JULY-AUG 2024

45 DAYS

COMPUTER NETWORKING

INDUSTRIAL TRAINING REPORT

Solitaire infosys

LUDHIANA COLLEGE OF ENGINEERING AND TECHNOLOGY

PREPARED BY: ABEL TELLO SENDOLO
UNI. ROLL NO.: 2205259
SUBMITTED TO: SOLITAIRE INFOSYS

ACKNOWLEDGEMENT

As I present this report, I would like to express my heartfelt appreciation to the entire Solitaire team, who played an essential role in my training by offering continuous guidance, motivation, and creating an excellent learning environment during my time at Solitaire Infosys Pvt. LTD. The training was incredibly valuable, providing not only technical knowledge but also practical skills. I am especially grateful to Mr. Sham Sunder, who dedicated a significant amount of time to supervise and advise me during my training. I am thankful for his invaluable guidance, which made this enriching and productive experience possible and opened up new opportunities for me.

ABSTRACT

The networking course aims to provide participants with a strong grasp of networking principles, protocols, and technologies. Throughout the course, participants will be familiarized with important concepts like network architecture and design. By combining theoretical learning with practical exercises, participants will develop the skills necessary to effectively set up, manage, and upkeep computer networks.

The course starts with an overview of networking basics, including a look at network models such as OSI and TCP/IP. Participants will become acquainted with different network topologies, protocols, cabling, and the roles of network devices. As the course advances, participants will delve into the complexities of routing protocols like RIP, OSPF, and EIGRP.

Network security is a critical focus of the course, encompassing topics such as virtual private networks (VPNs), DNS servers, email servers, NAT, and VOIP. Additionally, participants will gain insights into network design approaches, IP addressing, redistribution, and subnetting.

Upon completing the course, participants will have a thorough comprehension of networking fundamentals and will have acquired hands-on skills to design and configure computer networks. This knowledge and expertise will equip them to pursue careers in network administration, engineering, or security, contributing to the efficient and secure operation of modern digital infrastructures.

TABLE OF CONTENTS

Chapter

1

Computer Network Types, Topologies, Cabling & OSI Model

TOPICS COVERED IN THIS CHAPTER:

- ✓ Introduction of Networking & Networks
- ✓ Network Types
- ✓ Network Topologies
- ✓ Networking Components
- ✓ OSI Model & Cabling

It is important to have an understanding of basic personal computer networking concepts before you begin exploring the world of over-the-air (wireless) networking technology,
wireless terminology, and mobility. This chapter looks at various topics surrounding foundational computer networking, including computer network types, computer topologies, the OSI model, and network device addressing. It is intended to provide an overview of basic computer networking concepts as an introduction for those who need to gain a basic understanding or for those already familiar with this technology and want a review of these concepts.
You will look at the various types of wireless networks—including wireless personal area networks (WPANs), wireless local area networks (WLANs), wireless metropolitan area networks (WMANs), and wireless wide area networks (WWANs)—in Chapter 4, “Standards and Certifi cations for Wireless Technologies.”

INTRODUCTION

Computer networking is a cornerstone of modern technology, enabling the interconnected systems that power the Internet, business communications, and everyday digital interactions. Understanding the fundamentals of computer networking is essential for anyone involved in technology, from enthusiasts to professionals. This article will explore the basics of computer networking, including network types, components, protocols, and essential services like the Domain Name System (DNS).

What is Networking?

Networking, or computer networking, is the process of connecting two or more computing devices, such as desktop computers, mobile devices, routers, or applications, to enable the transmission and exchange of information and resources

What is a Network?

A network is a collection of interconnected devices that can communicate with each other to share resources and information. These devices can include computers, servers, smartphones, printers, and other hardware.

Network Types

Personal computer networking technology has evolved at a tremendous pace over the past couple of decades, and many people across the world now have some type of exposure to the technology. Initially, personal computers were connected, or networked, to share fi les and printers and to provide central access to the users’ data. This type of network was usually confi ned to a few rooms or within a single building and required some type of cabled physical

infrastructure. As the need for this technology continued to grow, so did the types of networks. Computer networking started with the local area network (LAN) and grew on to bigger and better types, including wide area networks (WANs), metropolitan area networks (MANs), and others. The following are some of the common networking types in use today:

- Local area networks (LANs)
- Wide area networks (WANs)
- Metropolitan area networks (MANs)
- Campus area networks (CANs)
- Personal area networks (PANs)

You may also come across the term *storage area network (SAN)*. The SAN is basically a separate subnet for offloading of large amounts of data used within an enterprise network. High-speed connections are used, so the data is easily accessible because it appears to be part of the network. The connections are commonly Fibre Channel or iSCSI utilizing the TCP/IP protocol.

Most computer networks now contain some type of wireless connectivity or may consist of mostly wireless connectivity. The need for wireless networking and mobility continues to be in great demand and is growing at a rapid pace.

The Local Area Network

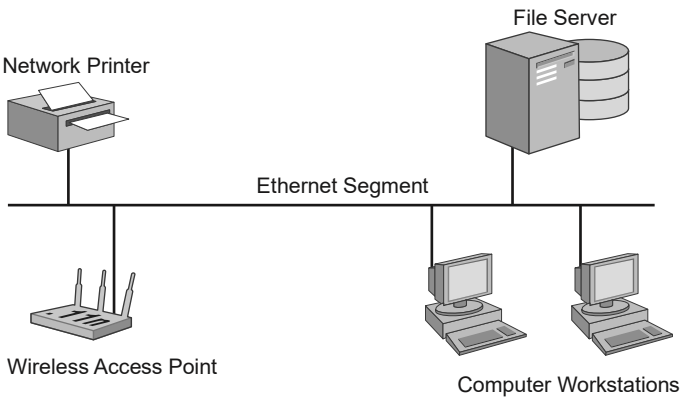
A local area network (LAN) can be defi ned as a group of devices connected in a specifi c arrangement called a topology. The topology used depends on where the network is installed. Some common legacy topologies such as the bus and ring and more modern topologies such as the star and mesh are discussed later in this chapter. Local area networks are contained in the same physical area and usually are bounded by the perimeter of a room or building. However, in some cases a LAN may span a group of buildings in close proximity that share a common physical connection.

Early LANs were mostly used for fi le and print services. This allowed users to store data securely and provided a centralized location of data for accessibility even when the user was physically away from the LAN. This central storage of data also gave a network administrator the ability to back up and archive all the saved data for disaster recovery purposes. As for print services, it was not cost effective to have a physical printer at every desk or for every user, so LANs allowed the use of shared printers for any user connected to the local area network. Figure 1.1 illustrates a local area network that includes both wired and wireless networking devices.

The Wide Area Network

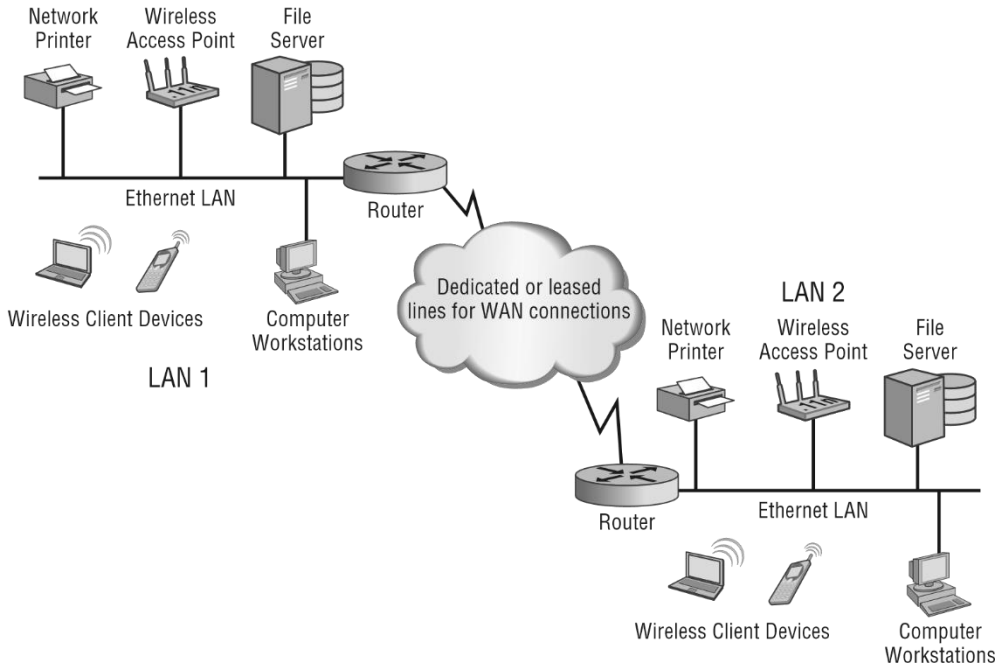
As computer networking continued to evolve, many businesses and organizations that used this type of technology needed to expand the LAN beyond the physical limits of a single room or building. These networks covered a larger geographical area and became known as *wide area networks (WANs)*. As illustrated in Figure 1.2, WAN connectivity mostly consists of point-to-point or point-to-multipoint connections between two or more LANs. The LANs may span a relatively large geographical area. (Point-to-point and point-tomultipoint connections are discussed later in this
chapter.) The WAN has allowed users and organizations to share data fi les and other resources with a much larger audience than a single LAN would.

FIGURE 1.1 Example of a local area network (LAN)



WANs can use leased lines from telecommunication providers (commonly known as *telcos*), fi ber connections, and even wireless connections. The use of wireless for bridging local area networks is growing at a fast pace because it can often be a cost-effective solution for connecting LANs

FIGURE 1.2 Wide area network (WAN) connecting two LANs



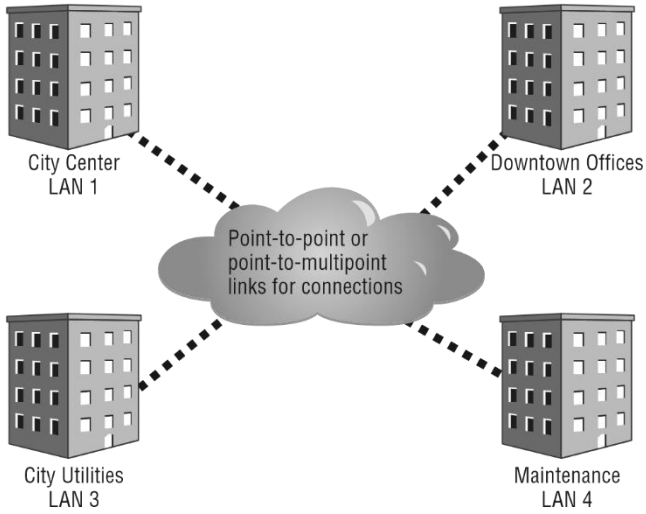
The Metropolitan Area Network

The metropolitan area network (MAN) interconnects devices for access to computer resources in a region or area larger than that covered by local area networks (LANs) but yet smaller than the areas covered by wide area networks (WANs). A MAN consists of networks that are geographically separated and can span from several blocks of buildings to entire cities (see Figure 1.3). MANs include fast connectivity between local networks and may include fi ber optics or other wired connectivity that is capable of longer distances and higher capacity than those in a LAN.

MANs allow for connections to outside larger networks such as the Internet. They may include cable television, streaming video, and telephone services. Devices and connectivity used with metropolitan area networks may be owned by a town, county, or other locality and may also include the property of individual companies. Wireless MANs are also becoming a common way to connect the same type of areas but without the physical cabling limitations.

The MAN is growing in popularity as the need for access in this type of environment also increases.

FIGURE 1.3 Example of a metropolitan area network connecting a small town



The Campus Area Network

A *campus area network (CAN)* includes a set of interconnected LANs that basically form a smaller version of a wide area network (WAN) within a limited geographical area, usually an offi ce or school campus. Each building within the campus generally has a separate LAN. The LANs are often connected using fi ber-optic cable, which provides a greater distance than copper wiring using IEEE 802.3 Ethernet technology. However, using wireless connections between the buildings in a CAN is an increasingly common way to connect the individual LANs. These wireless connections or wireless bridges provide a quick, costeffective way to connect buildings in a university campus, as shown in Figure 1.4.

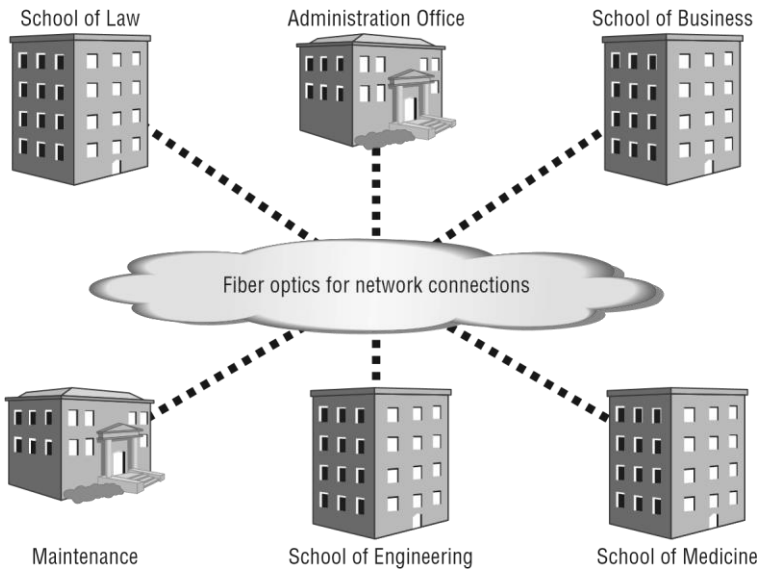
In a university campus environment, a CAN may link many buildings, including all of the various schools—School of Business, School of Law, School of Engineering, and so on—as well as the university library, administration buildings, and even residence halls. Wireless LAN deployments are becoming commonplace in university residence halls. With the rapidly increasing number of wireless mobile devices on university campuses, the number of wireless access points and the capacity of each need to be considered.

As in the university campus environment, a corporate offi ce CAN may connect all the various building LANs that are part of the organization. This type of network will have the characteristics of a WAN but be confi ned to the internal resources of the corporation or organization. Many organizations are deploying wireless networks within the corporate CAN as a way to connect various parts of the business together. As with the university CAN, in the

corporate world wireless can be a quick, cost-effective way to provide connectivity between buildings and departments.

All of the physical connection mediums and devices are the property of the offi ce or school campus, and responsibility for the maintenance of the equipment lies with the offi ce or campus as well.

FIGURE 1.4 Campus area network connecting a school campus

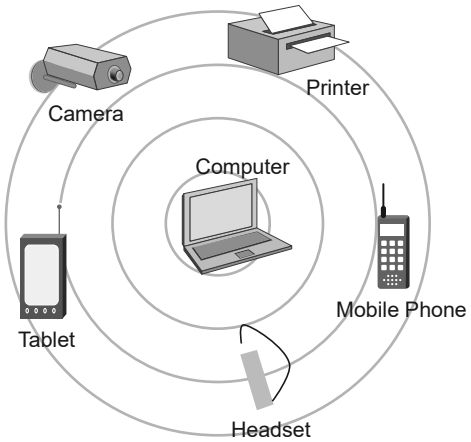


The Personal Area Network

Personal area networks (PANs) are networks that connect devices within the immediate area of individual people. PANs may consist of wired connections, wireless connections, or

both. On the wired side, this includes universal serial bus (USB) devices such as printers, keyboards, and computer mice that may be connected with a USB hub. With wireless technology, PANs are short-range computer networks and in many cases use Bluetooth wireless technology. Wireless Bluetooth technology is specifi ed by the IEEE 802.15 standard and is not IEEE 802.11 wireless local area technology. Bluetooth will be discussed in more detail in Chapter 4. Like wired PANs, wireless PANs are commonly used in connecting an individual's wireless personal communication accessories such as phones, headsets, computer mice, keyboards, tablets, and printers and are centered on the individual personal workspace without the need for physical cabling. Figure 1.5 illustrates a typical wireless PAN confi guration.

FIGURE 1.5 Wireless Bluetooth network connecting several personal wireless devices



Network Topologies

A computer physical network topology is the actual layout or physical design and interconnection of a computer network. A topology includes the cabling and devices that are part of the network. In the following sections you will learn about several different types of network topologies:

- Bus
- Ring
- Star
- Mesh
- Ad-hoc
- Point-to-point
- Point-to-multipoint

The bus, ring, star, mesh, and ad-hoc topologies are typically what make up the local area network (LAN) you learned about previously. Point-to-point and point-to-multipoint

topologies can be commonly used for connecting LANs and are mostly used for wide area network (WAN) connections. The size of your network will determine which topologies will apply. If your network is a single building and not part of a larger corporate network, the LAN topologies may be the extent of the technologies used. However, once that LAN connects to a different LAN, you are moving up and scaling to a wide area network.

The Bus Topology

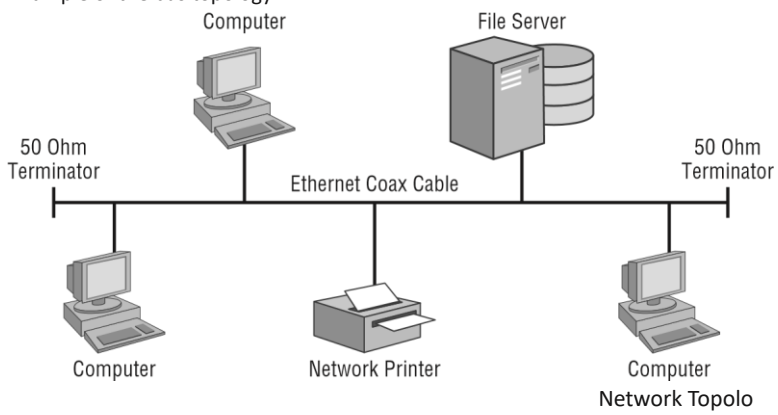
A *bus* topology consists of multiple devices connected along a single shared medium with two defi ned endpoints. It is sometimes referred to as a high-speed linear bus and is a single collision domain in which all devices on the bus network receive all messages. Both endpoints of a bus topology have a 50 ohm termination device, usually a Bayonet NeillConcelman (BNC) connector with a 50 ohm termination resistor. The bus topology was commonly used with early LANs but is now considered a legacy design.

One disadvantage to the bus topology is that if any point along the cable is damaged or broken, the entire LAN will cease to function. This is because the two endpoints communicate only across the single shared medium. There is no alternative route for them to use in the event of a problem.

Troubleshooting a bus network is performed by something known as the half-split method. A network engineer "breaks" or separates the link at about the halfway point and measures the resistance on both ends. If the segment measures 50 ohms of resistance, there is a good chance that side of the LAN segment is functioning correctly. If the resistance measurement is not 50 ohms, it signals a problem with that part of the LAN segment. The engineer continues with this method until the exact location of the problem is identifi ed.

Figure 1.6 illustrates an example of the bus topology.

FIGURE 1.6 Example of the bus topology



Network Topolo

Real World Scenario

Troubleshooting the Bus Topology

Many years ago I was called to troubleshoot a problem on a small local area network using a bus topology. The network consisted of a network fi le server, about 20 client stations, and a few network printers. The users complained of intermittent connection problems with the network. After spending some time looking over the network, I decided to test the bus using the half-split method and checked to verify that the cable was reporting the correct resistance using a volt-ohm-milliamp (VoM) meter. Sure enough, one side of the network cable reported the correct resistance reading, but the other side was giving intermittent results.

After spending some time repeating the troubleshooting method, I was able to determine the problem. It turns out that someone had run the coax (bus) cable underneath a heavy plastic offi ce chair mat and one of the little pegs used to protect the fl ooring was causing the intermittent connection as it struck the cable when the user moved their chair around the mat. I quickly replaced and rerouted the section of cable in question. It is a good thing I was there during the normal business operating hours when the person was moving around in the chair or I might have never found the problem. Ah, the joys of troubleshooting a bus topology.

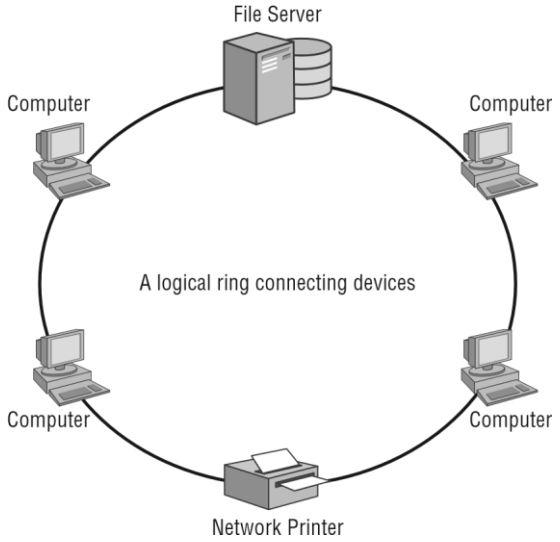
The Ring Topology

The ring topology is rarely used with LANs today, but it is still widely used by Internet service providers (ISPs) for high-speed, resilient backhaul connections over fi ber-optic links. In the ring topology, each device connects to two other devices, forming a logical ring pattern.

Ring topologies in LANs may use a token-passing access method, in which data travels around the ring in one direction. Only one device at a time will have the opportunity to transmit data. Because this access method travels in one direction, it does not need to use collision detection and often outperforms the bus topology, achieving higher data transfer rates than are possible using a collision detection access method. Each computer on the ring topology can act as a repeater, a capacity that allows for a much stronger signal.

The IEEE standard for LANs is IEEE 802.5, specifying Token Ring technology. IEEE 802.5 Token Ring technology used in LANs was a very effi cient method used to connect devices, but it was usually more expensive than the bus or star topologies. Because of the token-passing method used, early 4 Mbps Token Ring networks could sometimes outperform a 10 Mbps IEEE 802.3 collision-based Ethernet network. Token Ring technology speeds increased to 16 Mbps but decreased in popularity as Ethernet speeds increased. Even though this is a ring topology, devices are connected through a central device and appear to be similar to devices on an Ethernet hub or switch. Figure 1.7 shows an example of the ring topology.

FIGURE 1.7 An example of the ring topology



The Star Topology

The star topology, as shown in Figure 1.8, is the most commonly used method of connecting devices on a LAN today. It consists of multiple devices connected by a central connection device. Hubs, switches, and wireless access points are all common central connection devices, although hubs are rarely used today. The hub provides a single collision domain similar to a bus topology. However, the Ethernet switch and wireless access point both have more intelligence—the ability to decide which port specifi c network traffi c can be sent to. Note that in Figure 1.8, the wireless star topology includes an Ethernet switch, which could also have extended devices connected to it with wires. In that sense, it is possible to have a wired/wireless hybrid topology.

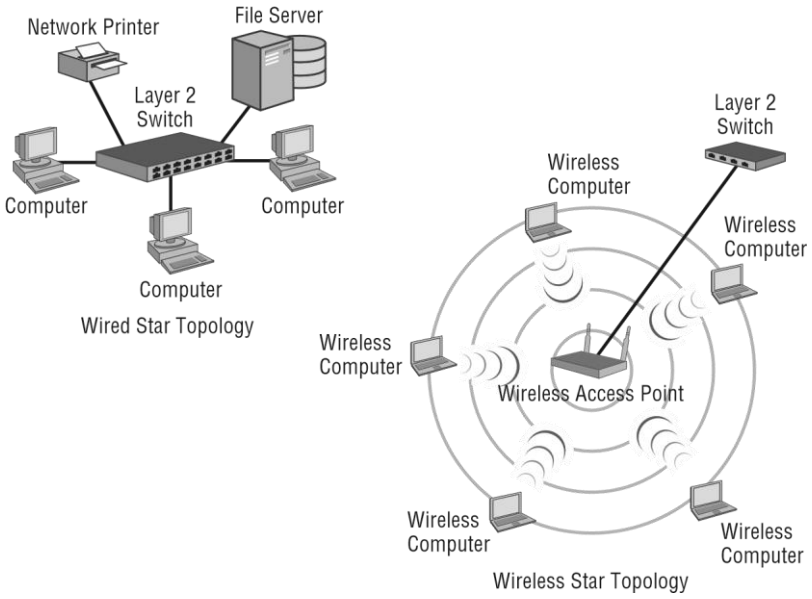
A big advantage to the star over the bus and some ring topologies is that if a connection is broken or damaged, the entire network does not cease to function; only a single device in the star topology is affected. However, the central connection device such as a switch or wireless access point can be considered a potential central point of failure.

The Mesh Topology

A device in a mesh network will process its own data as well as serving as a communication point for other mesh devices. Each device in a *mesh* topology (see Figure 1.9) has one or more connections to other devices that are part of the mesh. This approach provides both network resilience in case of link or device failure and a cost savings compared to full redundancy. Mesh technology can operate with both wired and wireless infrastructure network

devices. Wireless mesh networks are growing in popularity because of the potential uses in outdoor deployments and the cost savings they provide.

FIGURE 1.8 A common star topology using either wired or wireless devices



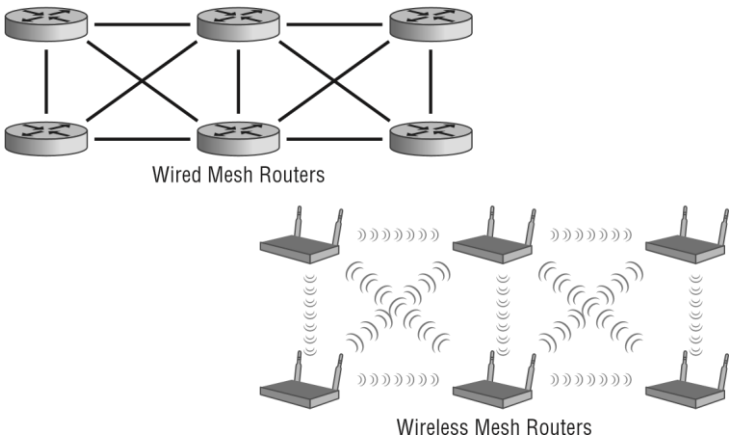
From an IEEE 802.11 wireless perspective, wireless mesh technology has now been standardized, although most manufacturers continue to use their proprietary methods. The amendment to the IEEE 802.11 standard for mesh networking is 802.11s. This amendment was ratifi ed in 2011 and is now part of the latest wireless LAN standard, IEEE 802.112012. In addition to IEEE 802.11 networks, mesh is also standardized in IEEE 802.15 personal area networks for use with Zigbee and IEEE 802.16 Wireless MAN networks.
Wireless standards will be discussed in more detail in Chapter 4.

As mentioned earlier, IEEE 802.11 wireless device manufacturers currently continue to use proprietary Layer 2 routing protocols, forming a self-healing wireless infrastructure (mesh) in which edge devices can communicate. Manufacturers of enterprise wireless networking infrastructure devices provide support for mesh access points (APs) such that the mesh APs connect back to APs that are directly wired into the network backbone infrastructure. The APs, wireless LAN controllers or software-based cloud solutions in this case, are used to confi gure both the wired and mesh APs.

Ad Hoc Connections

In the terms of computer networking, the *ad hoc* network is a collection of devices connected without a design or a plan for the purpose of sharing information or resources.
Another term for an ad hoc network is *peer-to-peer network*.

FIGURE 1.9 Mesh networks can include either wired or wireless devices.

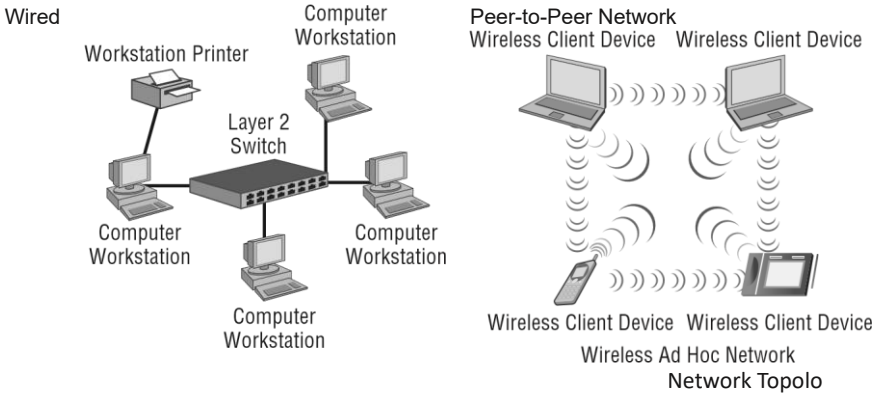


In a wired peer-to-peer network, all computing devices are of equal status. In other words, there is no server that manages the access to network resources. All peers can either share their own resources or access the resources of their devices on the network.

An ad hoc wireless network is one that does not contain a distribution system, which means no wireless access point is contained in the system to provide centralized communications.

Figure 1.10 shows an example of a wired peer-to-peer network and a wireless ad hoc network.

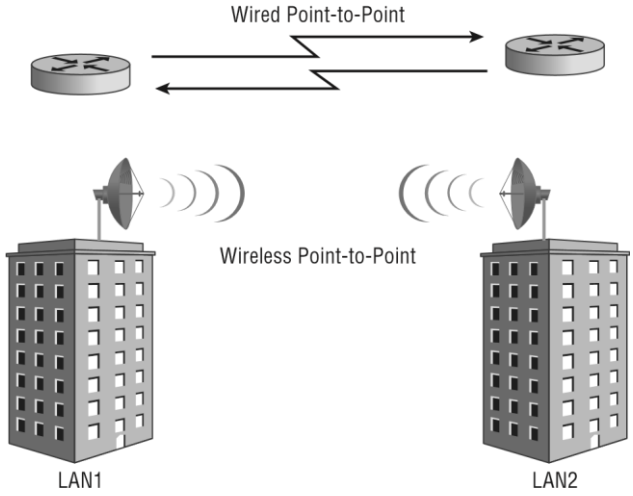
FIGURE 1.10 Wired peer-to-peer and wireless ad hoc networks



Point-to-Point Connections

When at least two LANs are connected, it is known as a *point-to-point connection* or link (see Figure 1.11). The connection can be made using either wired or wireless network infrastructure devices and can include bridges, wireless access points, and routers. Wireless point-to-point links can sometimes extend very long distances depending on terrain and other local conditions. Point-to-point links provide a connection between LANs, allowing users from one LAN to access resources on the other connected local area network.

FIGURE 1.11 Point-to-point connections using either wired or wireless



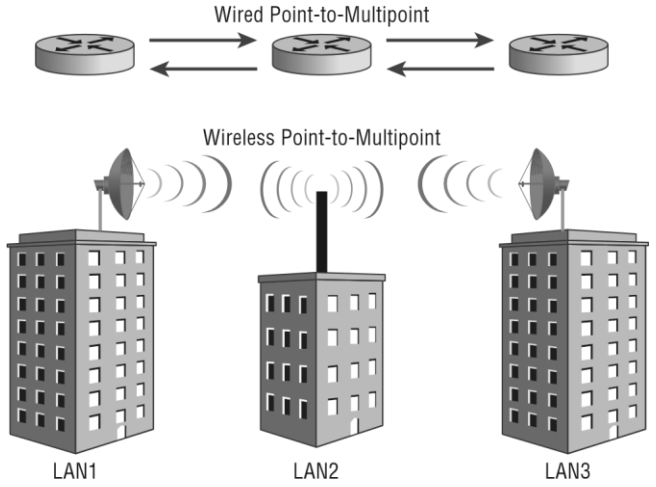
Wired point-to-point links consist of fi ber-optic connections or leased lines from local telecommunication providers. Wireless point-to-point links typically call for semidirectional or highly directional antennas. Wireless point-to-point links include directional antennas and encryption to protect the wireless data as it propagates through the

air from one network to the other. With some regulatory domains such as the Federal Communications Commission (FCC), when an omnidirectional antenna is used in this confi guration it is considered a special case, called a point-to-multipoint link.

Point-to-Multipoint Connections

A network infrastructure connecting more than two LANs is known as a point-to-multipoint connection or link (see Figure 1.12). When used with wireless, this confi guration usually consists of one omnidirectional antenna and multiple semidirectional or highly directional antennas. Point-to-multipoint links are often used in campus-style deployments, where connections to multiple buildings or locations may be required. Like point-to-point connections; wired point-to-multipoint connections can use either direct wired connections such as fi ber-optic cables or leased line connectivity available from telecommunication providers.

FIGURE 1.12 Point-to-multipoint connections using either wired or wireless connections



NETWORKING COMPONENTS

Networking components are the hardware devices that facilitate communication and data exchange within a network. Here are some key components:

1. MODEM

The modem is short for modulator-demodulator, and this is the device that connects you to the Internet. There are many types of modems in the market:

- **Dial-up modem**: Once up a time in the stone age of the Internet, we have to attach a phone line to this gadget and dial up to the Internet service provider (ISP) to access the Internet. Whenever someone else calls it, this connection will break and we get to curse at the caller… Good old days indeed.

- **Cable modem**: Smart monkeys soon realized that using the phone lines is not a great idea after all, and they moved to use the TV cables instead. It is a huge life savior without the Internet connection getting interrupted by calls, but technical limitations soon gave rise to the next generation of modems.
- **Optical Network Terminal (ONT)**: With a world hungry for a faster Internet, cable modems that use electrical signals soon hit a technical limit. This gave rise to a new generation of modems that uses optics (light) to transmit data instead – Which, light is one of the fastest medium that humans know of.
- **Wireless modem**: As you might already know, the Internet is no longer "bound" to landlines. Smartphones and tablets these days already have a

wireless modem built-in, but you can still buy a stand-alone wireless modem to share the Internet connection.

2. Router

A Router is a networking device that forwards data between computer networks. One or more packet-switched networks or subnetworks can be connected using a router. By sending data packets to their intended IP addresses, it manages traffic between different networks and permits several devices to share an Internet connection.

3. Switch

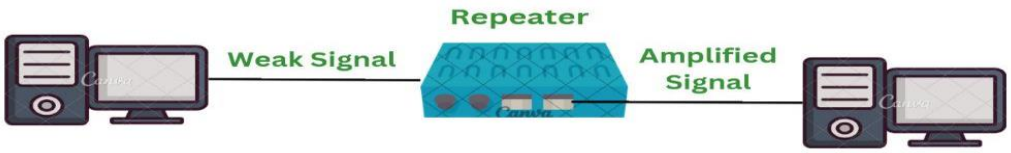
Network switches are “wired devices” that essentially serve the same function as a USB hub. You only have one port on your router but need more – This is where we use a network switch to “add” more ports to the router. For you guys who are wondering why switches are still necessary these days, there are many reasons.

4. Hub

The ancestor of network switches. We will not go into the details of how hubs and switches are different, as hubs are already extinct. Just know that hubs once exist, and if you search for "network hub" these days, you will get network switches instead; Hubs and switches are literally referring to the same thing these days.

5. Repeater

Repeaters are defined as a networking device that is used to amplify and generate the incoming signal. Repeaters work at the physical layer of the OSI model. The main aim of using a repeater is to increase the networking distance by increasing the strength and quality of signals. The performance of Local Area Networks (LANs) and Wide Area Networks (WANs) repeaters are used. Using repeaters helps to reduce error, and loss of data and provides with delivery of data at specified locations only. The major advantage of using a repeater is that it provides with transfer of data with more security and over a long distance.



6. Firewall

You have probably heard of a "firewall" from somewhere already – Windows Firewall and MacOS Firewall ring a bell? But not to be confused with the software firewall, this is an actual hardware firewall that protects your network by scanning all the incoming/outgoing traffic, and blocking all the shady deals.

7. Network Interface Card (NIC)

The NIC is the component that allows your device to connect to the network, comes in either wired or wireless. But these are pretty uncommon as "standalone devices" these days, as they are already integrated into devices – Smartphones, tablets, and laptops mostly already have a built-in wireless NIC.

OSI MODEL

Before we continue with other mobility topics, you should have some background on computer networking theory. The basics of a computer networking discussion start with the Open Systems Interconnection (OSI) model, a conceptual seven-layer model. The OSI model has been around for decades. It came about in 1984 and was developed by the International Organization for Standardization (ISO). The ISO is a worldwide organization that creates standards on an international scale. The OSI model describes the basic concept of communications in the computer network environment. Be careful not to confuse the two.

There are seven layers to the OSI model. Each layer is made up of many protocols and serves a specifi c function. You will take a quick look at all seven layers of the OSI model. Some wireless-specifi c functionality of the OSI model will be discussed later in Chapter 5, "IEEE 802.11 Terminology and Technology." Figure 1.13 illustrates the seven layers of the conceptual OSI model.

The following sections describe how each layer is used.

Layer 1 – The Physical Layer

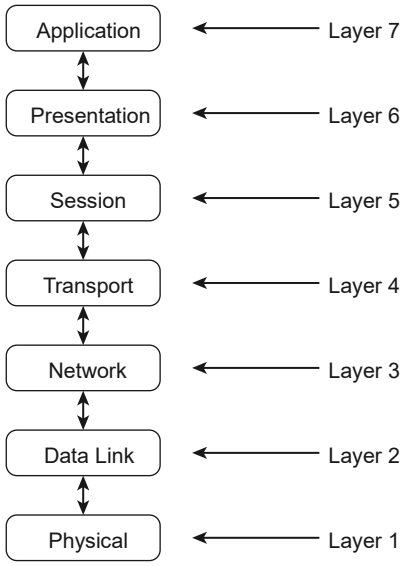
The Physical layer (sometimes referred as the PHY) is the lowest layer in the OSI model. The PHY consists of bit-level data streams and computer network hardware connecting the devices together. This hardware that connects devices includes network interface cards,

cables, Ethernet switches, wireless access points, and bridges. Keep in mind some of these hardware devices, such as Ethernet switches and bridges, actually have Data Link layer (Layer 2) functionally and operate at that layer but also make up the actual physical connections. In the case of wireless networking, radio frequency (RF) uses air as the medium for wireless communications. With respect to wireless networking, the Physical layer consists of two sublayers:

- Physical Layer Convergence Protocol (PLCP)
- Physical Medium Dependent (PMD)

The PLCP, the higher of the two layers, is the interface between the PMD and Media Access Control (MAC) sublayer of the Data Link layer. This is where the Physical layer header is added to the data. The PMD is the lower sublayer at the bottom of the protocol stack and is responsible for transmitting the data onto the wireless medium. Figure 1.14 shows the two sublayers that make up the Physical layer.

FIGURE 1.13 Representation of the OSI Model

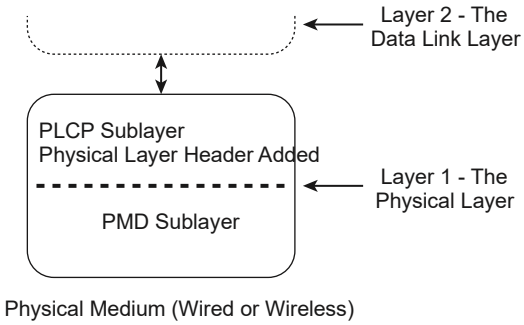


Layer 2 – The Data Link Layer

The Data Link layer is responsible for organizing the bit-level data for communication between devices on a network and detecting and correcting Physical layer errors. This layer consists of two sublayers

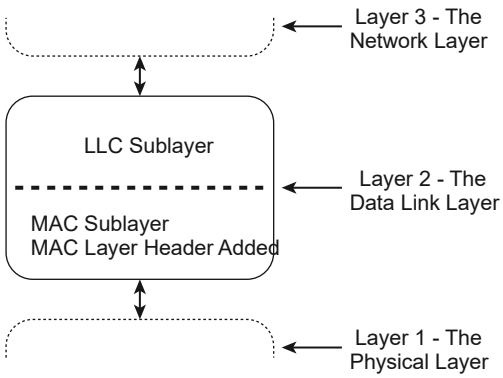
- Logical Link Control (LLC)
- Media Access Control (MAC)

FIGURE 1.14 Physical layer sublayers, PMD and PLCP



The bit-level communication is accomplished through Media Access Control (MAC) addressing. A MAC address is a unique identifi er of each device on the computer network and is known as the physical or sometimes referred to as the hardware address. (MAC addresses are discussed later in this chapter.) Figure 1.15 illustrates the two sublayers of the Data Link layer, Layer 2.

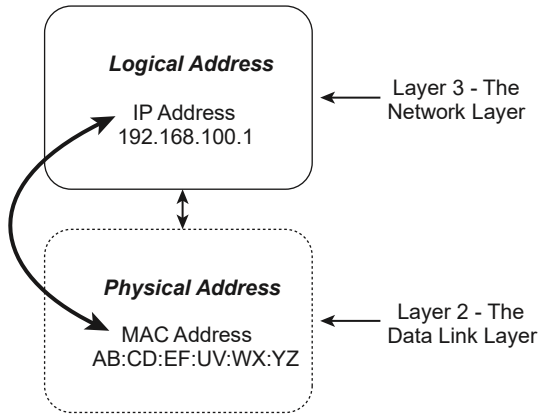
FIGURE 1.15 Data Link layer sublayers, LLC and MAC



Layer 3 – The Network Layer

The Network layer is where the Internet Protocol (IP) resides. The Network layer is responsible for addressing and routing data by determining the best route to take based on what it has learned or been assigned. An IP address is defi ned as a numerical identifi er or logical address assigned to a network device. The IP address can be static, manually assigned by a user, or it can be dynamically assigned from a server using Dynamic Host Confi guration Protocol (DHCP). (IP addresses are discussed later in this chapter.) Figure 1.16 illustrates the Layer 2 MAC address translation to a Layer 3 IP address.

FIGURE 1.16 Data Link layer (Layer 2) to Network layer (Layer 3) address translation



Layer 4 – The Transport Layer

The Transport layer consists of both connection-oriented and connectionless protocols providing communications between devices on a computer network. Although there are several protocols that operate at this layer, you should be familiar with two commonly used Layer 4 protocols:

- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)

TCP is a connection-oriented protocol and is used for communications that require reliability, analogous to a circuit-switched telephone call.

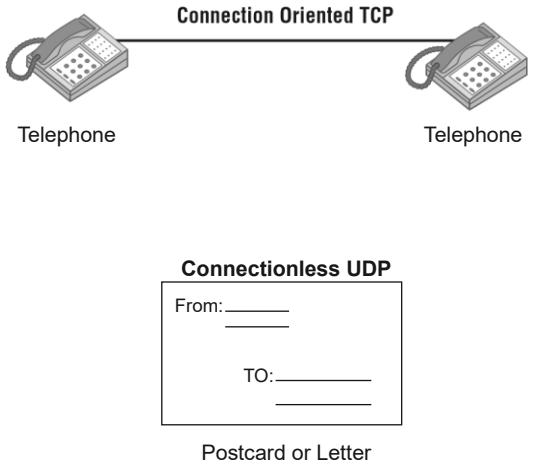
UDP is a connectionless protocol and is used for simple communications requiring effi ciency, analogous to sending a postcard through a mail service. You would not know if the postcard was received or not. UDP and TCP port numbers are assigned to applications for fl ow control and error recovery. Figure 1.17 represents the relationship between the Transport layer protocols TCP and UDP.

Layer 5 – The Session Layer

The Session layer opens, closes, and manages communications sessions between end-user application processes located on different network devices. The following protocols are examples of Session layer protocols:

- Network File System (NFS)
- Apple Filing Protocol (AFP)
- Remote Procedure Call Protocol (RPC)

FIGURE 1.17 Comparison between TCP and UDP protocols



Layer 6 – The Presentation Layer

The Presentation layer provides delivery and formatting of information for processing and display. This allows for information that is sent from one device on a network (the source) to be understood by another device (the destination) on the network.

Layer 7 – The Application Layer

The Application layer can be considered the interface to the user. Application is another term for a program that runs on a computer or other networking device and that is not what we are looking at here. Protocols at this layer are for network operations such as, for example, transferring fi les, browsing web pages, and sending email. The following list includes some of the more common examples of Application layer protocols we use daily:

- File Transfer Protocol (FTP) for transfering data
- Hypertext Transfer Protocol (HTTP) for web browsing
- Post Office Protocol v3 (POP3) for email

Common Application layer protocols will be discussed further in Chapter 2, “Common Network Protocols and Ports.”

How the Layers Work Together

In order for computers and other network devices to communicate with one another using the OSI model, a communication infrastructure of some type is necessary. In a wired network, such an infrastructure consists of cables, repeaters, bridges, and Layer 2 switches. In a

wireless network, the infrastructure consists of access points, bridges, repeaters, radio frequency, and the open air. Some of these devices will be discussed in more detail in Chapter 6, "Computer Network Infrastructure Devices."

Wireless networking functions at the two lowest layers of the OSI model, Layer 1 (Physical) and Layer 2 (Data Link). However, to some degree Layer 3 (Network) plays a role as well, generally for the TCP/IP protocol capabilities.

OSI Model Memorization Tip

One common method you can use to remember the seven layers of the OSI model from top to bottom is to memorize the following sentence: All people seem to need data processing. Take the first letter from each word and that will give you an easy way to remember the first letter that pertains to each layer of the OSI model.

- **A**ll (**A**pplication)
- **P**eople (**P**resentation)
- **S**eem (**S**ession)
- **T**o (**T**ransport)
- **N**eed (**N**etwork)
- **D**ata (**D**ata Link)
- **P**rocessing (**P**hysical)

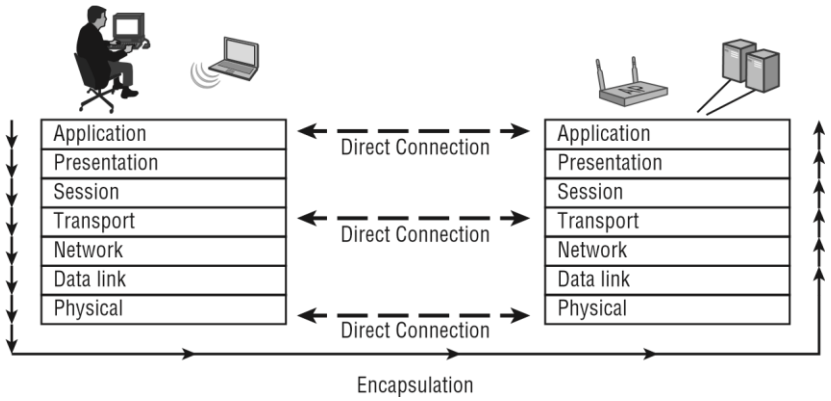
Here's another one, this time from the bottom to the top:

- **P**lease (**P**hysical)
- **D**o (**D**ata Link)
- **N**ot (**N**etwork)
- **T**hrow (**T**ransport)
- **S**ausage (**S**ession)
- **P**izza (**P**resentation)
- **A**way (**A**pplication)

Peer Layer Communication

Peer layers communicate with other layers in the OSI model and the layers underneath are their support systems. Peer layer communication is the "horizontal" link between devices on the network. Figure 1.18 shows three examples of *peer layer communication*. Keep in mind, however, that this principle applies to all seven layers of the OSI model. This allows for the layers to communicate with the layer to which a device is sending or receiving information.

FIGURE 1.18 Peer communication between three of the seven layers



Data Encapsulation

The purpose of *encapsulation* is to allow Application layer data communication between two stations on a network using the lower layers as a support system. As data moves down the OSI model from the source to the destination, it is encapsulated. As data moves back up the OSI model from the source to the destination, it is de-encapsulated. Some layers will add a header and/or trailer when information is being transmitted and remove it when information is being received. Encapsulation is the method in which lower layers support upper layers. Figure 1.19 illustrates this process.

Network Cables

An ethernet cable allows the user to connect their devices such as computers, mobile phones, routers, etc., to a Local Area Network (LAN) that will allow a user to have internet access, and able to communicate with each other through a wired connection. It also carries broadband signals between devices connected through it. In this article, we are going to discuss different types of ethernet cable used in local area networks for reliable internet connection.

Types of Ethernets Cables

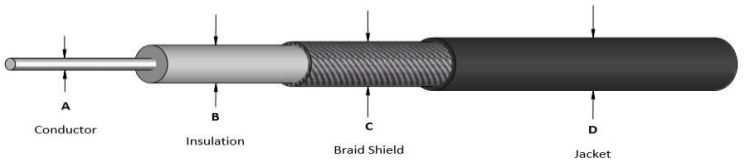
Mainly there are three types of ethernet cables used in LANs

- Coaxial Cables
- Twisted Pair Cables
- Fiber optic Cables

1. Coaxial Cables

A coaxial cable is used to carry high-frequency electrical signals with low losses. It uses 10Base2 and 10Base5 Ethernet variants. It has a copper conductor in the middle that is surrounded by a dielectric insulator generally made of PVC or Teflon. The dielectric insulator is surrounded by a plaited conducting metallic shield which reduces Electromagnetic Interference of the metal and outside interference and finally, the metallic shield is covered by a plastic covering called a sheath usually made of PVC or some other fire-resistant plastic material. Its maximum transmission speed is 10 Mbps. It is usually used in telephone systems, cable TV, etc.

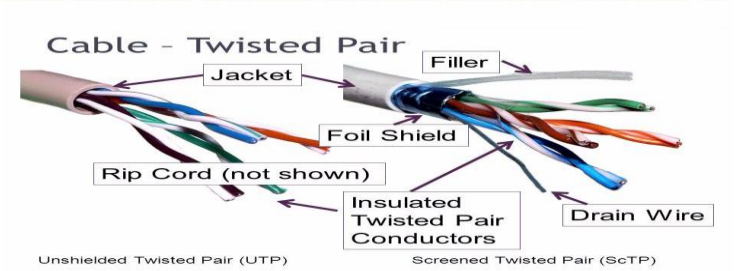
DESIGN: Coaxial cable design choices affect physical size, frequency performance, attenuation, power handling capabilities, flexibility, strength, and cost. It consists of an inner conductor which might be solid or stranded surrounded by an insulator and, to provide flexibility, it is further surrounded by a copper mesh which is further surrounded by a plastic or insulating jacket.



2. Twisted Pair Cable

A twisted pair is a copper wire cable in which two insulated copper wires are twisted around each other to reduce interference or crosstalk. It uses 10BASE-T, 100BASE-T, and some other newer ethernet variants. It uses RJ-45 connectors.

Design: A twisted pair cable usually contains two or more conducting wires either shielded by an insulator or not and, further these twisted pairs of wires are coated for protection from any damage.



Types of Twisted Pair Cable

Shielded Twisted Pair (STP) Cable: In STP the wires are covered by a copper braid covering or a foil shield, this foil shield adds a layer that protects it against interference leaking into and out of the cable. Hence, they are used for longer distances and higher transmission rates.
Unshielded Twisted Pair (UTP) Cable: Unshielded twisted pair cable is one of the most commonly used cables in computer networks at present time. UTP consists of two insulated copper wires twisted around one another, the twisting of wires helps in controlling interference.

Categories Of UTP Cables

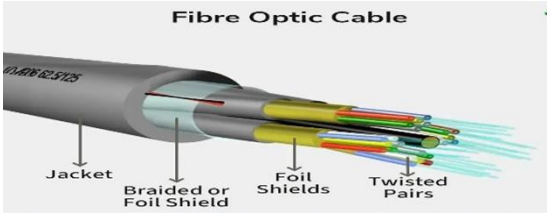
CATEGORIES	Bandwidth	Speed	Use
1	1.4 MHz	1 Mbps	Telephone wire
2	4 MHz	4 Mbps	Transmission Lines
3	16 MHz	16 Mbps	10BaseT Ethernet
4	20 MHz	20 Mbps	Used in Token Ring
5	100 MHz	100 Mbps	100BaseT Ethernet
5	100 MHz	1 Gbps	Gigabit Ethernet
5e	100 MHz	1 Gbps	Gigabit Ethernet
6	250 MHz	10 Gbps	Gigabit Ethernet
7	600 MHz	10 Gbps	Gigabit Ethernet
7a	1 GHz	Up to 10 Gbps	Gigabit Ethernet
8	2 GHz	25 Gbps up to 40 Gbps	Datacenters

3. Fiber optic cables

Fiber optic cables use optical fibers which are made of glass cores surrounded by several layers of covering material generally made of PVC or Teflon. It transmits data in the form of light signals due to which there are no interference issues in fiber optics. Fiber optics can transmit signals over a very long distance as compared to twisted pairs or coaxial cables. It uses 10BaseF,

100BaseFX, 100BaseBX, 100BaseSX, 1000BaseFx, 1000BaseSX, and 1000BaseBx ethernet variants. Hence, it is capable of carrying information at a great speed.

Design: An optical fiber consists of a core and a cladding chosen for their total internal reflection due to the difference in refractive index between the two. In real optical fibers, the cladding is usually covered with a layer of acrylate or polyimide polymer. The coating protects the fiber from damage and several layers of protective sheathing, depending on the application are added to form the cable.



Types of Fiber Optics Cable

Single-Mode Fiber: It uses one single ray of light to transmit data. It is used for long-distance transmission.

Multi-Mode Fiber: It uses multiple light rays to transmit data. It is comparatively less expensive.

Chapter

2

Protocols, IP Address Introduction to Cisco Packets Tracer, Basics Basics Commands & Etc.

TOPICS COVERED IN THIS CHAPTER:

- ✓ Networking Protocols
- ✓ Device Addressing
- ✓ Routing Protocols
- ✓ Servers
- ✓ TELNET, SSH & VPN
- ✓ Introduction To Cisco Packets Tracer
- ✓ Redistribution

Network Protocols

What is a Network Protocols?

A network protocol is a set of rules that govern data communication between different devices in the network. It determines what is being communicated, how it is being communicated, and when it is being communicated. It permits connected devices to communicate with each other, irrespective of internal and structural differences.

How do Network Protocols Work?

It is essential to understand how devices communicate over a network by recognizing network protocols. The Open Systems Interconnection (OSI), the most widely used model, illustrates how computer systems interact with one another over a network. The communication mechanism between two network devices is shown by seven different layers in the OSI model. Every layer in the OSI model works based on different network protocols. At every layer, one or more protocols are there for network communication. To enable network-to-network connections, the Internet Protocol (IP), for instance, routes data by controlling information like the source and destination addresses of data packets. It is known as a network layer protocol.

Types of Network Protocols

In most cases, communication across a network like the Internet uses the OSI model. The OSI model has a total of seven layers. Secured connections, network management, and network communication are the three main tasks that the network protocol performs. The purpose of protocols is to link different devices.

The protocols can be broadly classified into three major categories:

Network Communication
Network Management
Network Security

1. Network Communication

Communication protocols are important for the functioning of a network. They are so crucial that it is not possible to have computer networks without them. These protocols formally set out the rules and formats through which data is transferred. These protocols handle syntax, semantics, error detection, synchronization, and authentication. Below mentioned are some network communication protocols:

Hypertext Transfer Protocol (HTTP)

It is a layer 7 protocol that is designed for transferring a hypertext between two or more systems. HTTP works on a client-server model, most of the data sharing over the web is done through using HTTP.

Transmission Control Protocol (TCP)
TCP layouts a reliable stream delivery by using sequenced acknowledgment. It is a connection-oriented protocol i.e., it establishes a connection between applications before sending any data. It is used for communicating over a network. It has many applications such as emails, FTP, streaming media, etc.

User Datagram Protocol (UDP)
It is a connectionless protocol that lay-out a basic but unreliable message service. It adds no flow control, reliability, or error-recovery functions. UPD is functional in cases where reliability is not required. It is used when we want faster transmission, for multicasting and broadcasting connections, etc.

Internet Protocol (IP)
It is a protocol through which data is sent from one host to another over the internet. It is used for addressing and routing data packets so that they can reach their destination.

Dynamic Host Configuration Protocol (DHCP)
it's a protocol for network management and it's used for the method of automating the process of configuring devices on IP networks. A DHCP server automatically assigns an IP address and various other configurational changes to devices on a network so they can communicate with other IP networks. it also allows devices to use various services such as NTP, DNS, or any other protocol based on TCP or UDP.

2. Network Management
These protocols assist in describing the procedures and policies that are used in monitoring, maintaining, and managing the computer network. These protocols also help in communicating these requirements across the network to ensure stable communication. Network management protocols can also be used for troubleshooting connections between a host and a client.

Internet Control Message Protocol (ICMP)
It is a layer 3 protocol that is used by network devices to forward operational information and error messages. ICMP is used for reporting congestions, network errors, diagnostic purposes, and timeouts.

Simple Network Management Protocol (SNMP)
It is a layer 7 protocol that is used for managing nodes on an IP network. There are three main components in the SNMP protocol i.e., SNMP agent, SNMP manager, and managed device.

SNMP agent has the local knowledge of management details, it translates those details into a form that is compatible with the SNMP manager. The manager presents data acquired from SNMP agents, thus helping in monitoring network glitches, and network performance, and troubleshooting them.

File Transfer Protocol (FTP)
FTP is a client/server protocol that is used for moving files to or from a host computer, it allows users to download files, programs, web pages, and other things that are available on other services.

Post Office Protocol (POP3)
It is a protocol that a local mail client uses to get email messages from a remote email server over a TCP/IP connection. Email servers hosted by ISPs also use the POP3 protocol to hold and receive emails intended for their users. Eventually, these users will use email client software to look at their mailbox on the remote server and to download their emails. After the email client downloads the emails, they are generally deleted from the servers.

Telnet
It is a protocol that allows the user to connect to a remote computer program and to use it i.e., it is designed for remote connectivity. Telnet creates a connection between a host machine and a remote endpoint to enable a remote session.

3. Network Security
These protocols secure the data in passage over a network. These protocols also determine how the network secures data from any unauthorized attempts to extract or review data. These protocols make sure that no unauthorized devices, users, or services can access the network data. Primarily, these protocols depend on encryption to secure data.

Secure Socket Layer (SSL)
It is a network security protocol mainly used for protecting sensitive data and securing internet connections. SSL allows both server-to-server and client-to-server communication. All the data transferred through SSL is encrypted thus stopping any unauthorized person from accessing it.

Hypertext Transfer Protocol (HTTPS)
It is the secured version of HTTP. this protocol ensures secure communication between two computers where one sends the request through the browser and the other fetches the data from the web server.

Transport Layer Security (TLS)
It is a security protocol designed for data security and privacy over the internet, its functionality is encryption, checking the integrity of data i.e., whether it has been tampered

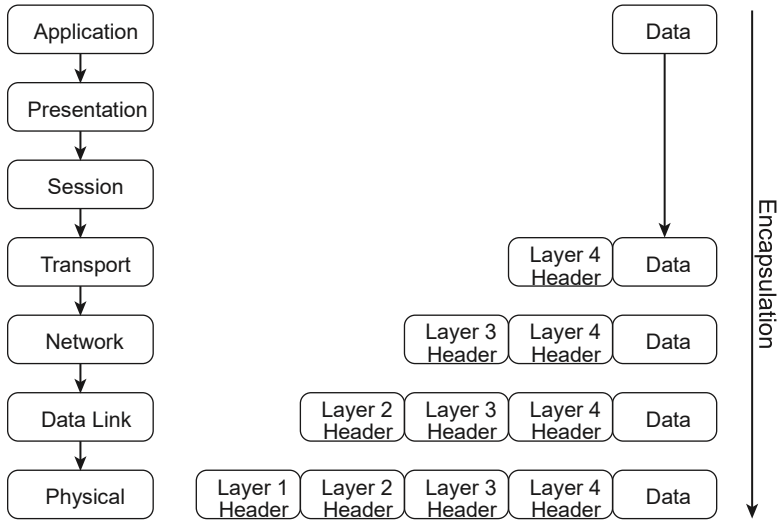
with or not, and authentication. It is generally used for encrypted communication between servers and web apps, like a web browser loading a website, it can also be used for encryption of messages, emails, and VoIP.

Device Addressing

Every device on a network requires unique identification. This can be accomplished in a couple of ways:

- Physical addresses
- Logical addresses

FIGURE 1.19 Information is added at each layer of the OSI model as data moves between devices



The physical address of a network adapter is also known as the Media Access Control (MAC) address. As shown in Figure 1.20, every device on a network (like every street address in a city) must have a unique address. The physical address is required in order for a device to send or receive information (data). An analogy to this is sending a package to be delivered via a courier service. Before you hand over the package to the courier, you would write the name and physical street address of the recipient on the package. This would ensure that the package is delivered correctly to the recipient.

The logical address is also known as the Internet Protocol (IP) address. Each device on a Layer 3 network or subnet must have a unique IP address (like every city's zip code). The IP address can be mapped to the physical address by using the Address Resolution Protocol (ARP).

The streets shown in Figure 1.20—1st, Main, and 2nd—represent local area network subnets. The street addresses—10, 20, and so on—represent the unique address of each structure on a street as a MAC address would a device on a LAN.

Physical Addressing

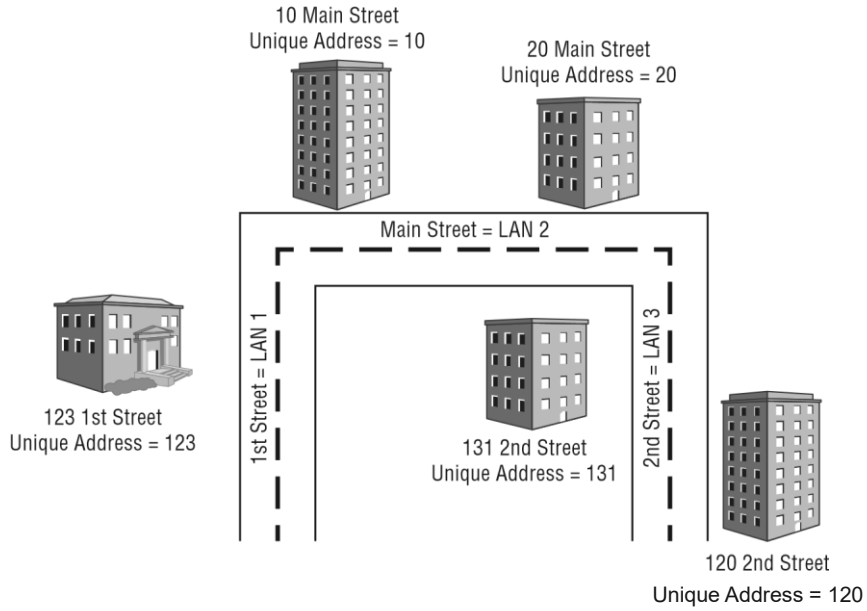
The physical address of a network device is called a MAC address because the *MAC sublayer* of the Data Link layer handles media access control. The MAC address is a 6-byte (12-character)

hexadecimal address in the format AB:CD:EF:12:34:56. The fi rst 3 bytes (or octets) of a MAC address are called the organizationally unique identifi er (OUI). Some manufacturers produce many network devices and therefore require several OUIs. A table of all OUIs is freely available from the IEEE Standards Association website at

http://standards.ieee.org/develop/regauth/oui/oui.txt

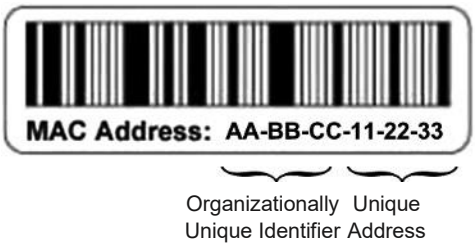
MAC addresses are globally unique; an example is shown in Figure 1.21. The fi rst 3 bytes or octets (6 characters) are issued to manufacturers by the IEEE. The last 3 bytes or octets (6 characters) are incrementally assigned to devices by the manufacturer.

FIGURE 1.20 The MAC address is analogous to the address of buildings on a street.



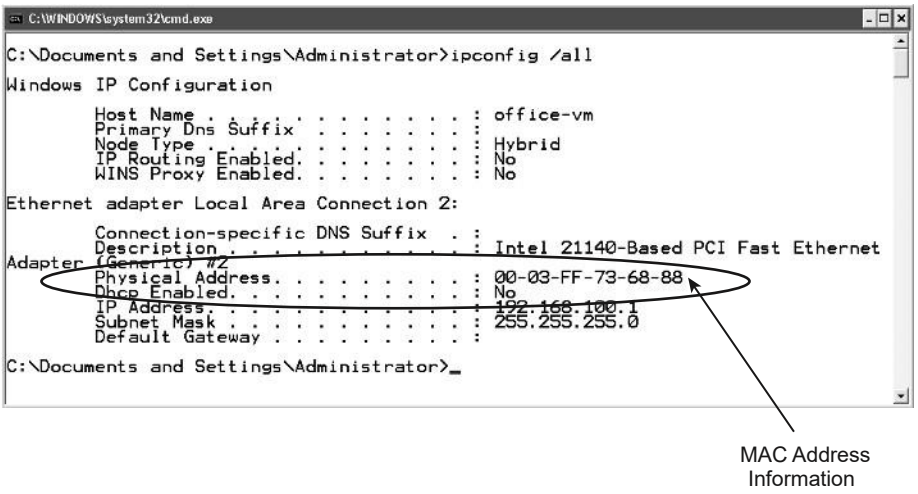
The streets shown—1st, Main, and 2nd—represent local area networks. The numbers 10, 20, 123, 131, and 120 represent the unique address of each structure on the streets just as MAC addresses would represent devices on a LAN.

FIGURE 1.21 Example of a Layer 2 MAC address shows the OUI and unique physical address



The MAC address of a device is usually stamped or printed somewhere on the device. This allows the device to be physically identifi ed by the MAC address. By typing the simple command **ipconfig /all** in the command-line interface of some operating systems, you can view the physical address of the network adapter. Figure 1.22 shows an example of the information displayed by using this command-line utility in the Microsoft Windows operating system.

FIGURE 1.22 The **ipconfig** command-line utility displaying a physical/MAC address in Microsoft Windows.



Logical Addressing

Network devices can also be identified by a logical address, known as the Internet Protocol (IP) address. The Layer 3 IP protocol works with a Layer 4 transport protocol, either User Datagram Protocol (UDP) or Transport layer Protocol (TCP). You learned earlier in this chapter that UDP is a connectionless protocol, and using it is analogous to sending a postcard through the mail. The sender has no way of knowing if the card was received by the intended recipient. TCP is a connection-oriented protocol, used for communications analogous to a telephone call, and provides guaranteed delivery of data through acknowledgements. During a telephone conversation, communication between two people will be confi rmed to be intact, with the users acknowledging the conversation. Routable logical addresses such as TCP/IP

addresses became more popular with the evolution of the Internet and the Hypertext Transfer Protocol (HTTP) that is used with the World Wide Web (WWW) service. IP moves data through an internetwork such as the Internet one router (or hop) at a time. Each router decides where to send the data based on the logical IP address. Figure 1.23 shows a basic network utilizing both Layer 2 and Layer 3 data traffic.

Logical addresses (IP addresses) are 32-bit dotted-decimal addresses usually written in the form www.xxx.yyy.zzz. Figure 1.24 illustrates an example of a logical Class C, 32-bit IP address. Each of the four parts is a byte, or 8 digital bits. There are two main IP address types: private addresses and public addresses. Private addresses are unique to an internal network, and public addresses are unique to the Internet. These addresses consist of two main parts: the network (subnet) and the host (device). Logical addresses also require a subnet mask and may have a gateway address depending on whether the network is routed. IPv4 addresses fall under three classes: Class A addresses, Class B addresses, and Class C addresses.

FIGURE 1.23 A network with Layer 3 network device logical addressing

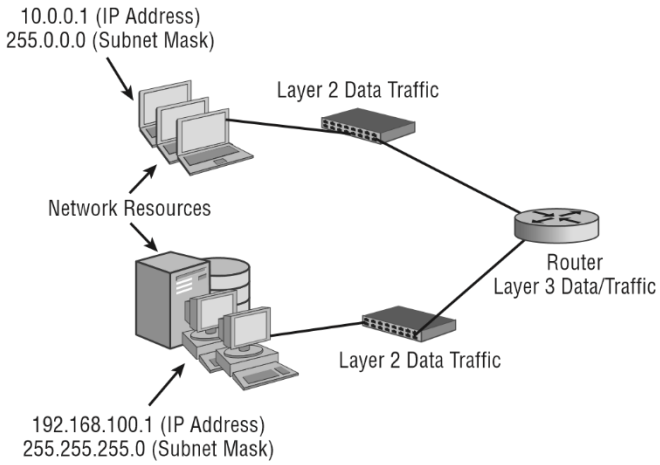
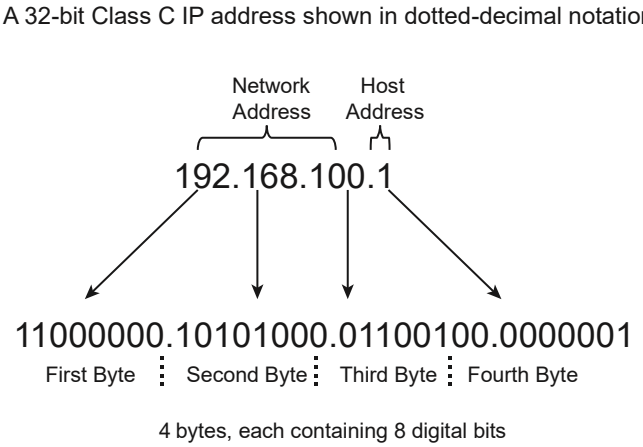
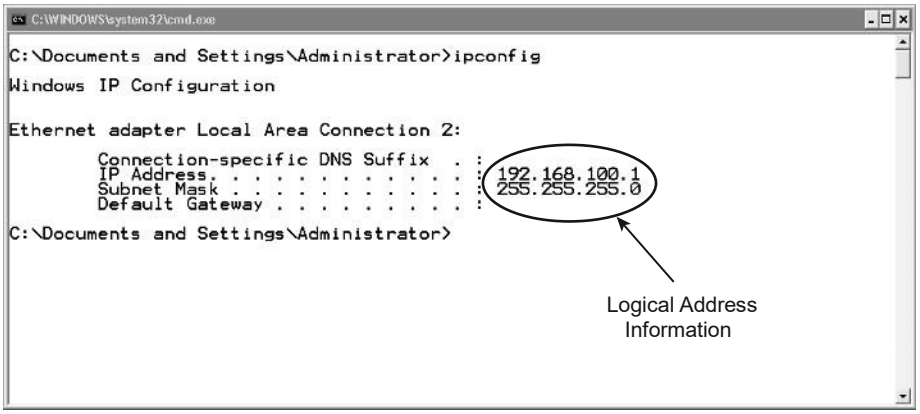


FIGURE 1.24 Example of a Class C logical IP address



Unlike a MAC address, an *IP address* is logical and can be either specifi ed as a static address assigned to the device manually by the user or dynamically assigned by a server. However, the same command-line utility used to identify the physical address of a device can be used to identify the logical address of a device. Typing **ipconfig** at a command prompt displays the logical address, including the IP address, subnet mask, and default gateway (router) of the device. The ipconfig /all command illustrated earlier in the chapter will yield additional information, including the physical or MAC address of the device's network adapter. This command is for a computer using the Microsoft Windows operating system. For some Apple and Linux devices, the ifconfig command will yield similar information. Figure 1.25 shows the ipconfig utility displaying the logical address information, including the IP address and subnet mask.

FIGURE 1.25 The Microsoft Windows **ipconfig** command-line utility showing logical address information



In Exercise 1.1, you will use the ipconfig utility from a command prompt on a computer using the Microsoft Windows operating system. This will allow you to see the address information for any available network adapters within the device.

Exercise 1.1 was written using a computer with the Microsoft Windows 7 operating system. If you're using another version of the operating system, the steps may vary slightly. Keep in mind that there are many different shortcuts and ways to get to a command prompt in the Microsoft operating systems. The steps in this exercise use one common method.

EXERCISE 1.1

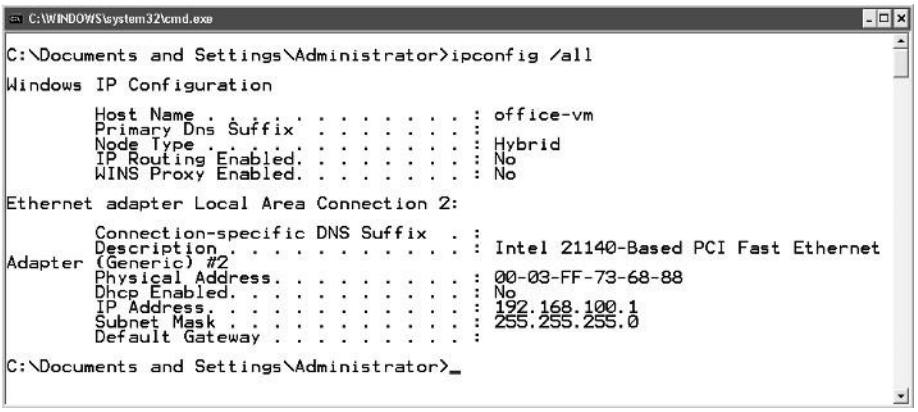
Viewing Device Address Information on a Computer

1. Click the Start button.
2. Mouse over the All Programs arrow. The All Programs window appears in the left pane.
3. Navigate to and click on the Accessories folder. The accessories programs appear.

4. Click the Command Prompt icon. The command window will appear.

5. In the command window, type **ipconfig /all**.

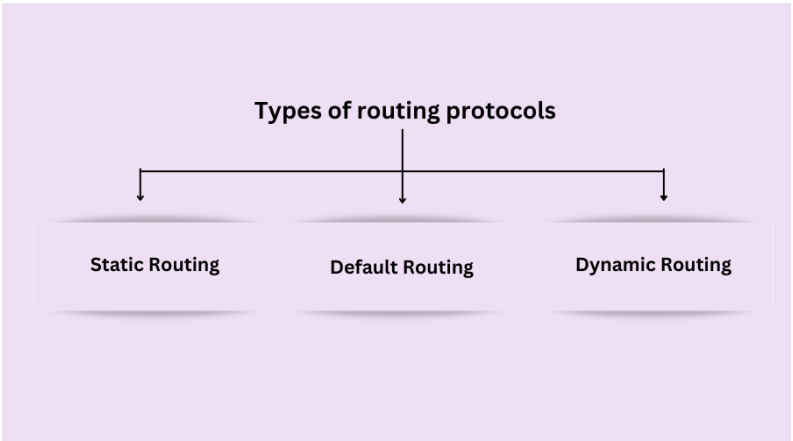
6. View the results in the command window. Notice the physical address of the network adapter as well as other information. The results should look similar to that shown here for Microsoft Windows 7 but may vary slightly based on the OS version in use.



Routing Protocols

Routing protocols are the set of rules and algorithms that routers use to communicate with each other to find the most efficient path to transmit data packets from a sender to a receiver. There are many routing protocols in computer networks, which we are going to discuss in this article, but to understand routing protocols properly, let us first understand routing.

The term "routing" comes from the word "route", which means the path used to transport data packets in computer networks. Routing is a procedure of moving data packets from one network to another by discovering the finest path from the source to the destination. The device that helps in finding the best path to forward data packets from the source of one network to the destination of another network is called a router.



1. Static Routing Protocol:

It can also be called **non-adaptive routing.** It is a manual configuration technique in which the network administrator selects the best path to transfer the data packet from source to destination. When a network administrator configures each router in the routing table by hand, it is called static routing. After that, the router forwards the data packets to the destination along the path defined by the network administrator.

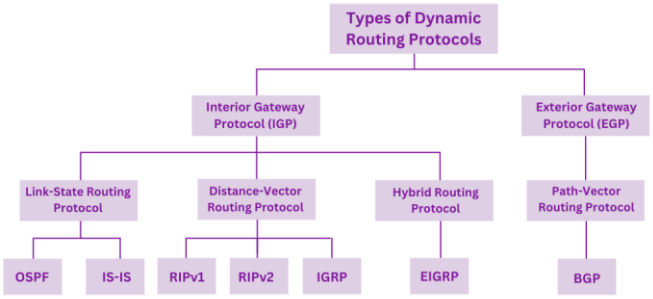
2. Default Routing Protocol:

The default routing protocol can also be called the default route. When a router faces a situation where it does not know the destination network of a data packet, then it uses a method called "default routing". It is an approach in which the router transfers all data packets to the single-hop device, regardless of the network.

The default route is the predetermined path the router uses to send all data packets when encountering such a situation. When the destination network is unknown to the router, then the router uses the default route and sends all data packets to that route.

3. Dynamic Routing Protocol:

It can also be called adaptive routing. It is an approach in which a router automatically finds the best path to transmit data packets from the sender to the receiver and puts the selected path information into the routing table of each router.
The router selects the path based on situations of the communication circuit or the network topology. If there is any loss of connection between the nodes or there is a problem with the route decided, the packed data is automatically adjusted on the new route to be forwarded towards t[illegible]ers are used.



Open Shortest Path First (OSPF)

is a link-state routing protocol that is used to find the best path between the source and the destination router using its own Shortest Path First). OSPF is developed by Internet Engineering

Task Force (IETF) as one of the Interior Gateway Protocol (IGP), i.e., the protocol which aims at moving the packet within a large autonomous system or routing domain. It is a network layer protocol which works on protocol number 89 and uses AD value 110. OSPF uses multicast address 224.0.0.5 for normal communication and 224.0.0.6 for update to designated router (DR)/Backup Designated Router (BDR).

Routing Information Protocol (RIP)

is a dynamic routing protocol that uses hop count as a routing metric to find the best path between the source and the destination network. It is a distance-vector routing protocol that has an AD value of 120 and works on the Network layer of the OSI model. RIP uses port number 520.

Hop Count:
Hop count is the number of routers occurring in between the source and destination network. The path with the lowest hop count is considered as the best route to reach a network and therefore placed in the routing table. RIP prevents routing loops by limiting the number of hops allowed in a path from source and destination. The maximum hop count allowed for RIP is 15 and a hop count of 16 is considered as network unreachable.

Dynamic routing Protocol performs the same function as static routing Protocol does. In dynamic routing Protocol, if the destination is unreachable then another entry, in the routing table, to the same destination can be used. One of the routing protocols is EIGRP.

Enhanced Interior Gateway Routing Protocol (EIGRP)

is a dynamic routing protocol that is used to find the best path between any two-layer 3 devices to deliver the packet. EIGRP works on network layer Protocol of OSI model and uses protocol number 88. It uses metrics to find out the best path between two layer 3 devices (router or layer 3 switches) operating EIGRP. Administrative Distance for EIGRP are:-

EIGRP routes	AD values
Summary Routes	5
Internal Routes	90
external routes	170

Servers

A server is a hardware device or software that processes requests sent over a network and replies to them. A client is the device that submits a request and waits for a response from the

server. The computer system that accepts requests for online files and transmits those files to the client is referred to as a “server” in the context of the Internet.

There are so many types of Servers below we are going to discuss few

1. A web server

A web server is a software application or hardware device that stores, processes, and serves web content to users over the internet. It plays a critical role in the client-server model of the World Wide Web, where clients (typically web browsers) request web pages and resources, and servers respond to these requests by delivering the requested content.
Web servers operate on the Hypertext Transfer Protocol (HTTP), which is the foundation of data communication on the World Wide Web. When you enter a website’s URL into your browser, it sends an HTTP request to the web server hosting that website, which then sends back the web page you requested, allowing you to view it in your browser.

2. An email server

also known as a mail server, is a specialized computer system that manages the sending, receiving, and storage of email messages. It plays a crucial role in the email delivery process by using specific protocols to transfer messages between email clients (like Gmail, Outlook, etc.).

There are two main types of email servers:
Outgoing Mail Servers (Mail Transfer Agents - MTA): These handle the sending of emails from the sender’s email client to the recipient’s email server using protocols like SMTP (Simple Mail Transfer Protocol).
Incoming Mail Servers (Mail Delivery Agents - MDA): These manage the retrieval and storage of emails for the recipient’s email client using protocols like IMAP (Internet Message Access Protocol) or POP3 (Post Office Protocol Version 3)

3. A DNS (Domain Name System) server

is like the internet’s phonebook. When you type a website’s name into your browser, the DNS server translates that name into an IP address, which is a series of numbers that computers use to identify each other on the network. This process allows your browser to find and load the website you’re looking for.
There are different types of DNS servers, including:
Recursive resolvers: These servers receive queries from clients and interact with other DNS servers to find the correct IP address.
Root nameservers: The first step in translating domain names into IP addresses.
TLD (Top-Level Domain) nameservers: These servers store information for domains like .com, .org, etc.
Authoritative nameservers: These servers provide the actual IP address for the requested domain

TELNET, SSH AND VPN

Telnet

Telnet is a network protocol used to provide a bidirectional interactive text-oriented communication facility using a virtual terminal connection.
Security: Telnet is not secure as it transmits data in plaintext, making it vulnerable to interception and attacks.
Usage: It's mostly used for remote management of devices and systems, but due to its lack of security, it's largely been replaced by more secure protocols like SSH.

SSH (Secure Shell)

SSH is a cryptographic network protocol for operating network services securely over an unsecured network.
Security: SSH encrypts the data being transferred, providing confidentiality and integrity.
Usage: Commonly used for secure remote login, command execution, and secure file transfers. It can also create secure tunnels for other applications.

VPN (Virtual Private Network)

VPN creates a secure connection over a less secure network, such as the internet.
Security: VPNs encrypt all internet traffic from your device, masking your IP address and protecting your data from eavesdropping.
Usage: Used for secure access to a private network, protecting data on public Wi-Fi, bypassing geo-restrictions, and enhancing online privacy.

Each of these technologies serves different purposes and offers varying levels of security. If you need secure remote access to a server, SSH is ideal. For securing all your internet traffic, a VPN is the better choice. Telnet, while useful in the past, is now largely obsolete due to its lack of security.

Introduction To Cisco Packets Tracer

Cisco Packet Tracer as the name suggests, is a tool built by Cisco. This tool provides a network simulation to practice simple and complex networks.

The main purpose of Cisco Packet Tracer is to help students learn the principles of networking with hands-on experience as well as develop Cisco technology specific skills.

Since the protocols are implemented in software only method, this tool cannot replace the hardware Routers or Switches. Interestingly, this tool does not only include Cisco products but also many more networking devices.

Using this tool is widely encouraged as it is part of the curriculum like CCNA, CCENT where Faculties use Packet Trace to demonstrate technical concepts and networking systems. Student's complete assignments using this tool, working on their own or in teams.

Engineers prefer to test any protocols on Cisco Packet Tracer before implementing them. Also, Engineers who would like to deploy any change in the production network prefer to use Cisco Packet Tracer to first test the required changes and proceed to deploy if and only if everything is working as expected.

This makes the job easier for Engineers allowing them to add or remove simulated network devices, with a Command line interface and a drag and drop user interface.

You can download the tool from https://www.netacad.com by clicking on the Packet Tracer graphic and selecting the appropriate OS package, then you are good to play with it.

This course will help you kick start using the tool: https://www.netacad.com/courses/packet-tracer/introduction-packet-tracer.

Workspace:

Logical –
Logical workspace shows the logical network topology of the network the user has built. It represents the placing, connecting and clustering virtual network devices.
Physical –
Physical workspace shows the graphical physical dimension of the logical network. It depicts the scale and placement in how network devices such as routers, switches and hosts would look in a real environment. It also provides geographical representation of networks, including multiple buildings, cities and wiring closets.

Key Features:

Unlimited devices
E-learning
Customize single/multi user activities
Interactive Environment
Visualizing Networks
Real-time mode and Simulation mode
Self-paced

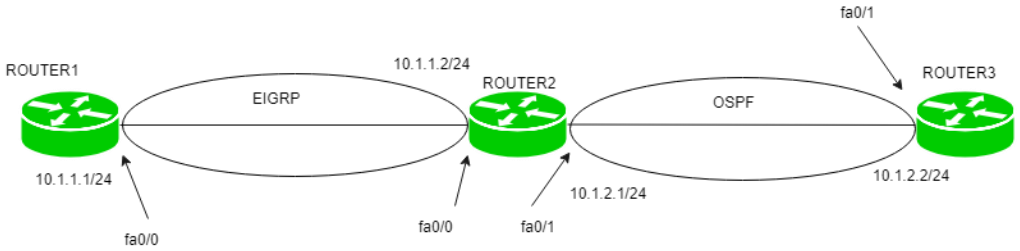
Supports majority of networking protocols
International language support
Cross platform compatibility

Redistribution in Computer Network

Often, using a single routing protocol in an organisation is preferred but there are some conditions in which we have to use multi protocol routing. These conditions include multiple administrator running multiple protocols, company mergers or usage of multi-vendors devices. Therefore, we have to advertise a route learned through a routing protocol or by any other means (like static route or directly connected route) in different routing protocol. This process is called redistribution.

Redistribution –

It is a process of advertising a route learned by method of static routing, directly connected route or a dynamic routing protocol into another routing protocol.Summary
This chapter provided a survey of networking topics to help you understand the basics of computer networking as an introduction or a simple review. It began with an outline of the common network technology types:



For example, here, router2 one interface (fa0/0) is running EIGRP and other interface(fa0/1) is running OSPF then we have to advertise the routes of OSPF into EIGRP and vice-versa so that the routes learned by these routing protocols are advertised with each other. This process is called redistribution. Otherwise, the router1 will not be able to learn routes of router3 and router3 will not be able to learn routes of router1.

Metric –
As we know, different routing protocols use different metrics to find out best path therefore when we redistribute route from one routing protocol to another, we must define metric which should be understandable by the routing protocol.

For example, as we know RIP uses hop count as metric whereas EIGRP uses composite matrix which consists of Bandwidth, load, delay, reliability and MTU (from which only Bandwidth

and delay are used). Therefore, when we will advertise the routes of EIGRP into RIP we have to define metric Hop count.

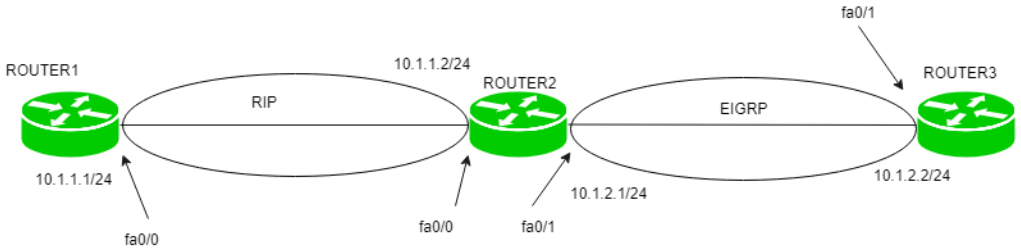
Example –

```
router(config)router rip
router(config-router)#redistribute Eigrp 1 metric 1
```

Where metric 1 means hop count 1 while EIGRP 1 means autonomous system 1.

Configuration –

1. When router's one interface is operating RIP and other interface is operating EIGRP.



Here is a small topology in which 3 routers are connected with each other. Router1 has IP address 10.1.1.1/24 on fa0/0, Router2 has IP address 10.1.1.2/24 on fa0/0 and 10.1.2.1/24 on fa0/1 and Router3 has ip address 10.1.2.1/24 on fa0/0.
Router2 has interface fa0/0 operating RIP and fa0/1 operating EIGRP and Router1 is operating RIP and Router3 is operating EIGRP as shown in the figure.

Now, configuring RIP on Router1.

```
Router1(config)#router rip
Router1(config-router)#network 10.1.1.0
Router1(config-router)#no auto-summary
```

Configuring EIGRP on Router3:

```
Router3(config)#router Eigrp 100
Router3(config-router)#network 10.1.2.0
Router3(config-router)#no auto-summary
```

Now, configuring RIP and EIGRP on Router2.

```
Router2(config)#router rip
```

```
Router2(config-router)#network 10.1.1.0
Router2(config-router)#no auto-summary
Router2(config-router)#exit
Router2(config)#router Eigrp 100
Router2(config-router)#network 10.1.2.0
Router2(config-router)#no auto-summary
```

Now, configuring redistribution on Router2, First redistributing routes of EIGRP in RIP:

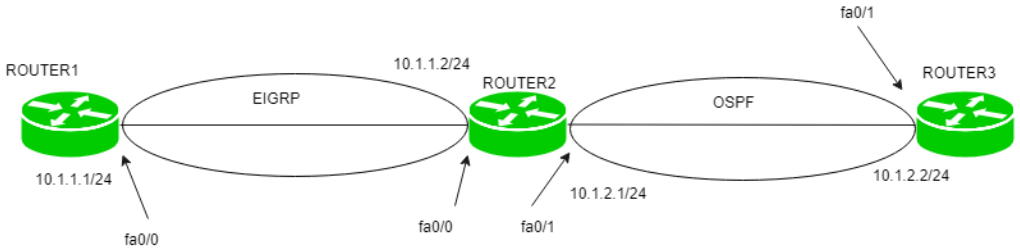
```
Router2(config)#router rip
Router2(config-router)#redistribute eigrp 100 metric 1
```

Here, RIP uses metric hop count therefore we have given metric 1. Now, redistributing routes of RIP in EIGRP:

```
Router2(config)#router eigrp 100
Router2(config-router)#redistribute rip metric 1 0 1 1 1
```

Here, EIGRP uses metric composite matrix therefore, we have used k values (1 0 1 1 1).

2. When router's one interface is operating OSPF and other interface is operating EIGRP.



Using the same topology. Router1 has IP address 10.1.1.1/24 on fa0/0, Router2 has IP address 10.1.1.2/24 on fa0/0 and 10.1.2.1/24 on fa0/1 and Router3 has ip address 10.1.2.1/24 on fa0/0.

Router2 has interface fa0/0 operating EIGRP and fa0/1 operating OSPF and Router1 is operating EIGRP and Router3 is operating OSPF as shown in the figure.

Now, configuring EIGRP on Router1.

```
Router1(config)#router Eigrp 100
```

```
Router1(config-router)#network 10.1.1.0
Router1(config-router)#no auto-summary
```

Configuring OSPF on Router3:

```
Router3(config)#router ospf 1
Router3(config-router)#network 10.1.2.0 0.0.0.255 area 0
```

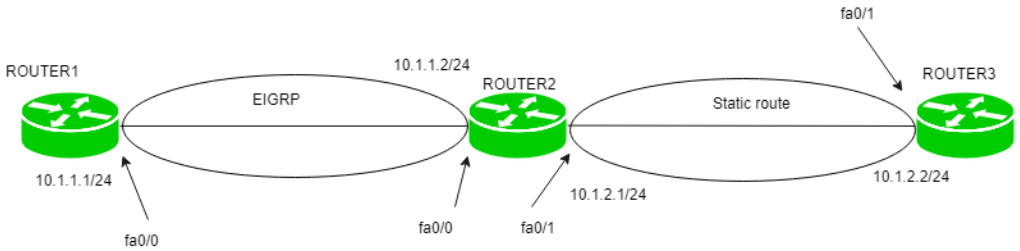
Configuring EIGRP and OSPF on Router2.

```
Router2(config)#router eigrp 100
Router2(config-router)#network 10.1.1.0
Router2(config-router)#no auto-summary
Router2(config-router)#exit
Router2(config-router)#router ospf 1
Router2(config-router)#network 10.1.2.0 0.0.0.255 area 0
```

Now, redistribution on Router2:

```
Router2(config)#router Eigrp 100
Router2(config-router)#redistribute ospf 1 metric 1 0 1
1 1
Router2(config-router)#exit
Router2(config)#router ospf 1
Router2(config-router)#redistribute eigrp 100 subnets
```

3. When router's one interface is operating EIGRP and other interface is given a static route.



Using the same topology. Router1 has IP address 10.1.1.1/24 on fa0/0, Router2 has IP address 10.1.1.2/24 on fa0/0 and Router2 has interface fa0/0 operating EIGRP and Router1 is operating EIGRP and Router3 is given static as shown in the figure.

```
Router1(config)#router eigrp 100
Router1(config-router)#network 10.1.1.0
Router1(config-router)#no auto-summary
```

Now, giving static route to Router3.

```
Router3(config)#ip route 10.1.1.0 255.255.255.0 10.1.2.2
```

Now, configuring EIGRP on Router2.

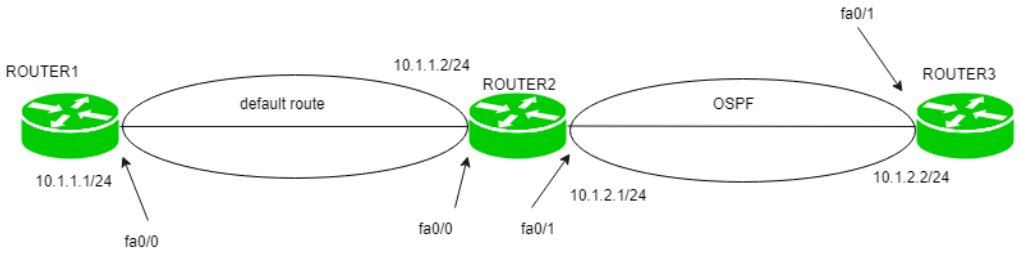
```
Router2(config)#router eigrp 100
Router2(config-router)#network 10.1.1.0
Router2(config-router)#no auto-summary
```

Now, redistribution on Router2

```
Router2(config)#router Eigrp 100
Router2(config-router)#redistribute static metric 1 0 1 1 1
```

Note – There is no need to give static route on Router2 as it is directly connected to 10.1.1.0 and 10.1.2.0 networks.

4. When router's one interface is operating OSPF and other interface is given a default route



Using the same topology. Router1 has IP address 10.1.1.1/24 on fa0/0, Router2 has IP address 10.1.1.2/24 on fa0/0 and 10.1.2.1/24 on fa0/1 and Router3 has ip address 10.1.2.1/24 on fa0/0.

Router2 has interface fa0/1 operating OSPF and Router1 is given default route and Router3 is operating OSPF as shown in the figure.

Configuring default route on Router1.

```
Router1(config)#ip route 0.0.0.0 0.0.0.0 10.1.1.2
```

Configuring OSPF on Router3:

```
Router3(config)#router ospf 1

Router3(config-router)#network 10.1.2.0 0.0.0.255 area 0
```

Configuring ospf on Router2:

```
Router2(config)#router ospf 1

Router2(config-router)#network 10.1.2.0 0.0.0.255 area 0
```

Now, redistributing on Router2:

```
Router2(config)#router OSPF 1

Router2(config-router)#default-information originate
```

Summary

This chapter provided a survey of networking topics to help you understand the basics of computer networking as an introduction or a simple review. It began with an outline of the common network technology types:

- Local area networks (LANs)
- Wide area networks (WANs)
- Metropolitan area networks (MANs)
- Campus area networks (CANs)
- Personal area networks (PANs)

The next fundamental networking concept discussed was computer network topologies. You learned about network topologies ranging from the legacy high-speed linear bus and ring to the current star topology, the most common topology used today with both wired and wireless networks. You looked at the following various topologies:

- Bus
- Ring
- Star
- Mesh
- Ad hoc
- Point-to-point
- Point-to-multipoint

You then reviewed the basics and different layers of the OSI model, including a brief overview of each layer illustrating the different protocols and sublayers where applicable. Then I discussed the basics of peer communications and data encapsulation. The chapter's final topic was device addressing. You explored the concepts of physical (MAC Sublayer) and logical (Network layer) addressing, including the IP address and sub net mask. A simple exercise using a computer with the Microsoft Windows operating sys tem showed how to view device addressing information.

Chapter Essentials

Understand the components of a local area network (LAN). A local area network is a group of computers connected by a physical medium in a specifi c arrangement called a topology.

Know the different types of networks. The basic networks types are LAN, WAN, CAN, MAN, and PAN.

Become familiar with various networking topologies. Bus, star, ring, mesh, and ad hoc are some of the topologies used in computer networking. Bus is considered legacy, and the star topology is one of the most common in use today.

Understand point-to-point and point-to-multipoint connections. These can consist of both wired and wireless connections and will connect two or more LANs.

Understand the OSI model basics. Each of the seven layers of the OSI model serves a specifi c function. It's benefi cial to have an overall understanding of all seven layers.

Remember the details of the lower two layers of the OSI model. The Physical layer and Data Link layer are the two lowest layers in the OSI model. Wireless networking technol ogy operates at these layers. The Data Link layer consists of two sublayers: the Logical Link Control (LLC) sublayer and the Media Access Control (MAC) sublayer.

Understand device addressing. Devices are assigned a unique physical address by the manufacturer. This address is known as the MAC address. MAC addresses consist of two parts, the organizationally unique identifi er (OUI) and the unique physical address. A logi cal address may also be assigned at the Network layer to identify devices on different inter networks using the Internet Protocol (IP).