners in representation CISCO (as authorized academy).

**Key Learning And Success**

- Timely completion of jobs as per requirement of client
- Ensuring customer satisfaction
- Developed competence in developing competence based training curriculum developing a system for its implementation
- Adopted system of dynamic work culture & organizational professionalism

# Chapter 2

# About the Department

## 2.1 Information Technology

Companies all over the world need talented people with the skills and know-how to drive their businesses forward into the networked economy. With expansion of operations of the Corporate, Information Technology has become an integral part of the business infrastructure. Almost all the industries and other organizations are using the technology for routine computing, office automation, project management and other business related activities. These activities need to interact continuously with each other using Local Area Networks and Wide Area Networks (LAN & WAN) to facilitate sharing of information and support decision making process.

Behind this technology revolution, you will find the integration of powerful, high-speed networks, secure servers, web-friendly applications and support services. Also the people with skills and knowledge to design, develop, deliver and maintain them.

## 2.2 Cisco Networking Academy

Cisco Networking Academy is a global education program that teaches students how to design, build, troubleshoot and secure computers and networks for increased access to career and economic opportunities in communities around the world. This program helps students build the next generation skills by encouraging practical application of knowledge through hand-on activities and complex network simulations using packet tracer and virtualization software on Cisco Device

The online courses provide access to all the benefits of Cisco Networking Academy programs and are designed to help students prepare for career opportunities, continuing education and globally recognized certifications.

KGTTI Bengaluru is an authorised Cisco Academy and Instructor Training Centre (ITC) for the SAARC region to provide quality training for students and Instructors.**IT ESSENTIALS**

This course provided an excellent introduction to information technology and overview of PC Hardware, Software and Network Operating Systems.

## 2.3 Course Outline - It Essentials

- Introduction to Personal Computers

- Lab Procedures and Tool Use
- Computer Assembly
- Overview of Preventive Maintenance
- Operating Systems
- Networks
- Laptops
- Mobile Devices
- Printers
- Security
- The IT Professional
- Advanced Troubleshooting

The course covers PC's, Laptops, Printers and associated peripherals, Assembling / Disassembling PC components, Wireless connectivity, Security, Safety and Environmental issues associated with installing, configuring troubleshooting a PC / associated peripheral devices. It also prepares the students for Comp TIA A+, Comp TIA N+, EUCIP IT Administrator Certifications.

### 2.4 CCNA Routing And Switching

Cisco Certified Network Associate (CCNA) Routing and Switching is a certifications program for entry-level network engineers that helps maximize your investment in foundational networking knowledge and increase the value of your employer's network. CCNA Routing and Switching is for Network Specialists, Network Administrators, and Network Support Engineers with 0-3 years of experience. The CCNA Routing and Switching validates the ability to install, configure, operate and troubleshoot medium-size routed and switched networks.

# Chapter 3

# Introduction

## 3.1 Exploring the Network

At a critical turning point in the use of technology to extend and empower our ability is to communicate. The globalization of the Internet has succeeded faster than anyone could have imagined. The manner in which social, commercial, political and personal interactions occur is rapidly changing to keep up with the evolution of this global network. In the next stage of our development, innovators will use the Internet as a starting point for their efforts, creating new products and services specifically designed to take advantage of the network capabilities. As developers push the limits of what is possible, the capabilities of the interconnected networks that form the Internet will play an increasing role in the success of these projects.

Overall chapter introduces the platform of data networks upon which our social and business relationships increasingly depend. The material lays the groundwork for exploring the services, technologies, and issues encountered by network professionals as they design, build, and maintain the modern network. The globalization of the Internet has ushered in new forms of communication that empower individuals to create information that can be accessed by a global audience.

Some forms of communication include:

- **Texting** – Texting enables instant real-time communication between two or more people.
- **Social Media** – Social media consists of interactive websites where people and communities create and share user-generated content with friends, family, peers, and the world.
- **Blogs** - Blogs, which is an abbreviation of the word “weblogs”, are web pages that are easy to update and edit. Unlike commercial websites, blogs give anyone a means to communicate their thoughts to a global audience without technical knowledge of web design.
- **Wikis** - Wikis are web pages that groups of people can edit and view together. Whereas a blog is more of an individual, personal journal, a wiki is a group creation. As such, it may

be subject to more extensive review and editing. Many businesses use wikis as their internal collaboration tool.

- **Podcasting** - Podcasting allows people to deliver their audio recordings to a wide audience. The audio file is placed on a website (or blog or wiki) where others can download it and play the recording on their computers, laptops, and other mobile devices.

- **Peer-to-Peer (P2P) File Sharing** – Peer-to-Peer file sharing allows people to share files with each other without having to store and download them from a central server. The user joins the P2P network by simply installing the P2P software. P2P file sharing has not been embraced by everyone. Many people are concerned about violating the laws of copyrighted materials.

## 3.2 LANs, WANs and the Internet

The path that a message takes from source to destination can be as simple as a single cable connecting one computer to another, or as complex as a collection of networks that literally spans the globe. This network infrastructure provides the stable and reliable channel over which these communications occur.

The network infrastructure contains three categories of network components:

- Devices
- Media
- Services

Click each button in the figure to highlight the corresponding network components.

Devices and media are the physical elements, or hardware, of the network. Hardware is often the visible components of the network platform such as a laptop, PC, switch, router, wireless access point, or the cabling used to connect the devices.

Services include many of the common network applications people use every day, like email hosting services and web hosting services. Processes provide the functionality that directs and

moves the messages through the network. Processes are less obvious to us but are critical to the operation of networks.

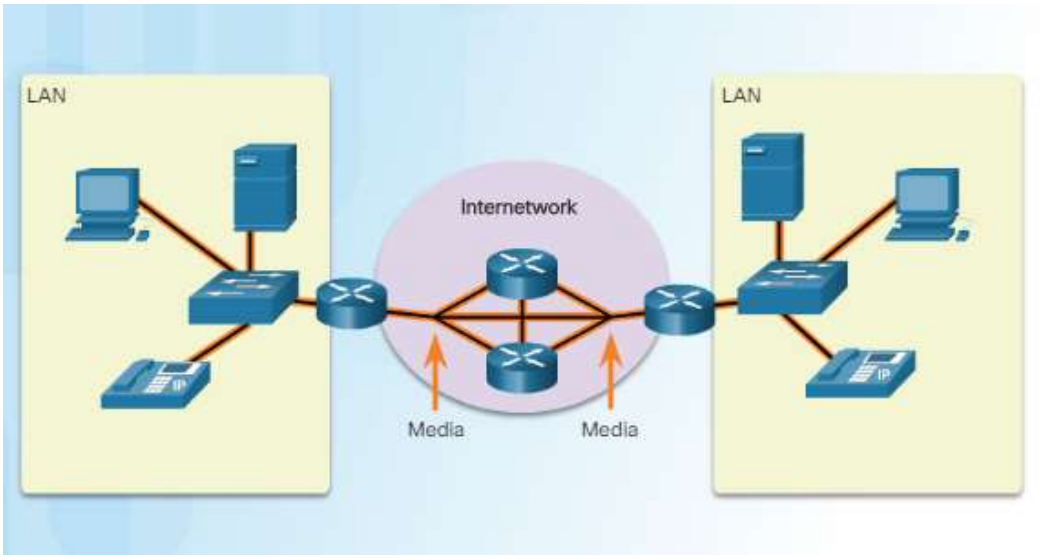


**Figure 3.1: Components of a Network - Media**

### 3.2.1 Network Media

Communication across a network is carried on a medium. The medium provides the channel over which the message travels from source to destination.

Modern networks primarily use three types of media to interconnect devices and to provide the pathway over which data can be transmitted. As shown in Figure 1, these media are:

- **Metallic wires within cables** - data is encoded into electrical impulses
- **Glass or plastic fibers (fiber optic cable)** - data is encoded as pulses of light
- **Wireless transmission** - data is encoded using wavelengths from the electromagnetic spectrum

Different types of network media have different features and benefits. Not all network media have the same characteristics, nor are they all appropriate for the same purpose.

## 3.3 Application Layer

The application layer is closest to the end user. As shown in the figure, it is the layer that provides the interface between the applications used to communicate and the underlying network over which messages are transmitted. Application layer protocols are used to exchange data between programs running on the source and destination hosts.

The upper three layers of the OSI model (application, presentation, and session) define functions of the single TCP/IP application layer.

There are many application layer protocols, and new protocols are always being developed. Some of the most widely known application layer protocols include Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Trivial File Transfer Protocol (TFTP), Internet Message Access Protocol (IMAP), and Domain Name System (DNS) protocol.

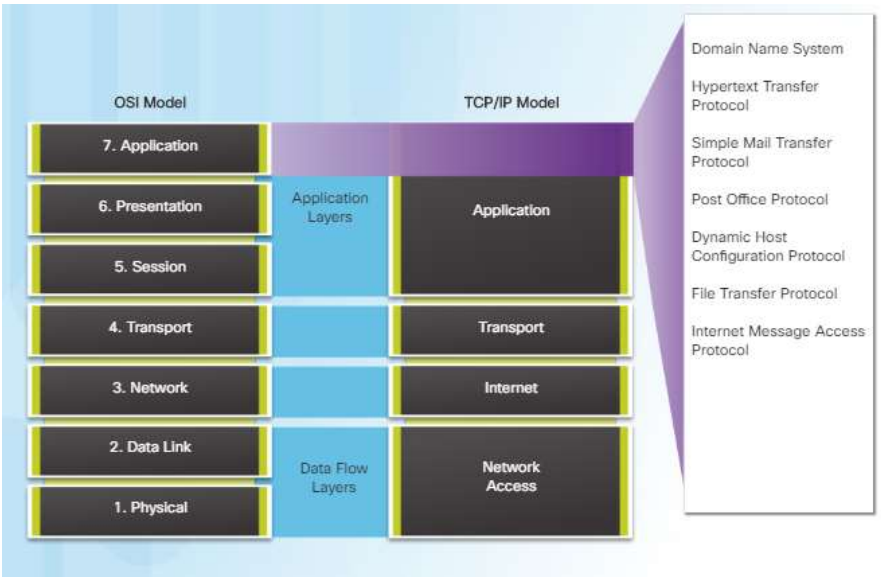


**Figure 3.2: OSI Model**

### 3.3.1 Client – Server Model

In the client-server model, the device requesting the information is called a client and the device responding to the request is called a server. Client and server processes are considered to be in the application layer. The client begins the exchange by requesting data from the server, which responds by sending one or more streams of data to the client. Application layer protocols describe the format of the requests and responses between clients and servers. In addition to

the actual data transfer, this exchange may also require user authentication and the identification of a data file to be transferred.

One example of a client-server network is using an ISP's email service to send, receive and store email. The email client on a home computer issues a request to the ISP's email server for any unread mail. The server responds by sending the requested email to the client. As shown in the figure, data transfer from a client to a server is referred to as an upload and data from a server to a client as a download.

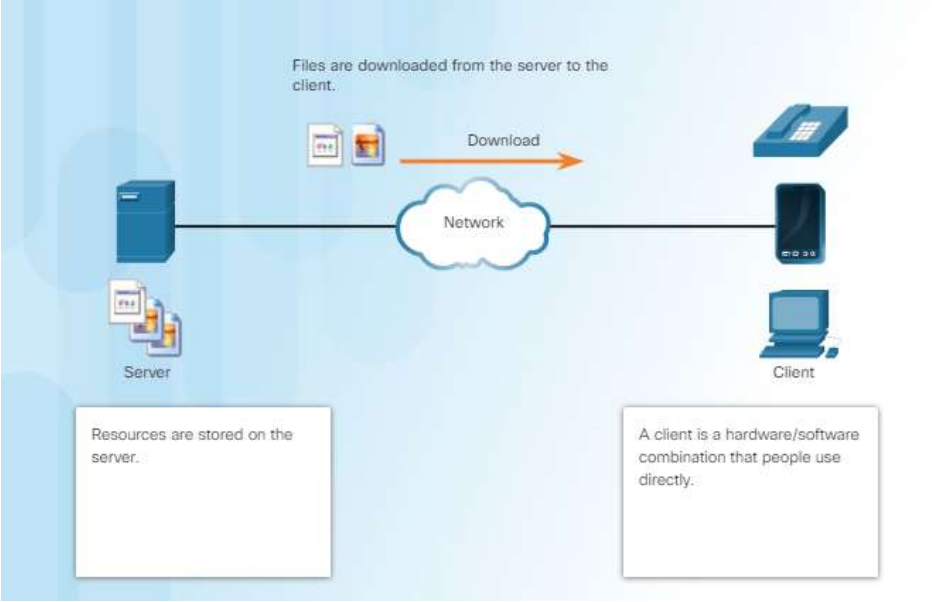


**Figure 3.3: Client – Server Model**

## 3.3.2 HTTP and HTTPS

HTTP is a request/response protocol. When a client, typically a web browser, sends a request to a web server, HTTP specifies the message types used for that communication. The three common message types are GET, POST, and PUT (see the figure):

- **GET** - A client request for data. A client (web browser) sends the GET message to the web server to request HTML pages.
- **POST** - Uploads data files to the web server such as form data.
- **PUT** - Uploads resources or content to the web server such as an image.

Although HTTP is remarkably flexible, it is not a secure protocol. The request messages send information to the server in plain text that can be intercepted and read. The server responses, typically HTML pages, are also unencrypted.

For secure communication across the Internet, the HTTP Secure (HTTPS) protocol is used. HTTPS uses authentication and encryption to secure data as it travels between the client and server. HTTPS uses the same client request-server response process as HTTP, but the data stream is encrypted with Secure Socket Layer (SSL) before being transported across the network.

## 3.4 Types of Malware

Malware or malicious code (malcode) is short for malicious software. It is code or software that is specifically designed to damage, disrupt, steal, or inflict "bad" or illegitimate action on data, hosts, or networks. Viruses, worms, and Trojan horses are types of malware.

**Viruses**

A computer virus is a type of malware that propagates by inserting a copy of itself into, and becoming part of, another program. It spreads from one computer to another, leaving infections as it travels. Viruses can range in severity from causing mildly annoying effects to damaging data or software and causing denial-of-service (DoS) conditions. Almost all viruses are attached to an executable file, which means the virus may exist on a system but will not be active or able to spread until a user runs or opens the malicious host file or program. When the host code is executed, the viral code is executed as well. Normally, the host program keeps functioning after it is infected by the virus. However, some viruses overwrite other programs with copies of themselves, which destroys the host program altogether. Viruses spread when the software or document they are attached to is transferred from one computer to another using the network, a disk, file sharing, or infected e-mail attachments.

**Worms**

Computer worms are similar to viruses in that they replicate functional copies of themselves and can cause the same type of damage. In contrast to viruses, which require the spreading of an infected host file, worms are standalone software and do not require a host program or human help to propagate. A worm does not need to attach to a program to infect a host and

enter a computer through a vulnerability in the system. Worms take advantage of system features to travel through the network unaided.

**Trojan Horses**

A Trojan horse is another type of malware named after the wooden horse the Greeks used to infiltrate Troy. It is a harmful piece of software that looks legitimate. Users are typically tricked into loading and executing it on their systems. After it is activated, it can achieve any number of attacks on the host, from irritating the user (popping up windows or changing desktops) to damaging the host (deleting files, stealing data, or activating and spreading other malware, such as viruses). Trojan horses are also known to create back doors to give malicious users access to the system.

### 3.4.1 Firewalls

A firewall is one of the most effective security tools available for protecting users from external threats. Network firewalls reside between two or more networks, control the traffic between them, and help prevent unauthorized access. Host-based firewalls or personal firewalls are installed on end systems. Firewall products use various techniques for determining what is permitted or denied access to a network. These techniques are:

- **Packet filtering** - Prevents or allows access based on IP or MAC addresses
- **Application filtering** - Prevents or allows access by specific application types based on port numbers
- **URL filtering** - Prevents or allows access to websites based on specific URLs or keywords
- **Stateful packet inspection (SPI)** - Incoming packets must be legitimate responses to requests from internal hosts. Unsolicited packets are blocked unless permitted specifically. SPI can also include the capability to recognize and filter out specific types of attacks, such as denial of service (DoS).Firewall products may support one or more of these filtering capabilities. Firewall products come packaged in various forms, as shown in the figure. Click each type to see more information.

### 3.4.2 The Traceroute and Tracert Command

Designed as a variation of the **traceroute** command, the extended **traceroute** command allows the administrator to adjust parameters related to the command operation. This is helpful when troubleshooting routing loops, determining the exact next-hop router, or to help determine where packets are getting dropped by a router, or denied by a firewall. While the extended ping command can be used to determine the type of connectivity problem, the extended **traceroute** command is useful in locating the problem.

Similar to ping, the Windows implementation of traceroute (tracert) sends ICMP Echo Requests. Unlike ping, the first IPv4 packet has a TTL value of one. Routers decrement TTL values by one before forwarding the packet. If the TTL value is decremented to zero, the router will drop the packet and return an ICMP Time Exceeded message back to the source. Each time the source of the traceroute receives an ICMP Time Exceeded message, it displays the source IPv4 address of the ICMP Time Exceeded message, increments the TTL by one and sends another ICMP Echo Request.

As each new ICMP Echo Request is sent, it makes it to one router more than the last Echo Request before receiving another ICMP Time Exceeded message.

Traceroute uses the returned ICMP Time Exceeded messages to display a list of routers that the IPv4 packets traverse on their way to the final destination, the destination IPv4 address of the traceroute. When the packet reaches the final destination, the source returns an ICMP Echo Reply.

Cisco IOS uses a slightly different approach with traceroute, which does not use ICMP Echo Requests. Instead, IOS sends out a sequence of UDP datagrams, each with incrementing TTL values and destination port numbers. The port number is an invalid port number (Cisco uses a default of 33434), and is incremented along with the TTL. Similar to the Windows implementation, when a router decrements the TTL to zero, it will return an ICMP Time Exceeded message back to the source. This informs the source of the IPv4 address of each router along the path.

When the packet reaches the final destination, because these datagrams tried to access an invalid port at the destination host, the host responds with an ICMP type 3, code 3 message

that indicates the port was unreachable. This event signals to the source of the traceroute that the traceroute program has reached its destination.

## 3.5 Transport Layer

The transport layer is responsible for establishing a temporary communication session between two applications and delivering data between them. An application generates data that is sent from an application on a source host to an application on a destination host. This is without regard to the destination host type, the type of media over which the data must travel, the path taken by the data, the congestion on a link, or the size of the network. As shown in the figure, the transport layer is the link between the application layer and the lower layers that are responsible for network transmission.

### 3.5.1 TCP Protocol

TCP transport is analogous to sending packages that are tracked from source to destination. If a shipping order is broken up into several packages, a customer can check online to see the order of the delivery.

With TCP, there are three basic operations of reliability:

- Numbering and tracking data segments transmitted to a specific host from a specific application
- Acknowledging received data
- Retransmitting any unacknowledged data after a certain period of time

## Features :

To understand the differences between TCP and UDP, it is important to understand how each protocol implements specific reliability features and how they track conversations. In addition to supporting the basic functions of data segmentation and reassembly, TCP, as shown in the figure, also provides other services. By numbering and sequencing the segments, TCP can ensure that these segments are reassembled into the proper order.

**1) Establishing a Session**

TCP is a connection-oriented protocol. A connection-oriented protocol is one that negotiates and establishes a permanent connection (or session) between source and destination devices prior to forwarding any traffic. Through session establishment, the devices negotiate the amount of traffic that can be forwarded at a given time, and the communication data between the two can be closely managed.

**2) Reliable Delivery**

In networking terms, reliability means ensuring that each segment that the source sends arrives at the destination. For many reasons, it is possible for a segment to become corrupted or lost completely, as it is transmitted over the network.

**3) Same-Order Delivery**

Because networks may provide multiple routes that can have different transmission rates, data can arrive in the wrong order. By numbering and sequencing the segments, TCP can ensure that these segments are reassembled into the proper order.

**4) Flow Control**

Network hosts have limited resources, such as memory and processing power. When TCP is aware that these resources are overtaxed, it can request that the sending application reduce the rate of data flow. This is done by TCP regulating the amount of data the source transmits. Flow control can prevent the need for retransmission of the data when the receiving host's resources are overwhelmed.

## 3.5.2 UDP Protocol

While the TCP reliability functions provide more robust communication between applications, they also incur additional overhead and possible delays in transmission. There is a trade-off between the value of reliability and the burden it places on network resources. Adding overhead to ensure reliability for some applications could reduce the usefulness of the application and can even be detrimental. In such cases, UDP is a better transport protocol.

UDP provides the basic functions for delivering data segments between the appropriate applications, with very little overhead and data checking. UDP is known as a best-effort delivery protocol. In the context of networking, best-effort delivery is referred to as unreliable because there is no acknowledgment that the data is received at the destination. With UDP, there are no transport layer processes that inform the sender of a successful delivery.

UDP is similar to placing a regular, non-registered, letter in the mail. The sender of the letter is not aware of the availability of the receiver to receive the letter. Nor is the post office responsible for tracking the letter or informing the sender if the letter does not arrive at the final destination.

### Features :

User Datagram Protocol (UDP) is considered a best-effort transport protocol. UDP is a lightweight transport protocol that offers the same data segmentation and reassembly as TCP, but without TCP reliability and flow control. UDP is such a simple protocol that it is usually described in terms of what it does not do compared to TCP.

## 3.5.3 TCP Three - way Handshake Analysis

Hosts track each data segment within a session and exchange information about what data is received using the information in the TCP header. TCP is a full-duplex protocol, where each connection represents two one-way communication streams or sessions. To establish the connection, the hosts perform a three-way handshake. Control bits in the TCP header indicate the progress and status of the connection.

The three-way handshake:

- Establishes that the destination device is present on the network
- Verifies that the destination device has an active service and is accepting requests on the destination port number that the initiating client intends to use
- Informs the destination device that the source client intends to establish a communication session on that port number

After the communication is completed, the sessions are closed, and the connection is terminated. The connection and session mechanisms enable TCP's reliability function.

The six bits in the Control Bits field of the TCP segment header are also known as flags. A flag is a bit that is either set to on or off. Click the Control Bits field in the figure to see all six flags. We have discussed SYN, ACK, and FIN. The RST flag is used to reset a connection when an error or timeout occurs. Click here to learn more about the PSH and URG flags.

## 3.6 IP Addressing

Addressing is a critical function of network layer protocols. Addressing enables data communication between hosts, regardless of whether the hosts are on the same network, or on different networks. Both Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) provide hierarchical addressing for packets that carry data.

Designing, implementing and managing an effective IP addressing plan ensures that networks can operate effectively and efficiently.

# Chapter 4

# Routing and Switching Essentials

## 4.1 Routing Concepts

A router connects one network to another network. The router is responsible for the delivery of packets across different networks. The destination of the IP packet might be a web server in another country or an email server on the local area network.

### 4.1.1 Routers Interconnect Networks

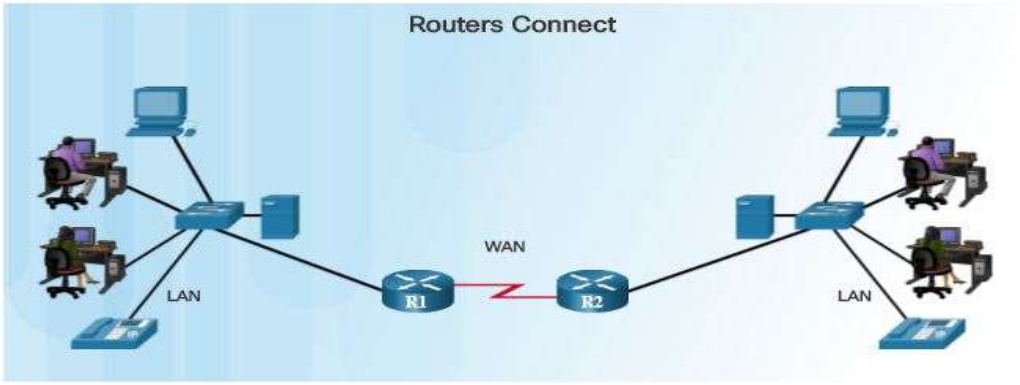


**Figure 4.1: Routers Interconnect Network**

A router connects multiple networks, which means that it has multiple interfaces that each belongs to a different IP network. When a router receives an IP packet on one interface, it determines which interface to use to forward the packet to the destination. The interface that the router uses to forward the packet may be the final destination, or it may be a network connected to another router that is used to reach the destination network.

### 4.1.2 Routers Choose Best Paths

The primary functions of a router are to:

- Determine the best path to send packets
- Forward packets toward their destination

The router uses its routing table to determine the best path to use to forward a packet. When the router receives a packet, it examines the destination address of the packet and uses the routing table to search for the best path to that network. The routing table also includes the interface to be used to forward packets for each known network. When a match is found, the router encapsulates the packet into the data link frame of the outgoing or exit interface, and the packet is forwarded toward its destination.

### 4.1.3 The Routing Table

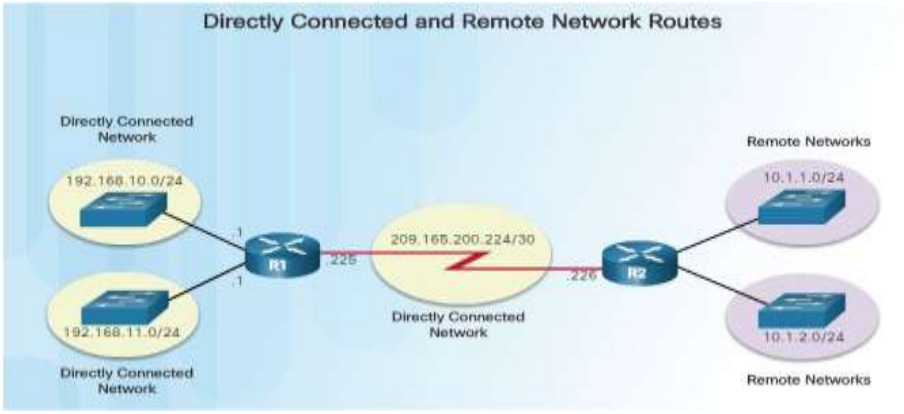


**Figure 4.2: Routing Table**

The routing table of a router stores information about:

- **Directly connected routes** - These routes come from the active router interfaces. Routers add a directly connected route when an interface is configured with an IP address and is activated.
- **Remote routes** - These are remote networks connected to other routers. Routes to these networks can either be statically configured or dynamically learned through dynamic routing protocols.

## 4.2 Static Routing.

Routers learn about remote networks either dynamically, using routing protocols, or manually, or using static routes. In many cases, routers use a combination of both dynamic routing protocols and static routes. This chapter focuses on static routing. Static routes are manually configured. They define an explicit path between two networking devices. The static routes must be manually reconfigured if the network topology changes.

Static routes are very common and do not require the same amount of processing and overhead as dynamic routing protocols.

### 4.2.1 Default Static Route

A default route is a route that matches all packets and is used by the router if a packet does not match any other, more specific route in the routing table. A default route can be dynamically learned or statically configured. A default static route is simply a static route with 0.0.0.0/0 as the destination IPv4 address. Configuring a default static route creates a Gateway of Last Resort.

Default static routes are used:

- When no other routes in the routing table match the packet destination IP address. In other words, when a more specific match does not exist. A common use is when connecting a company's edge router to the ISP network.
- When a router has only one other router to which it is connected. In this situation, the router is known as a stub router.

### 4.2.2 The ip route Command

Static routes are configured using the **ip route** global configuration command. The basic syntax for the command is:

- **ip route** network-address subnet-mask {ip-address | exit-intf}

The following parameters are required to configure static routing:

- network-address - Destination network address of the remote network to be added to the routing table, often this is referred to as the prefix.
- subnet-mask - Subnet mask, or just mask, of the remote network to be added to the routing table. The subnet mask can be modified to summarize a group of networks.

One or both of the following parameters must also be used:

- ip-address - The IP address of the connecting router to use to forward the packet to the remote destination network. Commonly referred to as the next hop.

- exit-intf - The outgoing interface to use to forward the packet to the next hop.

The basic command syntax of a default static route is:

- **ip route 0.0.0.0 0.0.0.0** {ip-address | exit-intf}

## 4.3 Dynamic Routing

Routers forward packets by using information in the routing table. Routes to remote networks can be learned by the router in two ways: static routes and dynamic routes.

A dynamic routing protocol allows the routers to automatically learn about the networks from other routers. These networks, and the best path to each, are added to the routing table of the router, and identified as a network learned by a specific dynamic routing protocol.

Dynamic routing protocols are used by routers to share information about the reachability and status of remote networks. Dynamic routing protocols perform several activities, including network discovery and maintaining routing tables.

### 4.3.1 Dynamic Routing Protocol Components

Routing protocols are used to facilitate the exchange of routing information between routers. A routing protocol is a set of processes, algorithms, and messages that are used to exchange routing information and populate the routing table with the routing protocol's choice of best paths. The purpose of dynamic routing protocols includes:

- Discovery of remote network
- Maintaining up-to-date routing information
- Choosing the best path to destination network
- Ability to find a new best path if the current path is no longer available

The main components of dynamic routing protocols include:

- **Data structures -** Routing protocols typically use tables or databases for its operations. This information is kept in RAM.

- **Routing protocol messages -** Routing protocols use various types of messages to discover neighbouring routers, exchange routing information, and other tasks to learn and maintain accurate information about the network.
- **Algorithm -** An algorithm is a finite list of steps used to accomplish a task. Routing protocols use algorithms for facilitating routing information and for best path determination.

### 4.3.2 Router RIP Configuration Mode

RIPv1 is used as the dynamic routing protocol. To enable RIP, use the router rip command in global configuration mode as follows:

R1(config)# **router rip**

R1(config-router)# **network 192.168.1.0**

R1(config-router)# **network 192.168.2.0**

To enable RIP routing for a network, use the **network** network-address router configuration mode command. Enter the classful network address for each directly connected network. This command:

- Enables RIP on all interfaces that belong to a specific network. Associated interfaces now both send and receive RIP updates.
- Advertises the specified network in RIP routing updates sent to other routers every 30 second.

## 4.4 Switched Networks

Modern networks continue to evolve to keep pace with the changing way organizations carry out their daily business. Users now expect instant access to company resources from anywhere and at any time. These resources not only include traditional data, but also video and voice. There is also an increasing need for collaboration technologies. These technologies allow real-time sharing of resources between multiple remote individuals, as though they were at the same physical location.

Different devices must seamlessly work together to provide a fast, secure, and reliable connection between hosts. LAN switches provide the connection point for end users into the enterprise network and are also primarily responsible for the control of information within the LAN environment. Routers facilitate the movement of information between LANs, and are generally unaware of individual hosts. All advanced services depend on the availability of a robust routing and switching infrastructure on which they can build. This infrastructure must be carefully designed, deployed, and managed, to provide a stable platform.

### 4.4.1 Role of Switched Networks

The role of switched networks has evolved dramatically in the last two decades. It was not long ago that flat Layer 2 switched networks were the norm. Flat Layer 2 switched networks relied on the Ethernet and the widespread use of hub repeaters to propagate LAN traffic throughout an organization. As shown in Figure 4.1, networks have fundamentally changed to switched LANs in a hierarchical network. A switched LAN allows more flexibility, traffic management, and additional features:

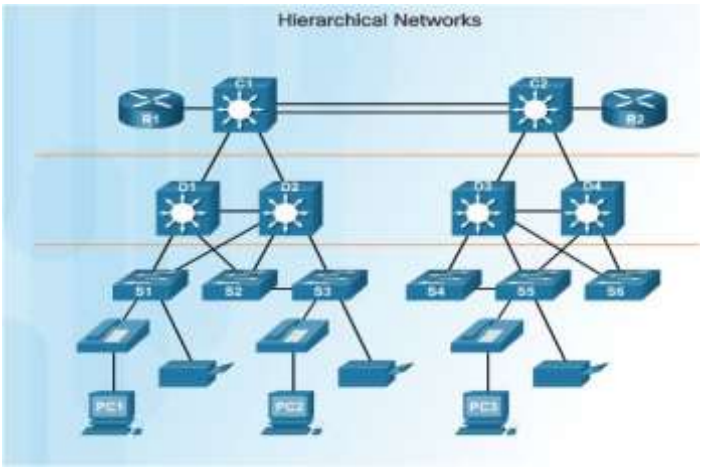


**Figure 4.3: Role of Switched Networks**

A switched LAN allows more flexibility, traffic management, and additional features:

- Quality of service
- Additional security
- Support for wireless networking and connectivity
- Support for new technologies, such as IP telephony and mobility services

### 4.4.2 Collision Domains

In hub-based Ethernet segments, network devices compete for the medium, because devices must take turns when transmitting. The network segments that share the same bandwidth between devices are known as collision domains. When two or more devices within that the same collision domain try to communicate at the same time, a collision will occur.

## 4.5 Switch Configuration

Switches are used to connect multiple devices together on the same network. In a properly designed network, LAN switches are responsible for directing and controlling the data flow at the access layer to networked resources.

### 4.5.1 SSH Operation

Secure Shell (SSH) is a protocol that provides a secure (encrypted) management connection to a remote device. SSH should replace Telnet for management connections. Telnet is an older protocol that uses unsecure plaintext transmission of both the login authentication (username and password) and the data transmitted between the communicating devices. SSH provides security for remote connections by providing strong encryption when a device is authenticated (username and password) and also for the transmitted data between the communicating devices. SSH is assigned to TCP port 22. Telnet is assigned to TCP port 23.

### 4.5.2 Configuring SSH

Before configuring SSH, the switch must be minimally configured with a unique hostname and the correct network connectivity settings.

**Step 1. Verify SSH support.**

Use the **show ip ssh** command to verify that the switch supports SSH. If the switch is not running an IOS that supports cryptographic features, this command is unrecognized.

**Step 2. Configure the IP domain :**Configure the IP domain name of the network using the **ip domain-name** domain-name global configuration mode command. In Figure 1, the domain-name value is **cisco.com**.

**Step 3. Generate RSA key pairs.**

Not all versions of the IOS default to SSH version 2, and SSH version 1 has known security flaws. To configure SSH version 2, issue the **ip ssh version 2** global configuration mode command. Generating an RSA key pair automatically enables SSH. Use the **crypto key generate rsa** global configuration mode command to enable the SSH server on the switch and generate an RSA key pair. When generating RSA keys, the administrator is prompted to enter a modulus length. The sample configuration in Figure 1 uses a modulus size of 1,024 bits. A longer modulus length is more secure, but it takes longer to generate and to use.

## 4.6 VLANs

VLANs allow an administrator to segment networks based on factors such as function, project team, or application, without regard for the physical location of the user or device. Each VLAN is considered a separate logical network. Devices within a VLAN act as if they are in their own independent network, even if they share a common infrastructure with other VLANs. Any switch port can belong to a VLAN. Unicast, broadcast, and multicast packets are forwarded and flooded only to end devices within the VLAN where the packets are sourced. Packets destined for devices that do not belong to the VLAN must be forwarded through a device that supports routing.

### 4.6.1 Types of VLANs

**Data VLAN**

A data VLAN is a VLAN that is configured to carry user-generated traffic. A VLAN carrying voice or management traffic would not be a data VLAN. It is common practice to separate voice and management traffic from data traffic. A data VLAN is sometimes referred to as a user VLAN. Data VLANs are used to separate the network into groups of users or devices.

**Default VLAN**

All switch ports become a part of the default VLAN after the initial boot up of a switch loading the default configuration. Switch ports that participate in the default VLAN are part of the same broadcast domain. This allows any device connected to any switch port to communicate with other devices on other switch ports. The default VLAN for Cisco switches is VLAN 1.

**Native VLAN**

A native VLAN is assigned to an 802.1Q trunk port. Trunk ports are the links between switches that support the transmission of traffic associated with more than one VLAN. An 802.1Q trunk port supports traffic coming from many VLANs (tagged traffic), as well as traffic that does not come from a VLAN (untagged traffic). Tagged traffic refers to traffic that has a 4-byte tag inserted within the original Ethernet frame header, specifying the VLAN to which the frame belongs. The 802.1Q trunk port places untagged traffic on the native VLAN, which by default is VLAN 1.

**Management VLAN**

A management VLAN is any VLAN configured to access the management capabilities of a switch. VLAN 1 is the management VLAN by default. To create the management VLAN, the switch virtual interface (SVI) of that VLAN is assigned an IP address and a subnet mask, allowing the switch to be managed via HTTP, Telnet, SSH, or SNMP. Because the out-of-the-box configuration of a Cisco switch has VLAN 1 as the default VLAN, VLAN 1 would be a bad choice for the management VLAN.

## 4.6.2 Creating a VLAN

The Cisco IOS command syntax used to add a VLAN to a switch is as below and give it a name. Naming each VLAN is considered a best practice in switch configuration.

S1(config)# **vlan** vlan_id

S1(config-vlan)# **name** vlan_name

S1(config-vlan)# **exit**

## 4.7 Access Control Lists

One of the most important skills a network administrator needs is mastery of access control lists (ACLs). ACLs provide security for a network. An ACL is a series of IOS commands that control whether a router forwards or drops packets based on information found in the packet header. ACLs are among the most commonly used features of Cisco IOS software.

## 4.7.1 ACL Operation

ACLs can be configured to apply to inbound traffic and outbound traffic.

Inbound ACLs - Incoming packets are processed before they are routed to the outbound interface. An inbound ACL is efficient because it saves the overhead of routing lookups if the packet is discarded. If the packet is permitted by the ACL, it is then processed for routing. Inbound ACLs are best used to filter packets when the network attached to an inbound interface is the only source of packets that need to be examined.

Outbound ACLs - Incoming packets are routed to the outbound interface, and then they are processed through the outbound ACL. Outbound ACLs are best used when the same filter will be applied to packets coming from multiple inbound interfaces before exiting the same outbound interface.

## 4.7.2 Calculating the Wildcard Mask

Calculating wildcard masks can be challenging. One shortcut method is to subtract the subnet mask from 255.255.255.255.

For example, assume you wanted to permit access to all users in the 192.168.3.0 network. Because the subnet mask is 255.255.255.0, you could take the 255.255.255.255 and subtract the subnet mask 255.255.255.0. The solution produces the wildcard mask 0.0.0.255.

**255 . 255 . 255 . 255** ⟶ SUBNET MASK

**-- 255 . 255 . 255 . 0**

**0 . 0 . 0 . 255** ⟶ WILDCARD MASK

Consider an example in which you need to match networks in the range between 192.168.16.0/24 to 192.168.31.0/24. These networks would summarize to 192.168.16.0/20. In this case, 0.0.15.255 is the correct wildcard mask to configure one efficient ACL statement, as shown: R1(config)# **access-list 10 permit 192.168.16.0 0.0.15.255**

# Chapter 5

# Scaling Networks

## 5.1 LAN Design

### 5.1.1 Introduction to LAN Design

There is a tendency to discount the network as just simple plumbing, to think that all you have to consider is the size and the length of the pipes or the speeds and feeds of the links, and to dismiss the rest as unimportant. Just as the plumbing in a large stadium or high rise has to be designed for scale, purpose, redundancy, protection from tampering or denial of operation, and the capacity to handle peak loads, the network requires similar consideration. As users depend on the network to access the majority of the information they need to do their jobs and to transport their voice or video with reliability, the network must be able to provide resilient, intelligent transport.

As a business grows, so does its networking requirements. Businesses rely on the network infrastructure to provide mission-critical services. Network outages can result in lost revenue and lost customers. Network designers must design and build an enterprise network that is scalable and highly available.

### 5.1.2 Hierarchical Design Model

The campus wired LAN uses a hierarchical design model to break the design up into modular groups or layers. Breaking the design up into layers allows each layer to implement specific functions, which simplifies the network design and therefore the deployment and management of the network.

The campus wired LAN enables communications between devices in a building or group of building, as well as interconnection to the WAN and internet edge at the network core.

A hierarchical LAN design includes the following three layers, as shown in Figure 5.1:

- Access layer
- Distribution layer

- Core layer

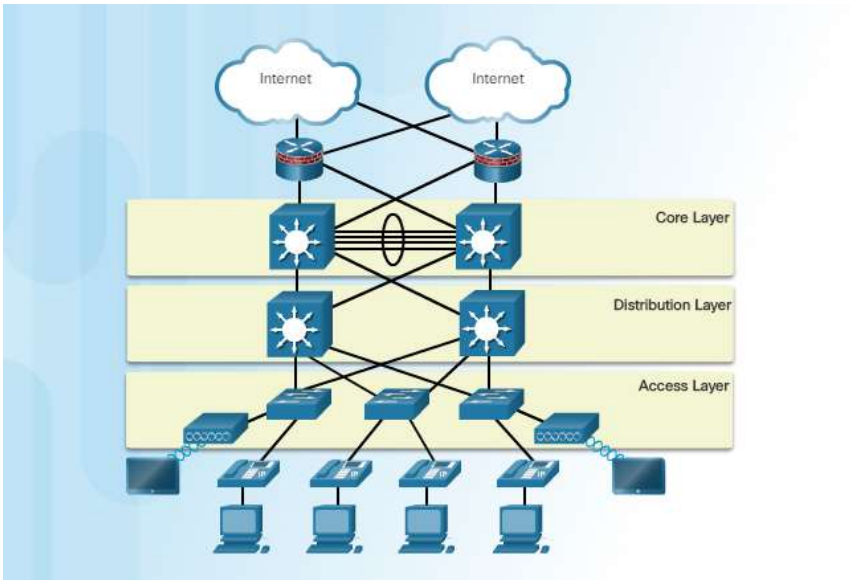


**Figure 5.1: Hierarchical Design Model**

Each layer is designed to meet specific functions.

The access layer provides endpoints and users direct access to the network. The distribution layer aggregates access layers and provides connectivity to services. Finally, the core layer provides connectivity between distribution layers for large LAN environments. User traffic is initiated at the access layer and passes through the other layers if the functionality of those layers is required.

Even though the hierarchical model has three layers, some smaller enterprise networks may implement a two-tier hierarchical design. In a two-tier hierarchical design, the core and distribution layers are collapsed into one layer, reducing cost and complexity.

In flat or meshed network architectures, changes tend to affect a large number of systems. Hierarchical design helps constrain operational changes to a subset of the network, which makes it easy to manage as well as improve resiliency. Modular structuring of the network into small, easy-to-understand elements also facilitates resiliency via improved fault isolation.

**5.1.3 Failure Domain:** A well-designed network not only controls traffic, but also limits the size of failure domains. A failure domain is the area of a network that is impacted when a critical device or network service experiences problems.

The function of the device that initially fails determines the impact of a failure domain. For example, a malfunctioning switch on a network segment normally affects only the hosts on that segment. However, if the router that connects this segment to others fails, the impact is much greater.

The use of redundant links and reliable enterprise-class equipment minimize the chance of disruption in a network. Smaller failure domains reduce the impact of a failure on company productivity. They also simplify the troubleshooting process, thereby, shortening the downtime for all users.

## 5.2 Selecting Network Devices

### 5.2.1 Routing Requirements

In the distribution layer of an enterprise network, routing is required. Without the routing process, packets cannot leave the local network.

Routers play a critical role in networking by connecting homes and businesses to the Internet, interconnecting multiple sites within an enterprise network, providing redundant paths, and connecting ISPs on the Internet. Routers can also act as a translator between different media types and protocols. For example, a router can accept packets from an Ethernet network and re-encapsulate them for transport over a Serial network.

Routers use the network portion of the destination IP address to route packets to the proper destination. They select an alternate path if a link or path goes down. All hosts on a local network specify the IP address of the local router interface in their IP configuration. This router interface is the default gateway. The ability to route efficiently and recover from network link failures is critical to delivering packets to their destination.

Routers also serve other beneficial functions:

- Provide broadcast containment
- Connect remote locations
- Group users logically by application or department

- Provide enhanced security

## 5.2.2 Cisco Routers

As the network grows, it is important to select the proper routers to meet its requirements. As shown in the figure, there are three categories of routers:

- **Branch Routers** - Branch routers optimize branch services on a single platform while delivering an optimal application experience across branch and WAN infrastructures. Maximizing service availability at the branch requires networks designed for 24x7x365 uptime. Highly available branch networks must ensure fast recovery from typical faults, while minimizing or eliminating the impact on service, and provide simple network configuration and management.


**Figure 5.2: Cisco Routers**

- **Network Edge Routers** - Network edge routers enable the network edge to deliver high-performance, highly secure, and reliable services that unite campus, data center, and branch networks. Customers expect a high-quality media experience and more types of content than ever before. Customers want interactivity, personalization, mobility, and control for all content. Customers also want to access content anytime and anyplace they choose, over any device, whether at home, at work, or on the go. Network edge routers must deliver enhanced quality of service and nonstop video and mobile capabilities.

- **Service Provider Routers** - Service provider routers differentiate the service portfolio and increase revenues by delivering end-to-end scalable solutions and subscriber-aware services. Operators must optimize operations, reduce expenses, and improve scalability and flexibility, to deliver next-generation Internet experiences across all devices and locations. These systems are designed to simplify and enhance the operation and deployment of service-delivery networks.

## 5.3 Dynamic Routing

The data networks that we use in our everyday lives to learn, play, and work range from small, local networks to large, global internetworks. A home network may have a router and two or more computers. At work, an organization may have multiple routers and switches servicing the data communication needs of hundreds, or even thousands, of end devices.

Routers forward packets by using information in the routing table. Routes to remote networks can be learned by the router in two ways: static routes and dynamic routes.

### 5.3.1 Classification of Routing Protocols

Dynamic routing protocols are used to facilitate the exchange of routing information between routers. A routing protocol is a set of processes, algorithms, and messages that are used to exchange routing information and populate the routing table with the routing protocol's choice of best paths. The purpose of dynamic routing protocols includes:

- Discovery of remote networks
- Maintaining up-to-date routing information
- Choosing the best path to destination networks
- Ability to find a new best path if the current path is no longer available

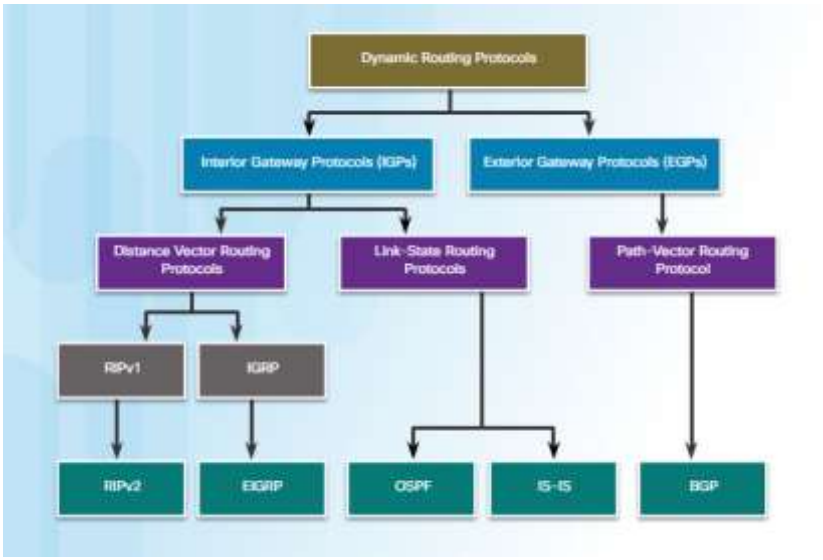


**Figure 5.3: Classification of Routing Protocols**

Routing protocols can be classified into different groups according to their characteristics. Specifically, routing protocols can be classified by their:

- **Purpose** - Interior Gateway Protocol (IGP) or Exterior Gateway Protocol (EGP)
- **Operation** - Distance vector protocol, link-state protocol, or path-vector protocol
- **Behaviour** - Classful (legacy) or classless protocol

For example, IPv4 routing protocols are classified as follows:

- **RIPv1 (legacy)** - IGP, distance vector, classful protocol
- **IGRP (legacy)** - IGP, distance vector, classful protocol developed by Cisco (deprecated from 12.2 IOS and later)
- **RIPv2** - IGP, distance vector, classless protocol
- **EIGRP** - IGP, distance vector, classless protocol developed by Cisco
- **OSPF** - IGP, link-state, classless protocol
- **IS-IS** - IGP, link-state, classless protocol
- **BGP** - EGP, path-vector, classless protocol

The classful routing protocols, RIPv1 and IGRP, are legacy protocols and are only used in older networks. These routing protocols have evolved into the classless routing protocols, RIPv2 and EIGRP, respectively. Link-state routing protocols are classless by nature.

## 5.3.2 IGP and EGP Routing Protocols

An autonomous system (AS) is a collection of routers under a common administration such as a company or an organization. An AS is also known as a routing domain. Typical examples of an AS are a company's internal network and an ISP's network.

The Internet is based on the AS concept; therefore, two types of routing protocols are required:

- **Interior Gateway Protocols (IGP)** - Used for routing within an AS. It is also referred to as intra-AS routing. Companies, organizations, and even service providers use an IGP on their internal networks. IGPs include RIP, EIGRP, OSPF, and IS-IS.

- **Exterior Gateway Protocols (EGP)** - Used for routing between ASes. It is also referred to as inter-AS routing. Service providers and large companies may interconnect using an EGP. The Border Gateway Protocol (BGP) is the only currently-viable EGP and is the official routing protocol used on the Internet.

The example in the figure provides simple scenarios highlighting the deployment of IGPs, BGP, and static routing:

- **ISP-1** - This is an AS and it uses IS-IS as the IGP. It interconnects with other autonomous systems and service providers using BGP to explicitly control how traffic is routed.

- **ISP-2** - This is an AS and it uses OSPF as the IGP. It interconnects with other autonomous systems and service providers using BGP to explicitly control how traffic is routed.

- **AS-1** - This is a large organization and it uses EIGRP as the IGP. Because it is multihomed (i.e., connects to two different service providers), it uses BGP to explicitly control how traffic enters and leaves the AS.

- **AS-2** - This is a medium-sized organization and it uses OSPF as the IGP. It is also multi homed; therefore, it uses BGP to explicitly control how traffic enters and leaves the AS.

- **AS-3** - This is a small organization with older routers within the AS; it uses RIP as the IGP. BGP is not required because it is single-homed (i.e., connects to one service provider). Instead, static routing is implemented between the AS and the service provider.

## 5.4 OSPF [Open Shortest Path First]

Open Shortest Path First (OSPF) is a link-state routing protocol that was developed as an alternative for the distance vector routing protocol, RIP. RIP was an acceptable routing protocol in the early days of networking and the Internet. However, RIP's reliance on hop count as the only metric for determining best route quickly became problematic. Using hop count does not scale well in larger networks with multiple paths of varying speeds. OSPF has significant advantages over RIP in that it offers faster convergence and scales to much larger network implementations.

OSPF is a classless routing protocol that uses the concept of areas for scalability. This chapter covers basic, single-area OSPF implementations and configurations.

# Chapter 6

## Screenshots

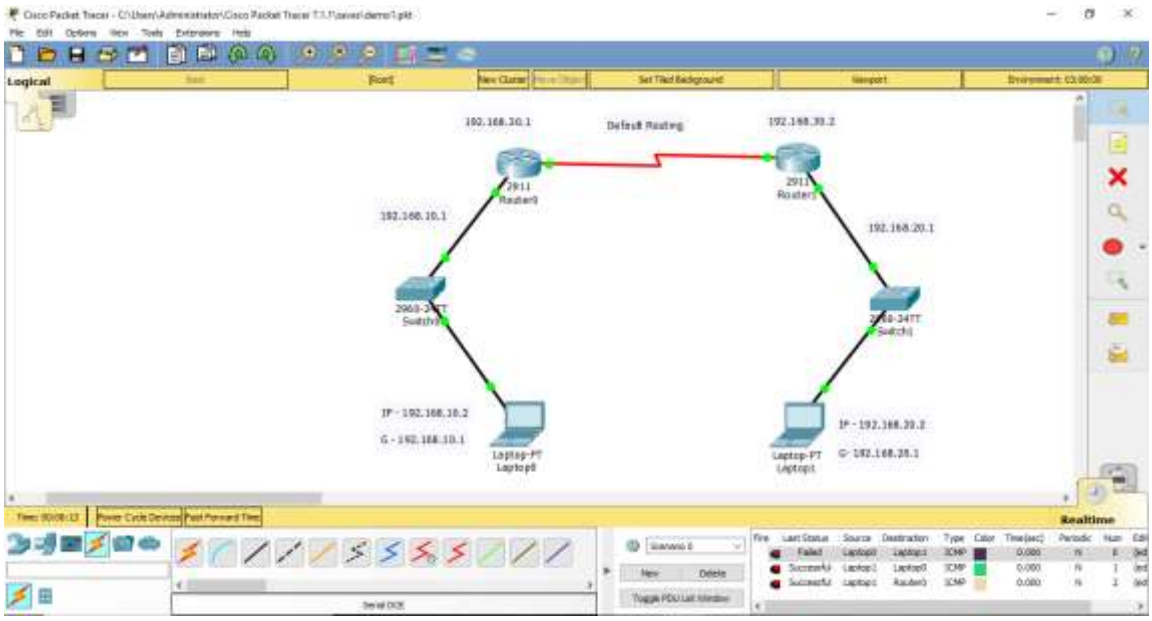


**Figure 6.1: Default Routing**

Default route which is also known as the gateway of last resort, is used in forwarding packets whose destination address does not match any route in the routing table.

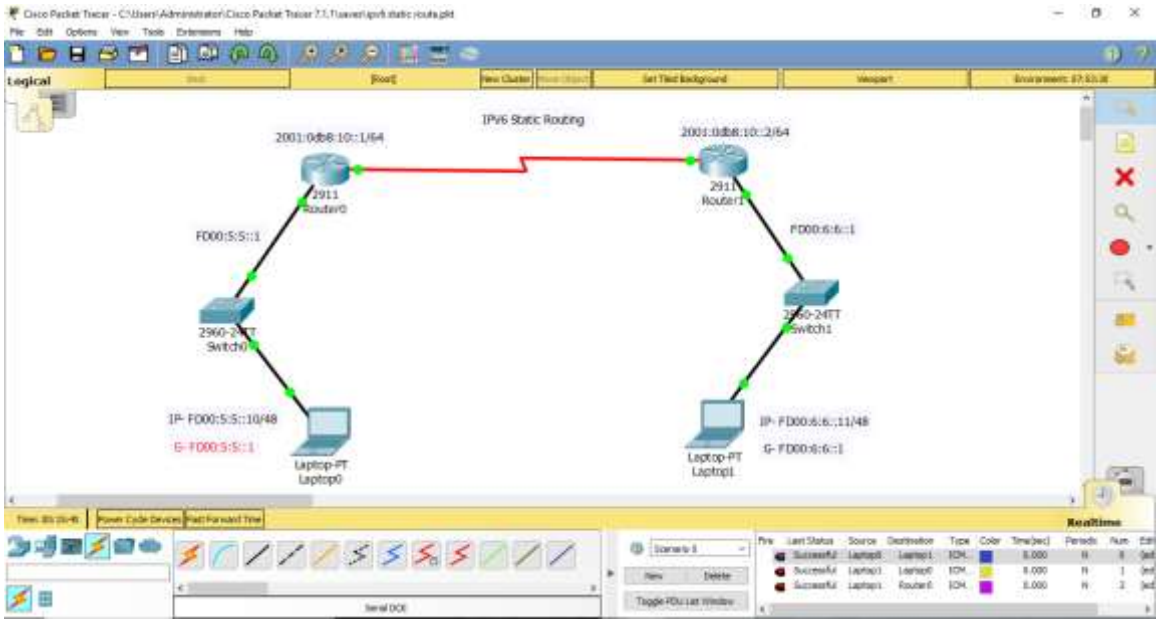


**Figure 6.2: IPV6 Static Routing**

IPv6 Static Routing feature provides static routing for IPv6. Static routes are manually configured and define an explicit path between two networking devices.

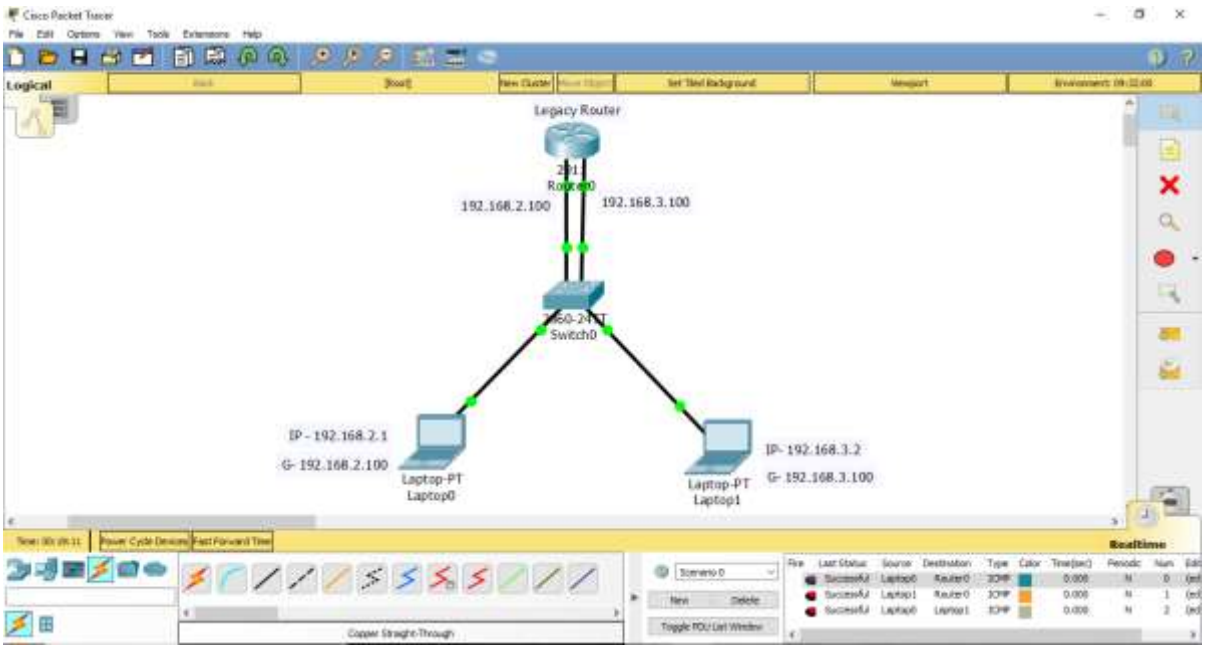


**Figure 6.3: Legacy Router**

In legacy approach, inter-VLAN routing is performed by connecting different physical router interfaces to different physical switch ports. The switch ports connected to the router are placed in access mode and each physical interface is assigned to a different VLAN.

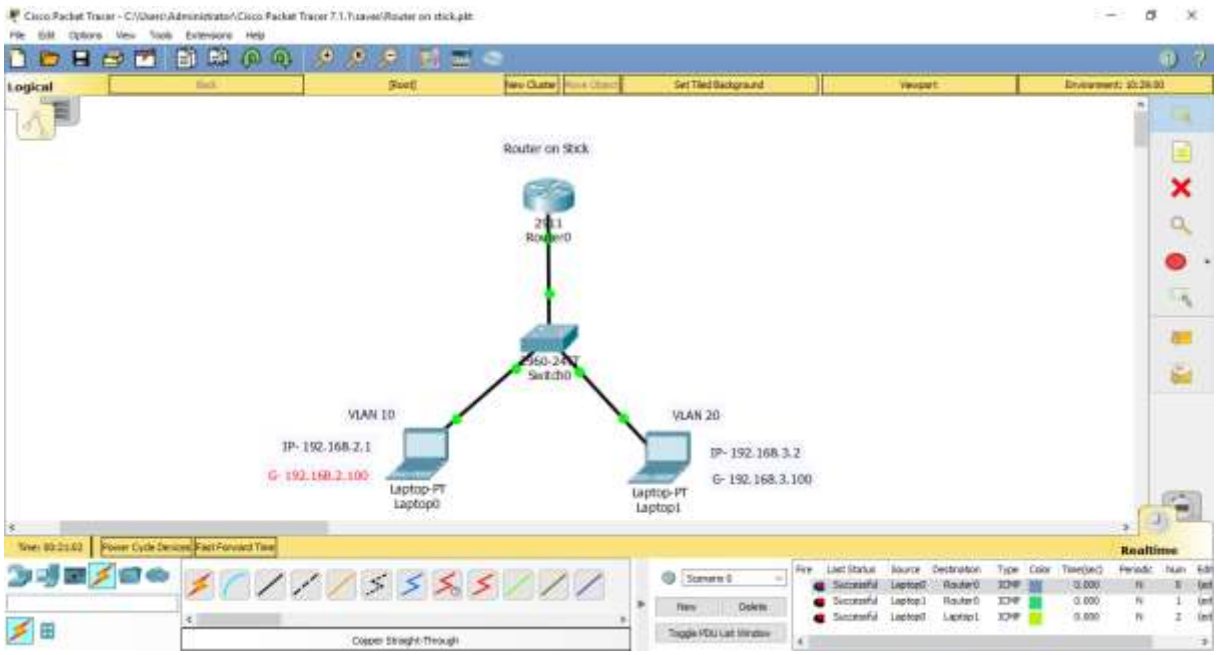


**Figure 6.4: Router on stick**

Router-on-a-stick is a term frequently used to describe a setup up that consists of a router and switch connected using one Ethernet link configured as an 802.1q trunk link.

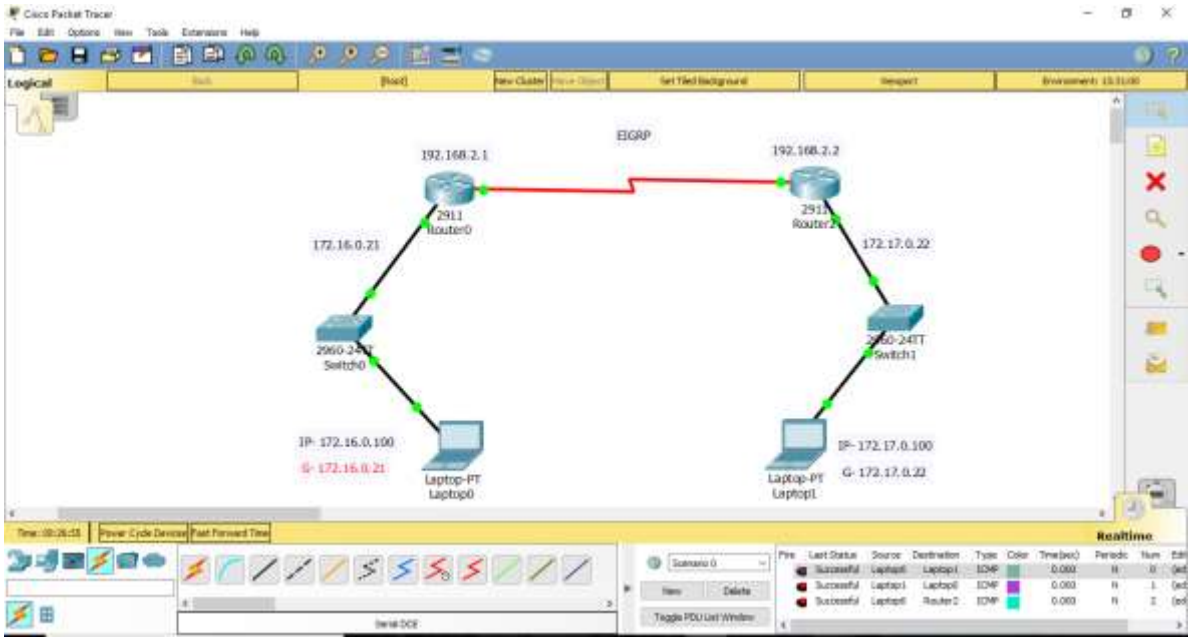


**Figure 6.5: EIGRP (Enhanced Interior Gateway Routing Protocol)**

Enhanced Interior Gateway Routing Protocol (EIGRP) is an advanced distance-vector routing protocol that is used on a computer network for automating routing decisions and configuration.

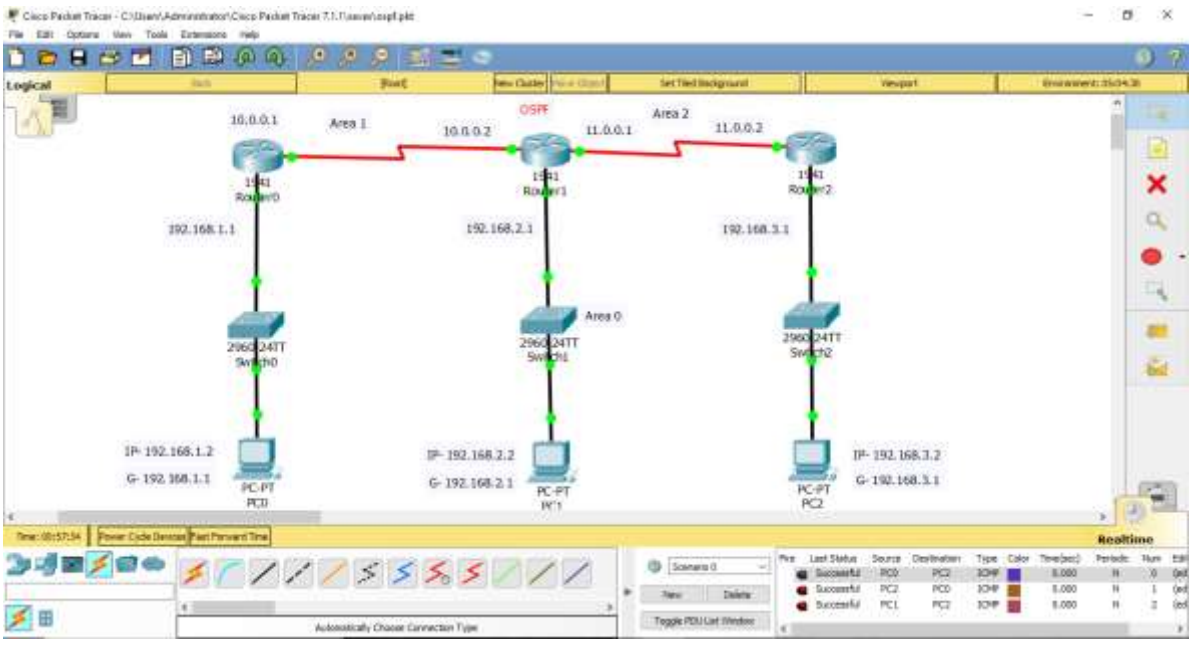


**Figure 6.6: OSPF (Open Shortest Path First)**

OSPF (Open Shortest Path First) is a preference to RIP (Routing Information Protocol) and they are used in autonomous system networks.

# Chapter 7

# Conclusion

In conclusion, it has been a reality fulfilling internship experience here at KGTTI not only gaining practical knowledge and real-life experience of branding and dealing with real clients, have also managed to develop relationships with my colleagues and honed my social skills. It also helps that my supervisor seldom directs me or oversees my work after the few days, learning to deal with other colleagues and clients by myself, and I am not protected or shielded from the reality of the working world. Sometimes, it also feels as if I am actually one of the staff here rather than an intern because of the level; of trust they have in me and the responsibilities they delegate to me.

The institute does not have the typical narrow-minded belief that an intern should always be "governed" and treated as a level beneath its staff, and be given mundane tasks to do to while away the time. Instead, KGTTI has given me much room to explore and discover the perks and difficulties of network servicing. I never excepted that it would be so satisfying and that It was so fortunate to meet such friendly and helpful colleagues and actually be extending my internship period for another month. However, now it feels as if the months have passed too quickly and this internship is too short as there is much more to learn and observe. It is with pleasure and gratitude that KGTTI has approved my internship extension.

I believe that the knowledge and experience gained through this time at KGTTI would come in handy and be able to put to good use upon my graduation, as it has opened up another possible carrier route for me.

# BIBLIOGRAPHY

## References:

**[1] Andrew S Tanenbaum**, Computer Networks, fifth edition, Pearson.

**[2] Behrouz A Forouzan**, Data Communications and Networking, Fifth Edition, McGraw Hill, Indian Edition.

**[3] James F Kurose and Keith W Ross**, Computer Networking, A Top - Down Approach, Sixth edition, Pearson, 2017.

**[4] Larry L Peterson and Brusce S Davie**, Computer Networks, fifth edition, ELSEVIER.

**[5] Mayank Dave**, Computer Networks, Second edition, Cengage Learning.

## Websites Referred:

**[1]** https://www.netacad.com.

**[2]** https://www.kgtti.com

**[3]** https://www.cisco.com

[**4**] https://www.ccnanetworking.com