INTRODUCTION TO COMPUTER NETWORK

By

Abdul Hadi Mohammed Alaidi
Haider TH. Salim ALRikabi
Omar Hisham Yahya

Deposit number in the Iraqi National Library (2672 30/9/2020)

AL-MUTANABE

PREFACE

This book is designed for a student who wants to study the principle of the computer network in Iraqi university. The text covers the concepts that students will encounter in many disciplines such as computer science and computer engineering. Besides reading the book, students are strongly encouraged to do all the exercises. Students are strongly encouraged to keep up with the exercises and the sequel of concepts as they are going along.

This text contains all information relevant for the exams. Furthermore, the exercises in this text are those which will be demonstrated in the tutorials. Each sheet of exercises contains some important ones marked with a star and some other ones

Table of Contents

Table of Figure

CHAPTER 1

Introduction

1.1 Bandwidth

Bandwidth is defined as the amount of information that can flow through a network connection in a given periodic time. It is important to understand the concept of bandwidth for the following reasons.

- **Bandwidth** is Finite. Regardless of the media used to build a network, there are limits on the network capacity to carry information. Bandwidth is limited by the laws of physics and by the technologies used to place information on the media. For example, the bandwidth of a conventional modem is limited to about 56 kbps by both the physical properties of twisted-pair phone wires and by modem technology. DSL uses the same twisted-pair phone wires. However, DSL provides much more bandwidth than conventional modems. So, even the limits imposed by the laws of physics are sometimes difficult to define. Optical fiber has the physical potential to provide virtually limitless bandwidth. Even so, the bandwidth of optical fiber cannot be fully realized until technologies are developed to take full advantage of its potential.

- **Bandwidth is not free**. It is possible to buy equipment for a LAN that will provide nearly unlimited bandwidth over a long period of time. For WAN connections, it is usually necessary to buy bandwidth from a service provider. In either case, individual users and businesses can save a lot of money if they understand bandwidth and how the demand will change over time. A network manager needs to make the right decisions about the kinds of equipment and services to buy.
- **Bandwidth is an important factor that is used to analyze network performance, design new networks, and understand the Internet.** A networking professional must understand the tremendous impact of bandwidth and throughput on network performance and design. Information flows as a string of bits from computer to computer throughout the world. These bits represent massive amounts of information flowing back and forth across the globe in seconds or less.
- **The demand for bandwidth continues to grow**. As soon as new network technologies and infrastructures are built to provide greater bandwidth, new applications are created to take advantage of the greater capacity. The delivery of rich media content such as streaming video and audio over a network requires tremendous amounts of bandwidth. IP telephony systems are now commonly installed in place of traditional voice systems, which further adds to the need for bandwidth. The successful networking professional must

anticipate the need for increased bandwidth and act accordingly.

1.2 Digital Versus Analog

Bandwidth Radio, television, and telephone transmissions have, until recently, been sent through the air and over wires using electromagnetic waves. These waves are called analog because they have the same shapes as the light and sound waves produced by the transmitters. As light and sound waves change size and shape, the electrical signal that carries the transmission changes proportionately. In other words, the electromagnetic waves are analogous to the light and sound waves. Analog bandwidth is measured by how much of the electromagnetic spectrum is occupied by each signal. The basic unit of analog bandwidth is hertz (Hz), or cycles per second. While analog signals are capable of carrying a variety of information, they have some significant disadvantages in comparison to digital transmissions. The analog video signal that requires a wide frequency range for transmission cannot be squeezed into a smaller band. Therefore, if the necessary analog bandwidth is not available, the signal cannot be sent. In digital signaling, all information is sent as bits, regardless of the kind of information it is. Voice, video, and data all become streams of bits when they are prepared for transmission over digital media. This type of transmission gives digital bandwidth an important advantage over analog bandwidth. Unlimited amounts of information can be sent over the smallest or lowest bandwidth digital channel. Regardless of how long it takes for the digital information to arrive at its destination and be reassembled, it can be viewed, listened to, read, or processed in its original form. It is important to understand the differences and similarities between digital and analog bandwidth. Both types of bandwidth are regularly encountered in the field of information technology. However, because this course is concerned primarily with digital networking, the term bandwidth will refer to digital bandwidth.

1.3 Bandwidth Measurement

In digital systems, the basic unit of bandwidth is bits per second (bps). Bandwidth is the measure of how many bits of information can flow from one place to another in a given amount of time. Although bandwidth can be described in bps, a larger unit of measurement is generally used in Table. (1). Although the terms bandwidth and speed are often used interchangeably, they are not the same thing. One may say, for example, that a T3 connection at 45 Mbps operates at a higher speed than a T1 connection at 1.544 Mbps. However, if only a small amount of their data-carrying capacity is being used, each of these connection types will carry data at roughly the same speed. For example, a small amount of water will flow at the same rate through a small pipe as through a large pipe. Therefore, it is usually more accurate to say that a T3 connection has greater bandwidth than a T1 connection. This is because the T3 connection is able to carry more information at the same time, not because it has a higher speed.

Table 1-1 Unit of Bandwidth

Unit of Bandwidth	Abbreviation	Equivalence
Bits per second	bps	1bps=fundamental unit of bandwidth
Kilobits per second	kbps	1kbps=1,000bps=10^{3}bps
Megabits per second	Mbps	1Mbps=1,000,000bps=10^{6}bps
Gigabits per second	Gbps	1Gbps=1,000,000,000bps=10^{9}bps
Terabits per second	Tbps	1Tbps=1,000,000,000,000bps=10^{12}bps

1.4 Bandwidth Limitation

Bandwidth varies depending upon the type of media as well as the LAN and WAN technologies used. The physics of the media account for some of the difference. Signals travel through a twisted-pair copper wire, coaxial cable, optical fiber, and air. The physical differences in the ways signals travel result in fundamental limitations on the information-carrying capacity of a given medium. However, the actual bandwidth of a network is determined by a combination of the physical media and the technologies chosen for signaling and detecting network signals. For example, current information about the physics of unshielded twisted-pair (UTP) copper cable puts the theoretical bandwidth limit at over 1 Gbps. However, in actual practice, the bandwidth is determined by the use of 10BASE-T, 100BASE-TX, or 1000BASE-TX Ethernet. The actual bandwidth is determined by the signaling methods, NICs, and other network equipment that is chosen. Therefore, the bandwidth is not determined solely by the limitations of the medium.

Table 1-2 Shows some common networking media types along with their distance and bandwidth limitations

Typical Media	**Maximum Theoretical Bandwidth**	**Maximum Theoretical Distance**
50-Ohm Coaxial Cable (10BASE2 Ethernet; Thinnet)	10Mbps	185m
50-Ohm Coaxial Cable (10BASE2 Ethernet; Thicknet)	10Mbps	500m
Category 5 Unshielded Twisted Pair (UTP) (10BASE-T Ethernet)	10Mbps	100m
Category 5 Unshielded Twisted Pair (UTP) (100BASE-TX Ethernet)	100Mbps	100m
Category 5 Unshielded Twisted Pair (UTP) (1000BASE-TX Ethernet)	1000Mbps	100m

Multimedia Optical Fiber (62.5/125μm) (100BASE-Fx Ethernet)	100Mbps	220m
Multimedia Optical Fiber (62.5/125μm) (100BASE-Fx Ethernet)	1000Mbps	220m
Multimedia Optical Fiber (50/125μm) (1000BASE-Sx Ethernet)	1000Mbps	550m
Single mode Optical Fiber (9/125μm) (1000BASE-Lx Ethernet)	1000Mbps	5000m

Table 1-3 Summarizes common WAN services and the bandwidth associated with each service

WAN Service	**Typical User**	**Bandwidth**
Modem	Individuals	56kbps=0.056Mbps
DSL	Individuals, Telecommuters, and Small Businesses	128kbps to 6.1Mbps= 0.128Mbps to 6.1Mbps
ISDN	Telecommuters and Small Businesses	128kbps=0.128Mbps
Frame Relay	Small institutions (schools) and reliable WANs	56kbps to 44.736Mbps (U.S.) or 34.368Mbps (Europe)= 0.056Mbps to 44.736Mbps (U.S.) or 34.368Mbps (Europe)
T1	Large entities	1.544Mbps
E1	Large entities	2.048Mbps

T3	Large entities	44.736Mbps
E3	Large entities	34.368Mbps
STS-1 (OC-1)	Phone companies; Data-Comm company backbones	51.840Mbps
STM-1	Phone companies; Data-Comm company backbones	155.52Mbps
STS-3 (OC-3)	Phone companies; Data-Comm	155.251Mbps
STS-3 (OC-3)	Phone companies; Data-Comm company backbones	155.251Mbps
STM-3	Phone companies; Data-Comm company backbones	466.56Mbps
STS-48 (OC-48)	Phone companies; Data-Comm company backbones	2.488320Gbps

1.5 Bandwidth Throughput

Bandwidth is the measure of the amount of information that can move through the network in a given time. Therefore, the amount of available bandwidth is a critical part of the specification of the network. A typical LAN might be built to provide 100 Mbps to every desktop workstation, but this does not mean that each user can move 100 megabits of data through the network for every second of use. This would be true only under the most ideal circumstances. Throughput refers to actual measured bandwidth, at a specific time of day, using specific internet routes, and while a specific set of data is transmitted on the network. Unfortunately, for many reasons, throughput is often far less than the maximum possible digital bandwidth of the medium that is being used. The following are some of the factors that determine throughput:

1. Internetworking devices
2. Type of data being transferred
3. Network topology
4. Number of users on the network
5. User computer
6. Server computer
7. Power conditions

The theoretical bandwidth of a network is an important consideration in network design because the network bandwidth will never be greater than the limits imposed by the chosen media and networking technologies. However, it is just as important for a network designer and administrator to consider the factors that may affect actual throughput. By measuring throughput regularly, a network administrator will be aware of changes in network performance and changes in the needs of network users. The network can then be adjusted accordingly.

1.6 Round-trip time (RTT)

The second performance metric, latency, corresponds to how long it takes a message to travel from one end of a network to the other. (As with bandwidth, we could be focused on the latency of a single link or an end-to-end channel.) Latency is measured strictly in terms of time. For example, a transcontinental network might have a latency of 24 milliseconds (ms); that is, it takes a message 24 ms to travel from one coast of North America to the other. There are many situations in which it is more important to know how long it takes to send a message from one end of a network to the other and back, rather than the one-way latency. We call this the *round-trip time (RTT)* of the network.

1.7 Data Transfer Calculations

Network designers and administrators are often called upon to make decisions regarding bandwidth. One decision might be whether to increase the size of the WAN connection to accommodate a new database. Another decision might be whether the current LAN backbone is of sufficient bandwidth for a streaming video training program. The answers to problems like these are not always easy to find, but one place to start is with a simple data transfer calculation. Using the formula transfer time = size of file/bandwidth (T=S/BW) allows a network administrator to estimate several of the important components of network performance. If the typical file size for a given application is known, dividing the file size by the network bandwidth yields an estimate of the fastest time that the file can be transferred.

$$Latency = Propagation + Transmit + Queue$$

$$Propagation = Distance/SpeedOfLight$$

$$Transmit = Size/Bandwidth$$

$$Best\ Download\ \ \mathrm{T} = \frac{\mathrm{S}}{\mathrm{BW}}$$

$$Typical\ Download\ \mathrm{T} = \frac{\mathrm{S}}{\mathrm{P}}$$

BW	Maximum theoretical bandwidth of the “slowest link” between the source host and the destination host (measured in bits per seconds)
P	Actual throughput at the moment of transfer (measured in bits per seconds)
T	Time for file transfer to occur (measured in seconds)
S	File size in bits

Two important points should be considered when doing this calculation.

1- The result is an estimate only because the file size does not include any overhead added by encapsulation.

2- The result is likely to be a best-case transfer time because available bandwidth is rarely at the theoretical maximum for the network type. A more accurate estimate can be attained if throughput is substituted for bandwidth in the equation.

For example:

Consider a digital library program that is being asked to fetch a 25-megabyte (MB) image—the more bandwidth that is available, the faster it will be able to return the image to the user. Here, the bandwidth of the channel dominates performance. To see this, suppose that the channel has a bandwidth of **10 Mbps**. It will take 20 seconds to transmit the image

$$\mathrm{T}=25 \times 10^{6} \times 8 \text{ bits} \div 10 \times 10^{6} \text{ Mbps} = 20 \text{ seconds}$$

Figure 1 gives you a sense of how latency or bandwidth can dominate performance in different circumstances. The graph shows how long it takes to move objects of various sizes (**1 byte, 2 KB, 1 MB**) across networks with RTTs ranging from 1 to 100 ms and link speeds of either 1.5 or 10 Mbps. We use logarithmic scales to show relative performance. For a 1-byte object (say, a keystroke), latency remains almost exactly equal to the RTT, so that you cannot distinguish between a 1.5-Mbps network and a 10-Mbps network. For a 2-KB object (say, an email message), the link speed makes quite a difference on a 1-ms RTT network but a negligible difference on a 100-ms RTT network. And for a 1-MB object (say, a digital image), the RTT makes no difference—it is the link speed that dominates performance across the full range of RTT.

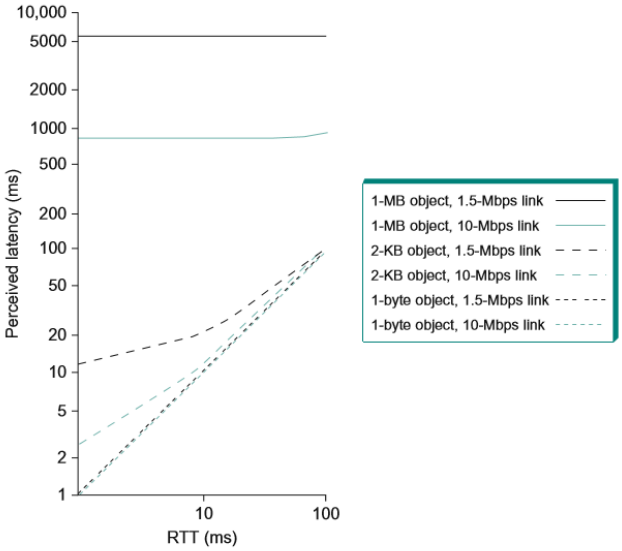


Figure 1-1 Perceived latency (response time) versus round trip time for various object sizes and link speeds

1.8 Exercise:

1- Define Bandwidth and why it’s important.?

2- What are the factors that determine throughput?

3- How long does it take to transmit a x KB over a y-Mbps link? Give your answer as a ratio of x and y.

4- Consider a point-to-point link 4 km in length. At what bandwidth would propagation delay (at a speed of $2 \times 10^8\ m/s$) equal transmit delay for 100-byte packets? What about 512-byte packets?

CHAPTER 2

Data Network

2.1 Introduction

Data networks developed as a result of business applications that were written for microcomputers. The microcomputers were not connected so there was no efficient way to share data among them. It was not efficient or cost-effective for businesses to use floppy disks to share data. Sneakernet created multiple copies of the data. Each time a file was modified it would have to be shared again with all other people who needed that file. If two people modified the file and then tried to share it, one of the sets of changes would be lost. Businesses needed a solution that would successfully address the following three problems:

- How to avoid duplication of equipment and resources
- How to communicate efficiently
- How to set up and manage a network.

Businesses realized that computer networking could increase productivity and save money. Networks were added and expanded almost as rapidly as new network technologies and products were introduced. The early development of networking was disorganized. However, a tremendous expansion occurred in the early 1980s. In the mid-1980s, the network technologies that emerged were created with a variety of hardware and software implementations. Each company that created network hardware and software used its company standards. These individual standards were developed because of competition with other companies. As a result, many of the network technologies were incompatible with each other. It became increasingly difficult for networks that used different specifications to communicate with each other. Network equipment often had to be replaced to implement new technologies.

Table 2-1 Summarizes the relative sizes of LANs and WANs.

Distance Between CPUs	**Location of CPUs**	**Name**
0.1m	Printed circuit board Personal data asst.	Motherboard Personal area network (PAN)
1.0m	Millimeter Mainframe	Computer system network
10m	Room	Local area network (LAN) Your classroom
100m	Building	Local area network (LAN) Your school
1000m=1km	Campus	Local area network (LAN) Stanford University

100,000m=100km	Country	Wide area network (WAN) Cisco Systems, Inc.
1,000,000m=1,000km	Continent	Wide area network (WAN) Africa
10,000,000m=10,000km	Planet	Wide area network (WAN) The Internet
100,000,000m=100,000km	Earth-moon system	Wide area network (WAN) Earth and artificial satellites

2.2 Network Devices

Equipment that connects directly to a network segment is referred to as a device. These devices are broken up into two classifications. The first classification is **End-user devices**. End-user devices include **computers**, **printers**, **scanners**, and other devices that provide services directly to the user. The second classification is **Network devices**. Network devices include all the devices that connect the end-user devices together to allow them to communicate. End-user devices that provide users with a connection to the network are also referred to as Hosts. These devices allow users to share, create, and obtain information. The host devices can exist without a network, but without the network, the host capabilities are greatly reduced Figure. (1).

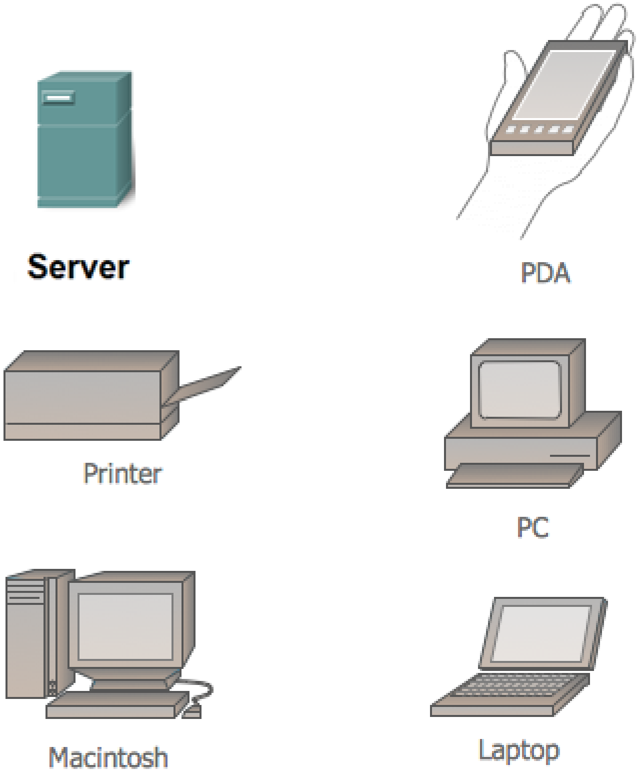


Figure 2-1 End-user Devise

2.2.1 Network Interface Card (NIC)

NIC is used to physically connect host devices to the network media. They use this connection to send e-mails, print reports, scan pictures, or access databases Figure. (2). A NIC is a printed circuit board that fits into the expansion slot of a bus on a computer motherboard. It can also be a peripheral device. NICs are sometimes called network adapters. Each NIC is identified by a unique code called a Media Access Control (MAC) address. This address is used to control data communication for the host on the network. More about the MAC address will be covered later. As the name implies, the NIC controls host access to the network.

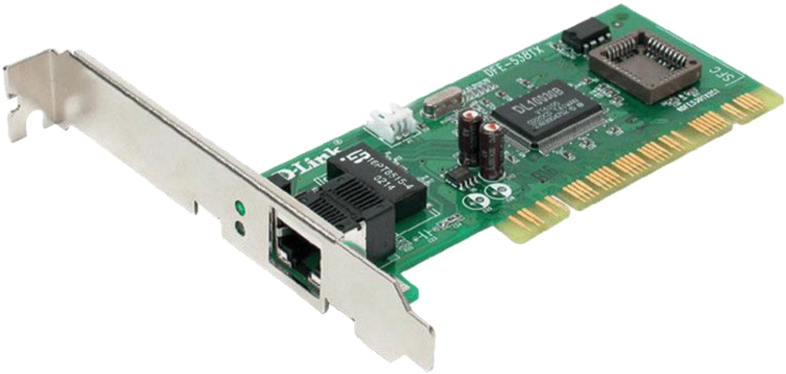


Figure 2-2 Network Interface Card (NIC)

2.2.2 Network devices

Network devices are used to extend cable connections, concentrate connections, convert data formats, and manage data transfers. Examples of devices that perform these functions are repeaters, hubs, bridges, switches, routers, and Network cloud Figure (3). All of the network devices mentioned here are covered in depth later in the course. For now, a brief overview of networking devices will be provided.

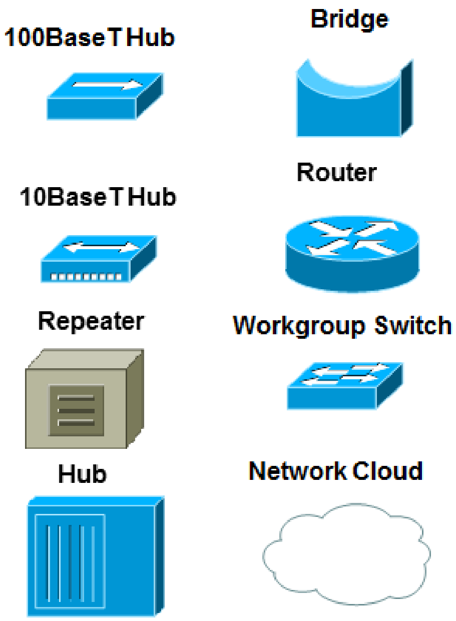


Figure 2-3 Network devices

A repeater is a network device used to regenerate a signal. Repeaters regenerate analog or digital signals that are distorted by transmission loss due to attenuation. A repeater does not make an intelligent decision concerning forwarding packets like a router or bridge Figure (4).

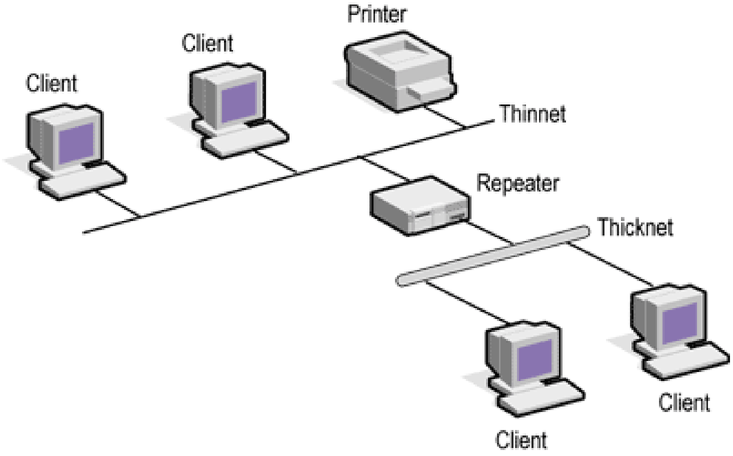


Figure 2-4 Repeater

Hubs concentrate on connections. In other words, they take a group of hosts and allow the network to see them as a single unit. This is done passively, without any other effect on the data transmission. Active hubs concentrate hosts and also regenerate signals.

Bridges convert network data formats and perform basic data transmission management. Bridges provide connections between LANs. They also check data to determine if it should cross the bridge. This makes each part of the network more efficient Figure (5).

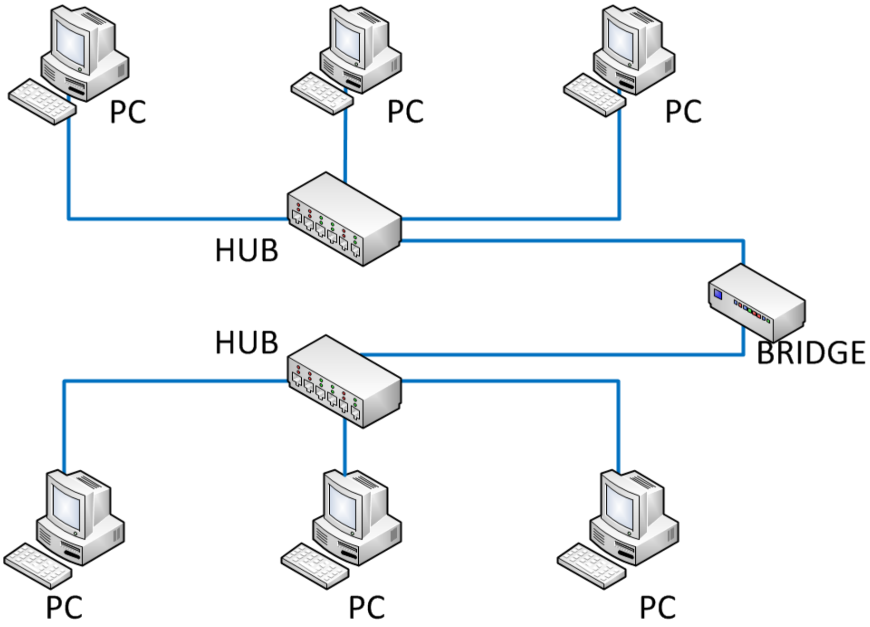


Figure 2-5 Hub and Bridge

Workgroup switches add more intelligence to data transfer management. They can determine if data should remain on a LAN and transfer data only to the connection that needs it. Another difference between a bridge and switch is that a switch does not convert data transmission formats Figure (6).

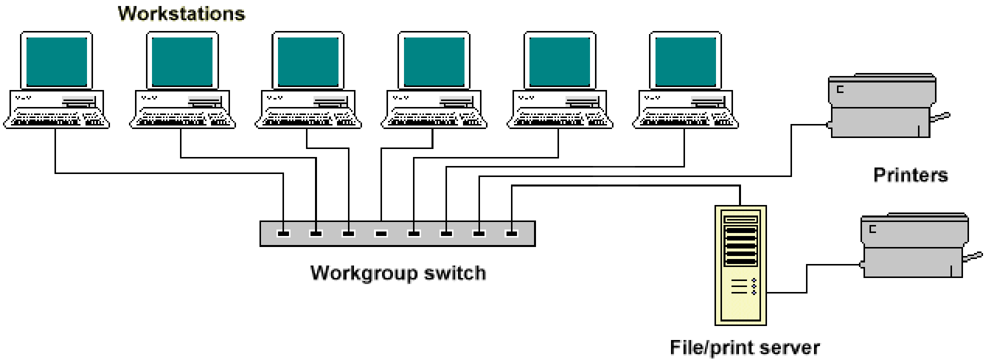


Figure 2-6 Workgroup switches

Routers have all the capabilities listed above. Routers can regenerate signals, concentrate multiple connections, convert data transmission formats, and manage data transfers. They can also connect to a WAN, which allows them to connect LANs that are separated by great distances. None of the other devices can provide this type of connection Figure (7).

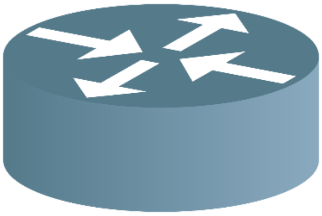


Figure 2-7 Router

2.3 Network Topology

Network topology defines the structure of the network. One part of the topology definition is the physical topology, which is the actual layout of the wire or media. The other part is the logical topology, which defines how the hosts access the media to send data. The physical topologies that are commonly used are as follows Figure (8):

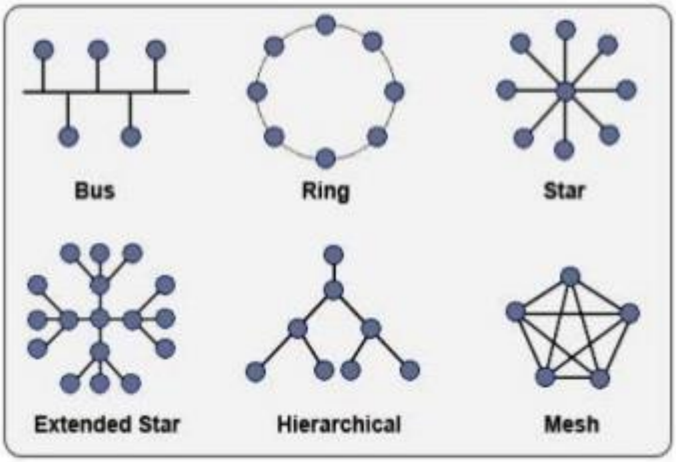


Figure 2-8 Physical topology

2.3.1 Bus topology

Bus Topology uses a single backbone cable that is terminated at both ends. All the hosts connect directly to this backbone.

Advantages:

1. There is no central controller.
2. Control resides in each station
3. The less interconnecting wire is required.
4. Ease of installation.
5. Backbone cable can be laid along the most efficient path, and then connected to the nodes by drop lines of various lengths.

Disadvantages:

1. It is possible that more than one station may attempt transmission simultaneously (collision or contention).
2. Difficult reconfiguration and fault isolation.
3. A fault or break in the bus cable stops all transmission, even between devices on the same side of the problem.
4. The damaged area reflects signals in the direction of origin, creating noise in both directions

2.3.2 Ring topology

Ring topology connects one host to the next and the last host to the first. This creates a physical ring of cable.

Advantages:

1. Avoids the collisions that are possible in the bus topology.
2. Each pair of stations has a point-to-point connection.
3. A signal is passed along the ring in one direction, from device to another, until it reaches its destination.
4. Each device incorporates a repeater.
5. Relatively easy to install and reconfigure.
6. Fault isolation is simplified.

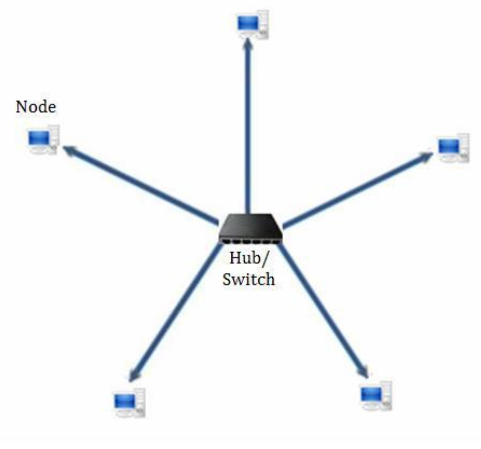
Disadvantages:

1. A break in the ring (such as station disabled) can disable the entire network.
2. Unidirectional traffic.

2.3.3 A star topology connects all cables to a central point.

Advantages:

1. Easy to install and reconfigure.
2. Robustness, if one link fails; only that link is affected. All other links remain active.
3. Easy fault identification and isolation. As long as the hub is working, it can be used to monitor link problems and bypass defective links.



Disadvantages:

1. The devices are not linked to each other.

2. If one device wants to send data to another, it sends it to the controller, which then relays the data to the other connected device.

2.3.3 An extended star

An extended star topology links individual stars together by connecting the hubs or switches.

2.3.4 A hierarchical (tree) topology

A hierarchical (tree) topology is similar to an extended star. However, instead of linking the hubs or switches together, the system is linked to a computer that controls the traffic on the topology.

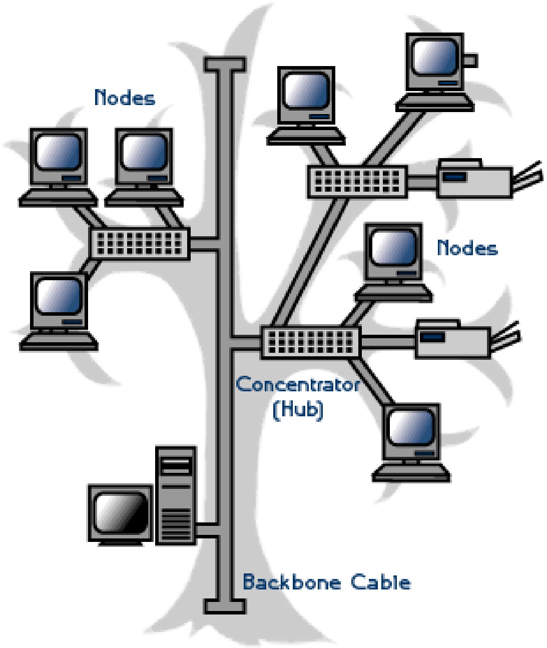


Figure 2-9 Hierarchical Topology

Advantages:

1. It allows more devices to be attached to a single central hub and can therefore increase the distance a signal can travel between devices.
2. It allows the network to isolate and prioritize communications from different computers.

Disadvantages:

1. The devices are not linked to each other.
2. If one device wants to send data to another, it sends it to the controller, which then relays the data to the other connected device.
3. The addition of secondary hubs brings two further advantages.

2.3.5 Mesh

Mesh topology is implemented to provide as much protection as possible from interruption of service. For example, a nuclear power plant might use a mesh topology in the networked control systems. As seen in the graphic, each host has its connections to all other hosts. Although the Internet has multiple paths to any one location, it does not adopt the full mesh topology.

Advantages:

1. The use of dedicated (link carries traffic only between the two devices it connects) links guarantees that each connection can carry its data load, thus eliminating the traffic problems that can occur when links must be shared by multiple devices.
2. It is robust, if one link becomes unusable, it does not incapacitate (affect) the entire system.

3. Privacy and Security (every message sent travels along a dedicated line; only the intended recipient sees it).
4. Point-to-point links make fault identification and fault isolation easy.

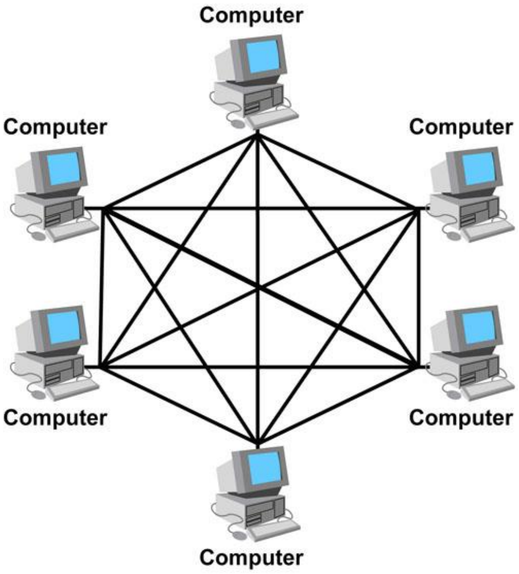


Figure 2-10 Mesh Topology

Disadvantages:

1. A large amount of cabling required.
2. A large amount of I/O ports required.
3. Installation and reconfiguration are difficult.
4. The sheer bulk of the wiring can be greater than the available space (in the walls, ceiling, or floors) can accommodate.
5. The hardware required to connect each link (I/O ports and cables) can be prohibitively expensive.

The logical topology of a network determines how the hosts communicate across the medium. The two most common types of logical topologies are **broadcast** and **token passing**.

The use of a **Broadcast topology** indicates that each host sends its data to all other hosts on the network medium. There is no order that the stations must follow to use the network. It is first-come, first-serve. Ethernet works this way as will be explained later in the course.

The second logical topology is **Token passing**. In this type of topology, an electronic token is passed sequentially to each host. When a host receives the token, that host can send data on the network. If the host has no data to send, it passes the token to the next host and the process repeats itself. Two examples of networks that use token passing are Token Ring and Fiber Distributed Data Interface (FDDI). The diagram in Figure (9) shows many different topologies connected by network devices (**Hybrid topologies**). It shows a network of moderate complexity that is typical of a school or a small business. The diagram includes many symbols and networking concepts that will take time to learn.

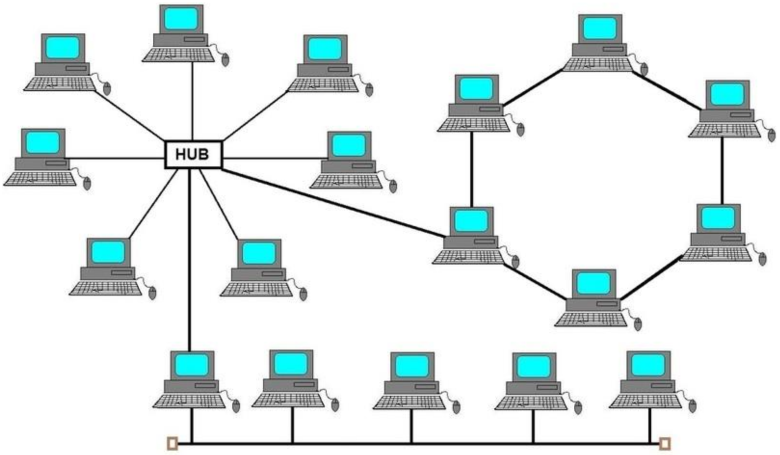


Figure 2-11 Different Topologies Connected by Network Devices

2.4 Local Area Network (LAN)

A local area network (LAN) is a group of computers and network communication devices interconnected within a geographically limited area, such as a building or campus. A LAN tends to use only one type of transmission medium—cabling. LANs allow businesses to locally share computer files and printers efficiently and make internal communications possible. A good example of this technology is email. LANs manage data, local communications, and computing equipment. LANs are characterized by the following:

- They transfer data at high speeds.
- They exist in a limited geographical area.
- Their technology is generally less expensive.

LANs consist of the following components:

- Computers
- Network interface cards
- Peripheral devices
- Networking media
- Network devices

Some common LAN technologies include the following:

- Ethernet
- Token Ring
- FDDI

2.5 Wide Area Network (WAN)

A wide area network (WAN) interconnects LANs. A WAN may be located entirely within a state or country, or it may be interconnected around the world, which then provides access to computers or file servers in other locations. Because WANs connect user networks over a large geographical area, they make it possible for businesses to communicate across great distances. WANs allow computers, printers, and other devices on a LAN to be shared with distant locations. WANs are characterized by the following:

- They exist in an unlimited geographical area.
- They are more sophisticated and complex than LANs.
- Provide e-mail, Internet, file transfer, and e-commerce services.
- Their technology is expensive.

Some common WAN technologies include the following:

- Modems.
- Integrated Services Digital Network (ISDN).
- Digital subscriber line (DSL).
- Frame Relay.
- T1, E1, T3, and E3
- Synchronous Optical Network (SONET).

2.6 Metropolitan-area networks (MAN)

Metropolitan-area networks (MAN) usually consists of two or more LANs in a common geographic area. For example, a bank with multiple branches may utilize a MAN. Typically, a service provider is used to connect two or more LAN sites using private communication lines or optical services. A MAN can also be created using wireless bridge technology by beaming signals across public areas Figure (10).

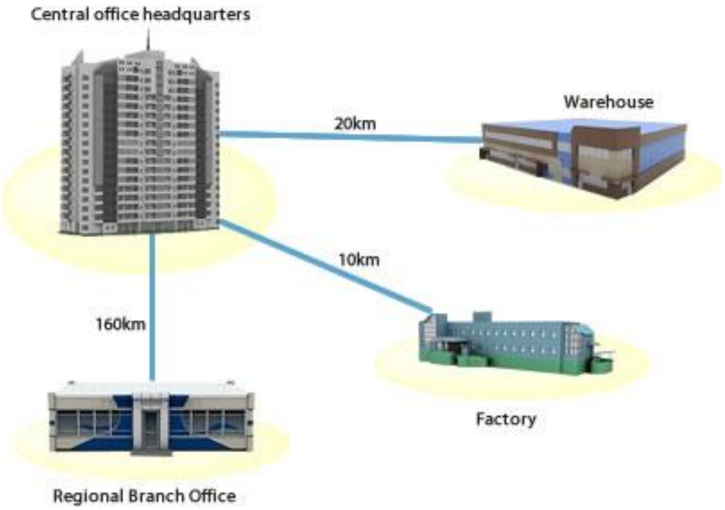


Figure 2-12 Metropolitan-area networks (MAN)

2.6 Storage-area networks (SAN)

A storage-area network (SAN) is a dedicated, high-performance network used to move data between servers and storage resources. Because it is a separate, dedicated network, it avoids any traffic conflict between clients and servers. SAN technology allows high-speed server-to-storage, storage-to-storage, or server-to-server connectivity. This method uses a separate network infrastructure that relieves any problems associated with existing network connectivity Figure (11). SANs offer the following features:

- **Performance**: SANs allow concurrent access of disk or tape arrays by two or more servers at high speeds. This provides enhanced system performance.

- **Availability**: SANs Data can be duplicated on a SAN up to 10 km (6.2 miles) away. **Scalability**: A SAN can use a variety of technologies.

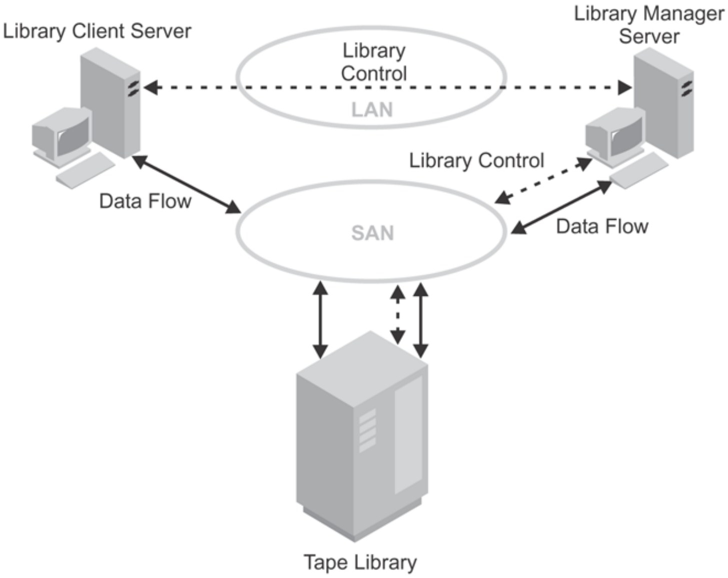


Figure 2-13 Storage-area networks (SAN)

2.7 Virtual Private Network (VPN)

A virtual private network (VPN) is a private network that is constructed within a public network infrastructure such as the global Internet. Using a VPN, a telecommuter can remotely access the network of the company headquarters. Through the Internet, a secure tunnel can be built between the PC of the telecommuter and a VPN router at the company headquarters Figure (12).

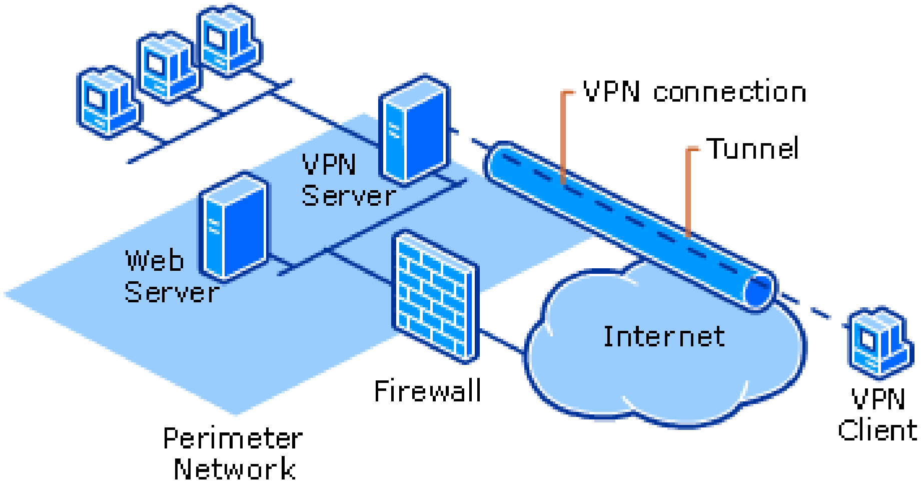


Figure 2-14 Virtual Private Network (VPN)

2.8 Intranets and Extranets

One common configuration of a LAN is an intranet. Intranet Web servers differ from public Web servers in that the public must have the proper permissions and passwords to access the intranet of an organization. Intranets are designed to permit users who have access privileges to the internal LAN of the organization. Within an intranet, Web servers are installed in the network. Browser technology is used as the common front end to access information on servers such as financial, graphical, or text-based data. Extranets refer to applications and services that are Intranet-based and use extended, secure access to external users or enterprises. This access is usually accomplished through passwords, user IDs, and other application-level security. An extranet is the extension of two or more intranet strategies with a secure interaction between participant enterprises and their respective intranets.

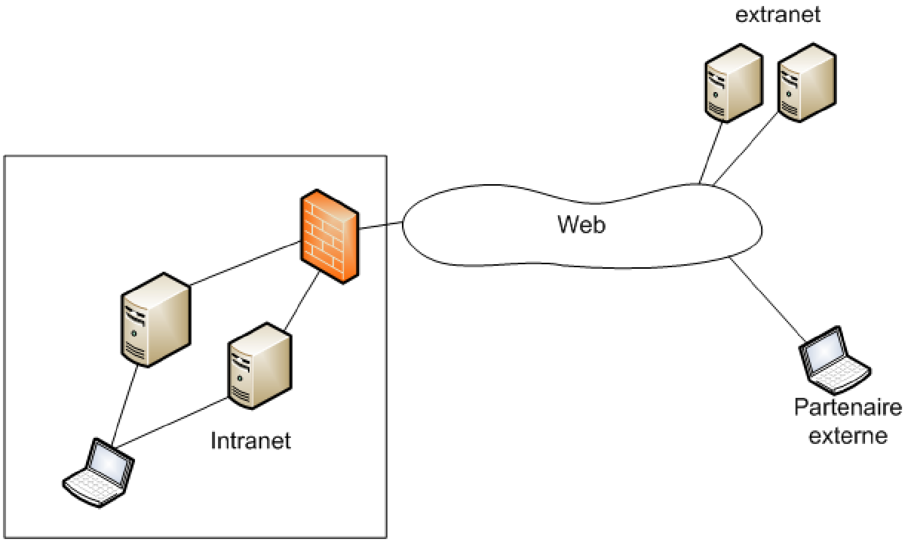


Figure 2-15 Intranets and Extranet

2.9 Network Interconnection

When LAN and WAN technologies are used, many computers are interconnected to provide services to their users. To accomplish this, networked computers take on different roles or functions in relation to each other. Some types of applications require computers to function as equal partners. Other types of applications distribute their work so that one computer functions to serve several others in an unequal relationship. Two computers generally use request and response protocols to communicate with each other. One computer issues a request for a service, and a second computer receives and responds to that request. The requestor acts like a client and the responder acts like a server.

2.9.1 Peer-to-Peer Network

In a peer-to-peer network, networked computers act as equal partners, or peers. As peers, each computer can take on the client's function or the server function. Computer A may request a file from Computer B, which then sends the file to Computer A. Computer A acts as the client, and Computer B acts as the server. At a later time, Computers A and B can reverse roles. In a peer-to-peer network, individual users control their resources. The users may decide to share certain files with other users. Peer-to-peer networks are relatively easy to install and operate. No additional equipment is necessary beyond a suitable operating system installed on each computer. Since users control their resources, no dedicated administrators are needed. As networks grow, peer-to-peer relationships become increasingly difficult to coordinate. A peer-to-peer network works well with ten or fewer computers. Since peer-to-peer networks do not scale well, their efficiency decreases rapidly as the number of computers on the network increases. Also, individual users control access to the resources on their computers, which means security may be difficult to maintain. The client/server model of networking can be used to overcome the limitations of the peer-to-peer network.

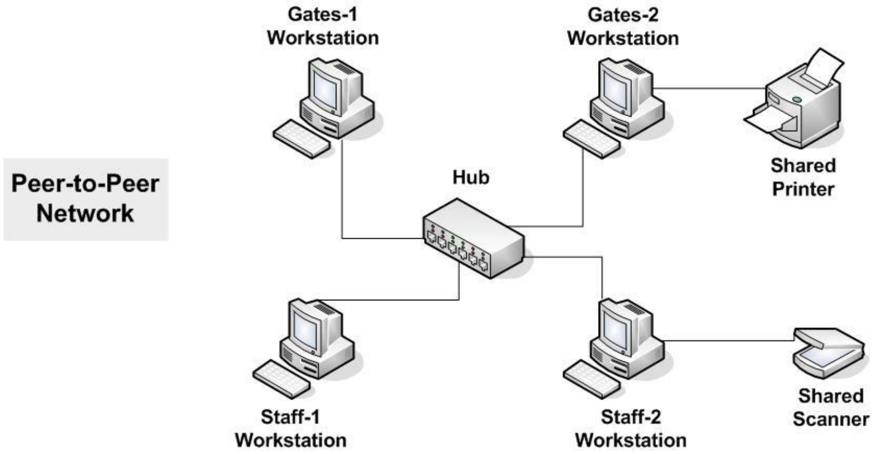


Figure 2-16 Peer-to-Peer Network

2.9.2 Client/Server

In a client/server arrangement, network services are located on a dedicated computer called a server. The server responds to the requests of clients. The server is a central computer that is continuously available to respond to requests from clients for file, print, application, and other services. Most network operating systems adopt the form of a client/server relationship. Typically, desktop computers function as clients, and one or more computers with additional processing power, memory, and specialized software function as servers. Servers are designed to handle requests from many clients simultaneously. Before a client can access the server resources, the client must be identified and be authorized to use the resource. Each client is assigned an account name and password that is verified by an authentication service. The authentication service guards access to the network. With the centralization of user accounts, security, and access control, server-based networks simplify the administration of large networks. The concentration of network resources such as files, printers, and applications on servers also makes it easier to back-up and maintain the data. Resources can be located on specialized, dedicated servers for easier access. Most client/server systems also include ways to enhance the network with new services that extend the usefulness of the network. The centralized functions in a client/server network have substantial advantages and some disadvantages. Though a centralized server enhances security, ease of access, and control, it introduces a single point of failure into the network. Without an operational server, the network cannot function at all. Servers require a trained, expert staff member to administer and maintain. Server systems also require additional hardware and specialized software that added to the cost.

Advantages of a Peer-to-Peer Network	Advantages of a Client/Server Network
Less expensive to implement.	Provides for better security.
Does not require additional specialized network administration software.	Easier to administer when the network is large because the administration is centralized.
Does not require a dedicated network administrator.	All data can be backed up on one central location.

Disadvantages of a Peer-to-Peer Network	Disadvantages of a Client/Server Network
Does not scale well to large networks and administration becomes unmanageable.	Requires expensive specialized network administrative and operational software.
Each user must be trained to perform administrative tasks.	Requires expensive, more powerful hardware for the server machine.
Less secure.	Requires a professional administrator.
All machines sharing the resources negatively impact the performance.	Has a single point failure. User data is unavailable if the server is down.

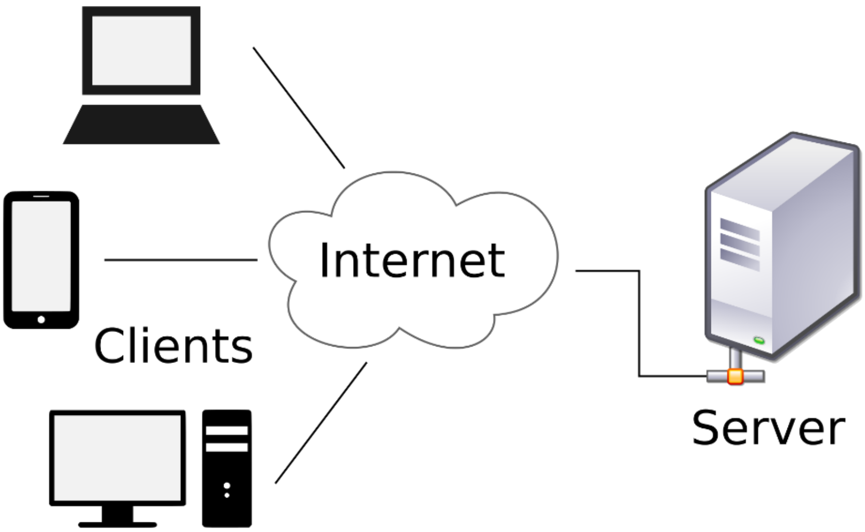


Figure 2-17 Client/Server Network

2.10 Exercise

1. Which of the following are propositions?
2. What are the problems that Businesses needed a solution for?
3. Give an example of a Network device?
4. List advantage of Ring topology and disadvantage of A star topology
5. What are the differences of :

   a) Bridge and router

   b) Bus and ring topology

   c) LAN and WAN

   d) Peer to peer and client-server

6. A cable break in a _______ topology stops all transmission.

   a) mesh

   b) star

   c) primary

   d) bus

7. The term used to describe the physical layout of a network?

   a) protocol

   b) server

   c) topology

   d) schema

CHAPTER 3

Network Media

3.1 Introduction

The **Network Media** is the device that physically carries the data from computer to computer. The three major types of network media are:

- Copper Cable
- Fiber-Optic Cable
- Wireless

Each computer network can be built with many different media types. The **function of the media** is to carry a flow of information through a LAN. Wireless LANs use the atmosphere, or space, as the medium. Other networking media confine network signals to a wire, cable, or fiber.

Each type of media has advantages and disadvantages. These are based on the following factors:

1. Cable Length
2. Cost
3. Ease of Installation
4. Susceptibility to Interference

3.2 Copper Cable

Copper cable is the most common type of network media used today. The data is carried over the copper cable in the form of electrical signals from the computer to the computer. The **disadvantage** of sending data over copper wire is that the **further the signal travels, the weaker it becomes**. Copper is, however, **the easiest, quickest, and cheapest form of network media to install.**

Figure 3-1 Copper Cable

3.2.1 Cable Specification

Copper cables have different specifications and expectations. Important considerations related to performance are as follows:

- What speeds for data transmission can be achieved? The speed of bit transmission through the cable is extremely important.

The speed of transmission is affected by the kind of conduit used.

- Will the transmissions be digital or analog? Digital or baseband transmission and analog or broadband transmission require different types of cable.
- How far can a signal travel before attenuation becomes a concern? If the signal is degraded, network devices might not be able to receive and interpret the signal. The distance the signal travels through the cable affects the attenuation of the signal. Degradation is directly related to the distance the signal travels and the type of cable used.

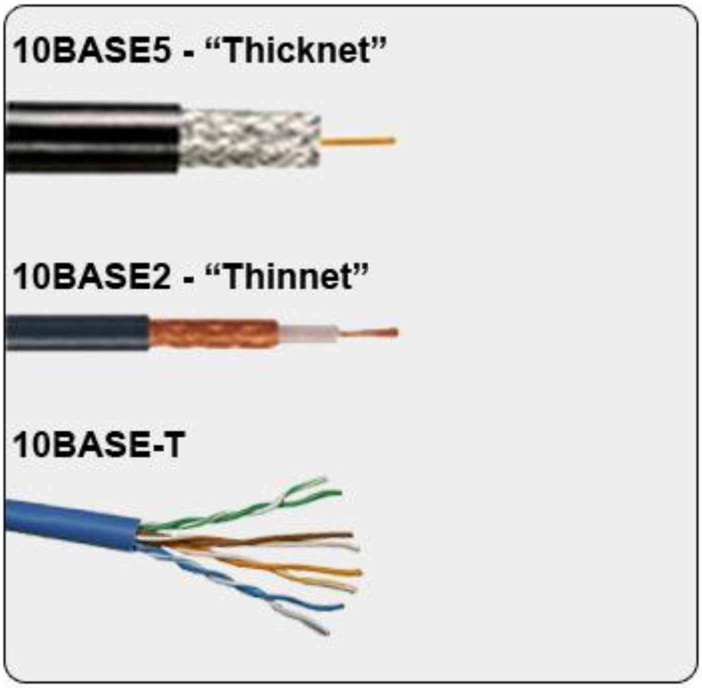


Figure 3-2 Copper Cable Type

The following Ethernet specifications relate to cable type:

- 10BASE-T

- 10BASE5
- 10BASE2

10BASE-T refers to the speed of transmission at 10Mbps. The type of transmission is baseband, or digitally interpreted. The T stands for twisted pair.

10BASE5 refers to the speed of transmission at 10 Mbps. The type of transmission is baseband, or digitally interpreted. The 5 indicates that a signal can travel for approximately 500 meters before attenuation could disrupt the ability of the receiver to interpret the signal. 10BASE5 is often referred to as **Thicknet**.

10BASE2 refers to the speed of transmission at 10 Mbps. The type of transmission is baseband, or digitally interpreted. The 2, in 10BASE2, refers to the approximate maximum segment length being 200 meters before attenuation could disrupt the ability of the receiver to appropriately interpret the signal being received. The maximum segment length is 185 meters. 10BASE2 is often referred to as **Thinnet**.

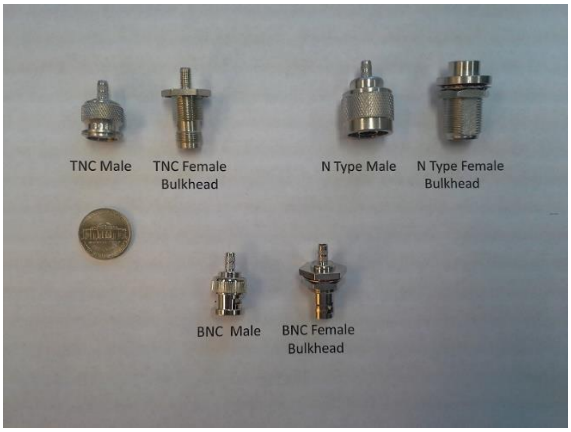


Figure 3-3 Copper Cable Connector

3.2.2 Coaxial Cables

Coaxial Cable consists of a copper conductor surrounded by a layer of flexible insulation. The center conductor can also be made of tin-plated aluminum cable allowing for the cable to be manufactured inexpensively. Over this insulating material is a woven copper braid or metallic foil that acts as the second wire in the circuit and as a shield for the inner conductor. This second layer or shield also reduces the amount of outside electromagnetic interference. Covering this shield is the cable jacket. For LANs, the coaxial cable offers **several advantages**. **It can be run longer distances than shielded twisted pair, STP, unshielded twisted pair, UTP, and screened twisted pair, SCTP, cable without the need for repeaters**. Coaxial cable is less **expensive than fiber-optic cable and the technology is well known**. It has been used for many years for many types of data communication such as cable television.

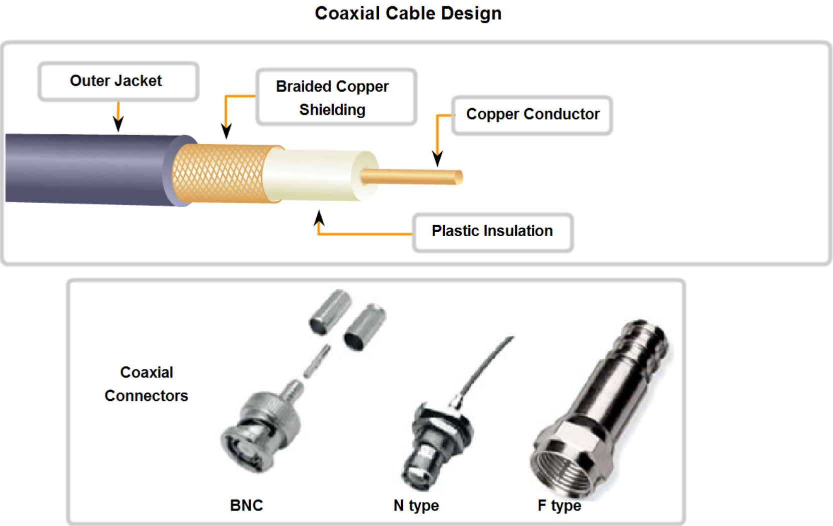


Figure 3-4 Coaxial Cables

- Speed and throughput: 10-100Mbps
- Cost: Inexpensive
- Media and connector size: Medium
- Maximum cable length: 500m

3.2.3 STP Cable

In **Shielded Twisted Pair** STP each pair of wires is wrapped in a metallic foil. The two pairs of wires are wrapped in an overall metallic braid or foil. It is usually a 150-ohm cable. As specified for use in Token Ring network installations, STP reduces electrical noise within the cable such as pair to pair coupling and crosstalk. STP also reduces electronic noise from outside the cable such as electromagnetic interference (EMI) and radio frequency interference (RFI). STP cable shares many of the advantages and disadvantages of UTP cable. STP provides more protection from all types of external interference. However, STP is more expensive and difficult to install than UTP.

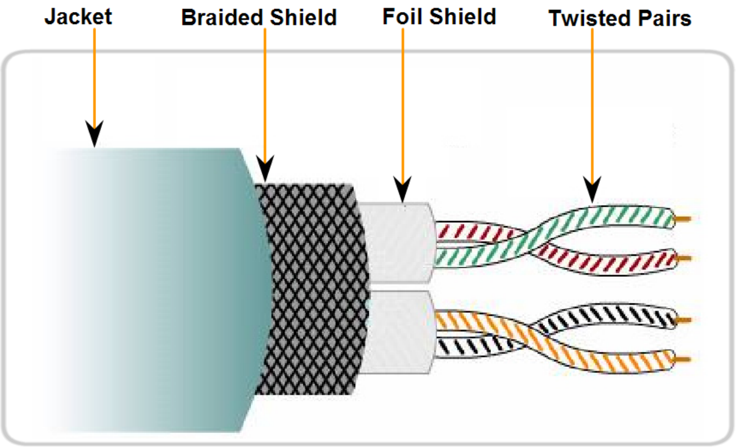


Figure 3-5 Shielded Twisted Pair

- Speed and throughput: 0-100Mbps
- Cost: Moderate
- Media and connector size: Medium to large
- Maximum cable length: 100m

3.2.4 Screened UTP (SCTP)

A new hybrid of UTP is Screened UTP (SCTP), which is also known as a foil screened twisted pair (FTP). SCTP is essentially UTP wrapped in a metallic foil shield or screen. SCTP, like UTP, is also a 100-ohm cable. Many cable installers and manufacturers may use the term STP to describe SCTP cabling. It is important to understand that most references made to STP today refer to Four-Pair Shielded Cabling. It is highly unlikely that true STP cable will be used during a cable installation job.

The shield prevents incoming electromagnetic waves from causing noise on data wires, and it also minimizes the outgoing radiated electromagnetic waves. These waves could cause noise in other devices. STP and SCTP cable cannot be run as far as other networking media, such as coaxial cable or optical fiber, without the signal being repeated. More insulation and shielding combine to considerably increase the size, weight, and cost of the cable.

- Speed and throughput: 0-100Mbps
- Cost: Moderately Expensive
- Media and connector size: Medium to large
- Maximum cable length: 100m

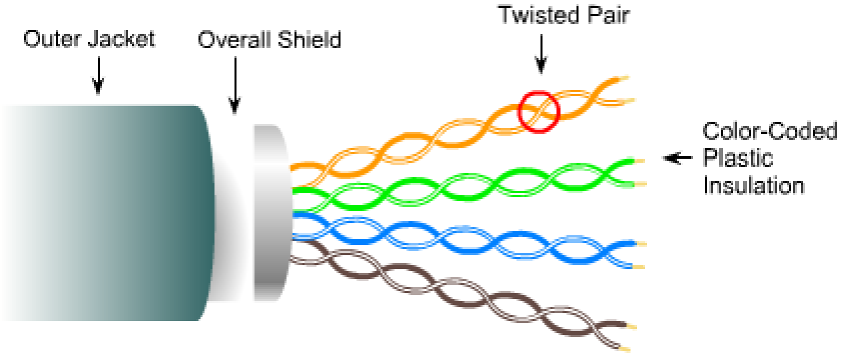


Figure 3-6 Screened UTP

3.2.5 UTP Cable Unshielded Twisted Pair

UTP is a four-pair wire medium used in a variety of networks. Each of the eight copper wires in the UTP cable is covered by insulating material. In addition, each pair of wires is twisted around each other. This type of cable relies on the cancellation effect produced by the twisted wire pairs to limit signal degradation caused by EMI and RFI. To further reduce crosstalk between the pairs in UTP cable, the number of twists in the wire pairs varies. Like STP cable, UTP cable must follow precise specifications as to how many twists or braids are permitted per foot of cable.

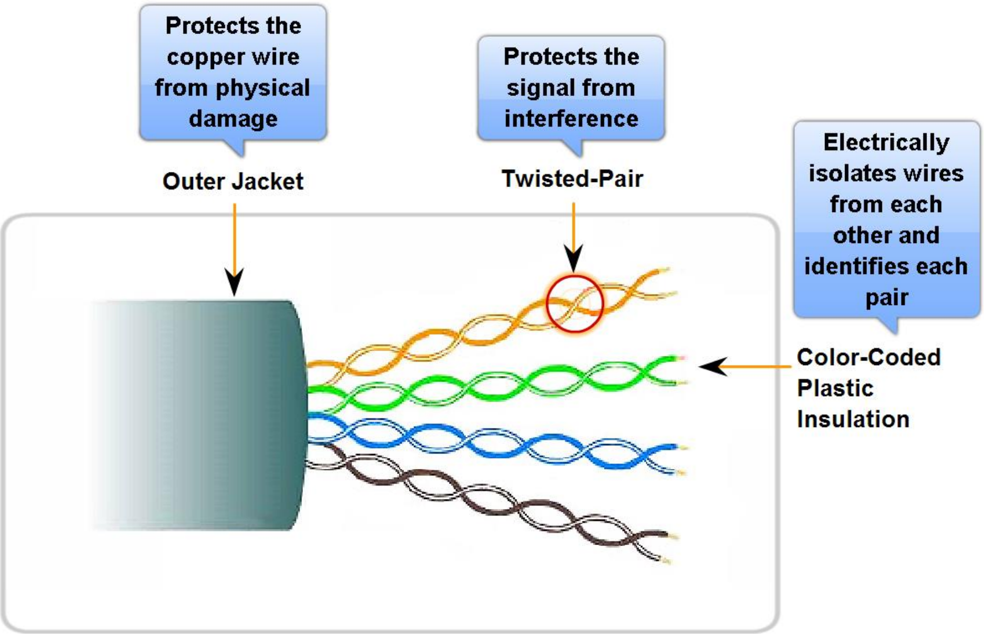

Protects the copper wire from physical damage
Outer Jacket
Protects the signal from interference
Twisted-Pair
Electrically isolates wires from each other and identifies each pair
Color-Coded Plastic Insulation

Figure 3-7 Unshielded Twisted Pair (UTP) Cable

- Speed and throughput: 10-100-1000Mbps*
- Cost: Least Expensive
- Media and connector size: Small
- Maximum cable length: 100m * (Depending on the quality/category of cable)

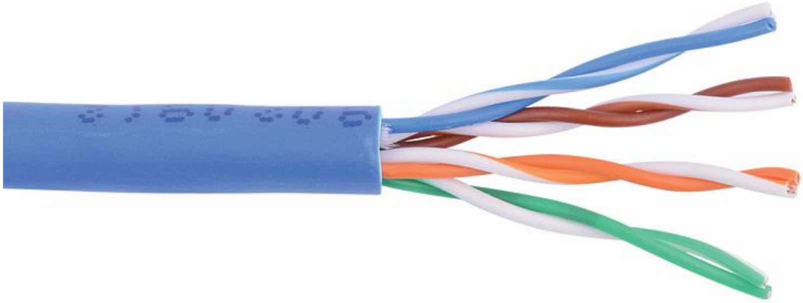


Figure 3-8 UTP example

UTP cable has many advantages. It is easy to install and is less expensive than other types of networking media. UTP costs less per meter than any other type of LAN cabling.

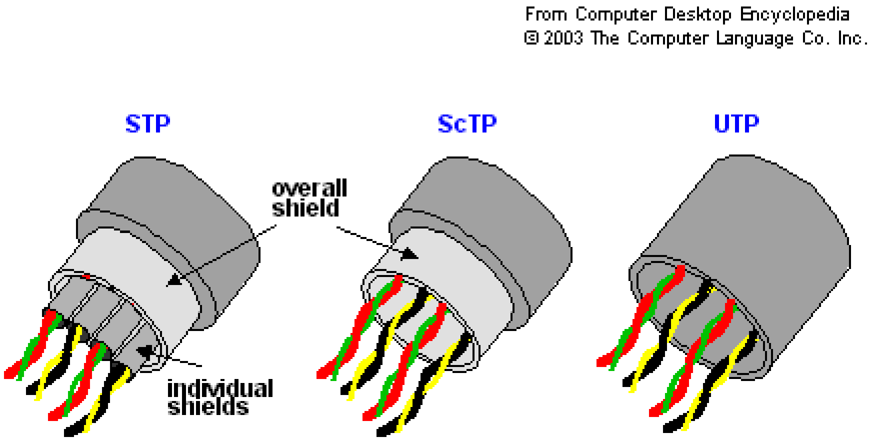

From Computer Desktop Encyclopedia
© 2003 The Computer Language Co. Inc.
STP
ScTP
UTP
overall shield
individual shields

Figure 3-9 Deference between STP, ScTP, and UTP

3.2.6 UTP Implementation

EIA/TIA specifies an RJ-45 connector for UTP cable. The letters RJ stand for registered jack and the number 45 refers to a specific wiring sequence. The RJ-45 transparent end connector shows eight colored wires. Four of the wires, T1 through T4, carry the voltage and are called the tip. The other four wires, R1 through R4, are grounded and are called a ring. Tip and ring are terms that originated in the early days of the telephone. Today, these terms refer to the positive and the negative wire in a pair. The wires in the first pair in a cable or a connector are designated as T1 and R1. The second pair is T2 and R2, the third is T3 and R3, and the fourth is T4 and R4. The RJ-45 connector is the male component, which is crimped on the end of the cable. When a male connector is viewed from the front, the pin locations are numbered from 8 on the left to 1 on the right as seen in the following figure.

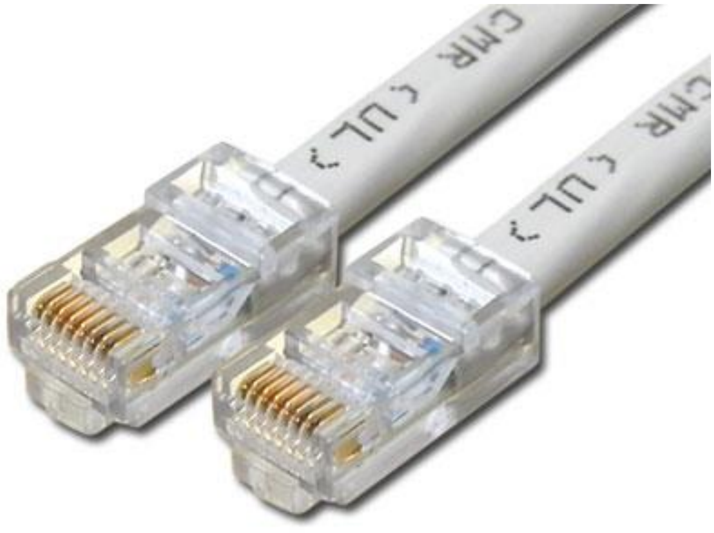


Figure 3-10 RJ-45

The jack is the female component in a network device, wall outlet, or patch panel as seen in the following figure.

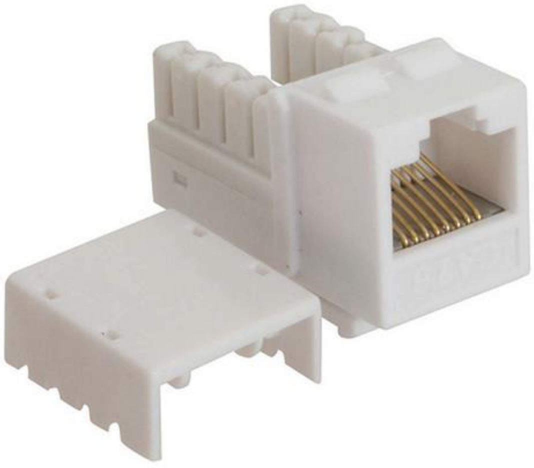


Figure 3-11 RJ45 Termination Cap

For electricity to run between the connector and the jack, the order of the wires must follow the **T568A** or **T568B** color code found in the EIA/TIA-568-B.1 standard, as shown in Figure.

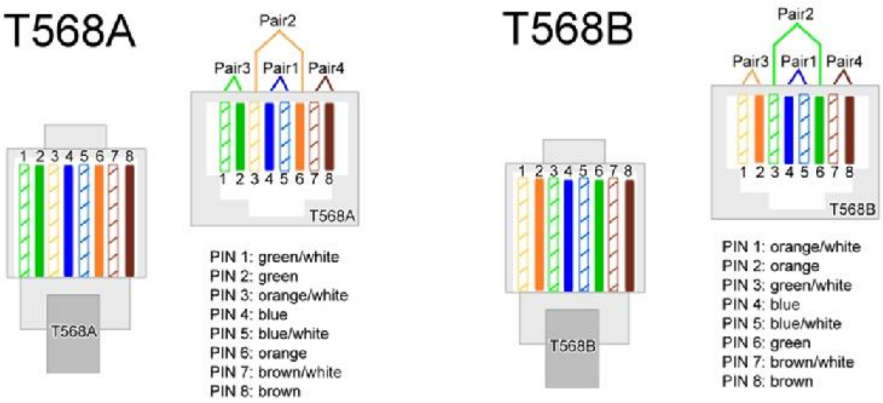


Figure 3-12 EIA/TIA-568-B.1 standard

If the two RJ-45 connectors of a cable are held side by side in the same orientation, the colored wires will be seen in each. If the order of the colored wires is the same at each end, then the cable is a Straight-Through, as seen in the next figure.

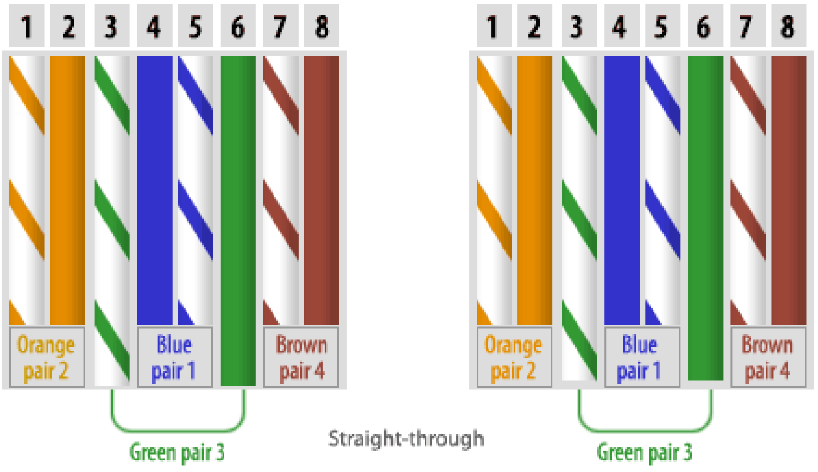


Figure 3-13 Straight Cable

In a Crossover Cable, the RJ-45 connectors on both ends show that some of the wires are connected to different pins on each side of the cable. The following figure shows that pins 1 and 2 on one connector connect to pins 3 and 6 on the other.

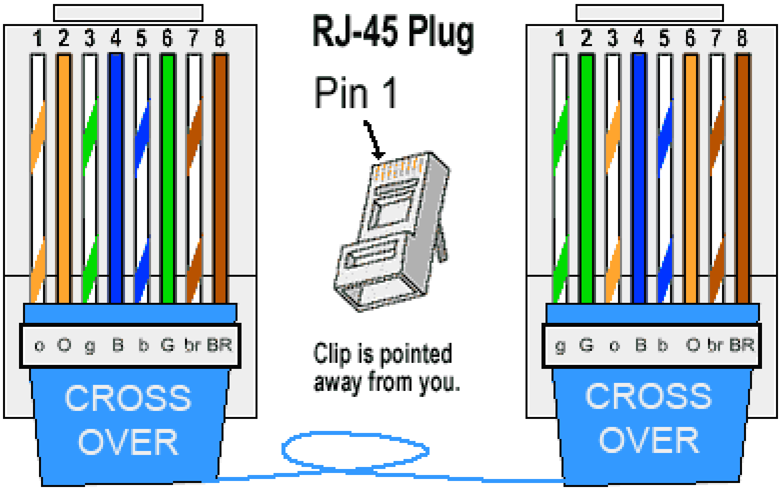


Figure 3-14 Crossover Cable

Use straight-through cables for the following connections:

- Switch to Router
- Switch to PC or Server
- Hub to PC or Server

Use crossover cables for the following connections:

The next figure illustrates how a variety of cable types may be required in a given network. The category of UTP cable required is based on the type of Ethernet that is chosen.

- Switch to Switch
- Switch to Hub

- Hub to Hub
- Router to Router
- PC to PC
- Router to PC

Twisting provide:

1- protection against crosstalk, noise generated by adjacent pairs &

2- cancellation of the magnetic field.

Based on the connection layout, 3 types of UTP have existed:

Straight UTP Cable

Side1:	WO	O	WG	B	WB	G	WBr	Br
Side2:	WO	O	WG	B	WB	G	WBr	Br

Cross-Over UTP Cable

Side1:	WO	O	WG	B	WB	G	WBr	Br
Side2:	WG	G	WO	B	WB	O	WBr	Br

Roll-Over UTP Cable (Console UTP Cable)

Side1:	WO	O	WG	B	WB	G	WBr	Br
Side2:	Br	WBr	G	WB	B	WG	O	WO

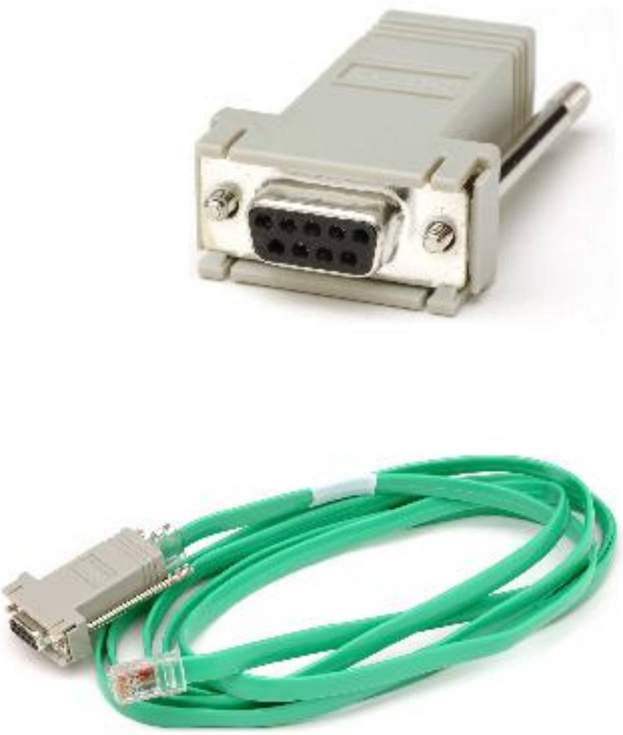


Figure 3-15 Console Cable

Types of Cable

- UTP & STP (CAT 5 & 6)
- Coax
- Fiber

UTP Cables

- Straight for different devices
- Cross Over for similar devices
- Roll Over for configuration of routers

Connectors

- BNC : Coax
- RJ-45 : UTP & STP
- RJ-11: Phone, VSAT
- Type F: Fiber

3.3 Fiber-Optic

Fiber-Optic cable uses glass strands to transmit data at the speed of light. The data is carried over these glass strands in the form of light beams. These beams of light can carry signals a much greater distance at a much higher speed than copper cable. These signals are not as subject to degradation or electronic interference as is the case with copper.

The part of an optical fiber through which light rays travel is called the core of the fiber. Light rays can only enter the core if their angle is inside the numerical aperture of the fiber. Likewise, once the rays have entered the core of the fiber, there are a limited number of optical paths that a light ray can follow through the fiber. These optical paths are called modes. If the diameter of the core of the fiber is large enough so that there are many paths that light can take through the fiber, the fiber is called "multimode" fiber. Single-mode fiber has a much smaller core that only allows light rays to travel along with one mode inside the fiber.

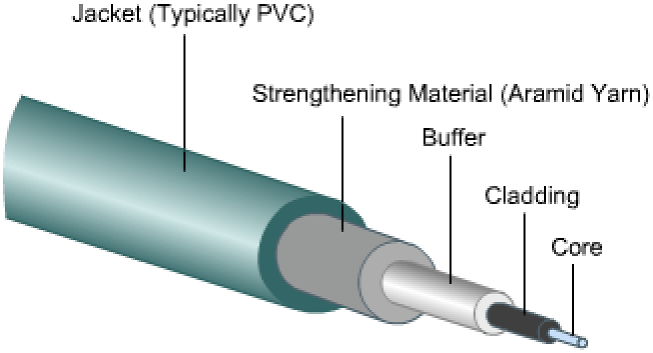


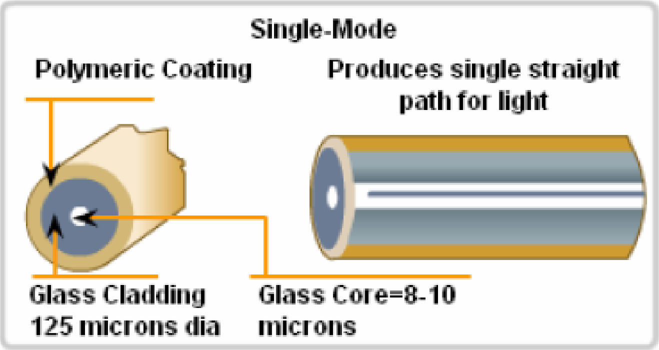
Figure 3-16 Fiber-Optic

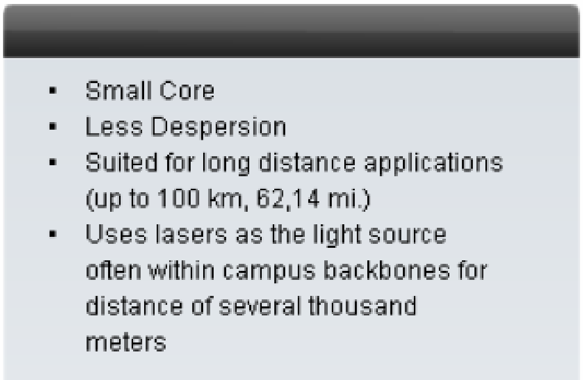
Every fiber-optic cable used for networking consists of two glass fibers encased in separate sheaths. One fiber carries transmitted data from device A to device B. The second fiber carries data from device B to device A. The fibers are similar to two one-way streets going in opposite directions. This provides a full-duplex communication link. Copper twisted-pair uses a wire pair to transmit and a wire pair to receive. Fiber-optic circuits use one fiber strand to transmit and one to receive. Typically, these two fiber cables will be in a single outer jacket until they reach the point at which connectors are attached.

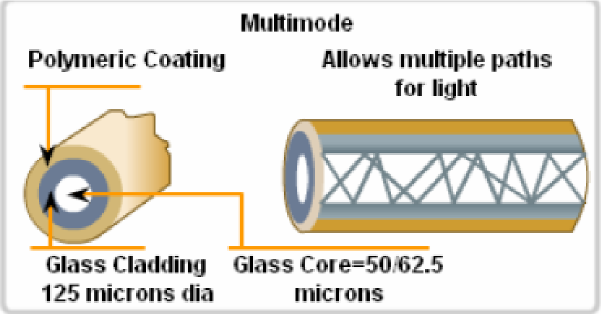
Until the connectors are attached, there is no need for shielding, because no light escapes when it is inside a fiber. This means there are no crosstalk issues with fiber. It is very common to see multiple fiber pairs encased in the same cable. This allows a single cable to be run between data closets, floors, or buildings. One cable can contain 2 to 48 or more separate fibers. With copper, one UTP cable would have to be pulled for each circuit. Fiber can carry many more bits per second and carry them farther than copper can.

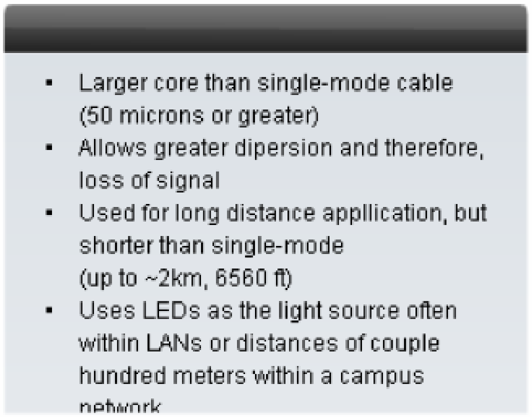
3.3.1 Single-Mode and Multi-Mode

Fiber Single-mode fiber consists of the same parts as multimode. The outer jacket of single-mode fiber is usually yellow. The major difference between multimode and single-mode fiber is that single-mode **allows only one mode of light to propagate through the smaller, fiber-optic core**. The single-mode core is eight to ten microns in diameter. Nine-micron cores are the most common. A 9/125 marking on the jacket of the single-mode fiber indicates that the core fiber has a diameter of 9 microns and the surrounding cladding is 125 microns in diameter. An infrared laser is used as the light source in single-mode fiber. The ray of light it generates enters the core at a 90-degree angle. As a result, the data-carrying light ray pulses in single-mode fiber are essentially transmitted in a straight line right down the middle of the core. This greatly increases both the speed and the distance that data can be transmitted. Because of its design, single-mode fiber is capable of higher rates of data transmission (bandwidth) and greater cable run distances than multimode fiber. Single-mode fiber can carry LAN data up to 3000 meters. Although this distance is considered a standard, newer technologies have increased this distance and will be discussed in a later module. Multimode is only capable of carrying up to 2000 meters. Lasers and single-mode fibers are more expensive than LEDs and multimode fiber. Because of these characteristics, single-mode fiber is often used for inter-building connectivity.


Single-Mode
Polymeric Coating
Produces single straight path for light
Glass Cladding 125 microns dia
Glass Core=8-10 microns


- Small Core
- Less Despersion
- Suited for long distance applications (up to 100 km, 62,14 mi.)
- Uses lasers as the light source often within campus backbones for distance of several thousand meters


Multimode
Polymeric Coating
Allows multiple paths for light
Glass Cladding 125 microns dia
Glass Core=50/62.5 microns


- Larger core than single-mode cable (50 microns or greater)
- Allows greater dipersion and therefore, loss of signal
- Used for long distance appllication, but shorter than single-mode (up to ~2km, 6560 ft)
- Uses LEDs as the light source often within LANs or distances of couple hundred meters within a campus network

3.3.2 Other Optical Components

Connectors are attached to the fiber ends so that the fibers can be connected to the ports on the transmitter and receiver. The type of connector most commonly used with multimode fiber is the Subscriber Connector (SC). On single-mode fiber, the Straight Tip (ST) connector is frequently used.

In addition to the transmitters, receivers, connectors, and fibers that are always required on an optical network, repeaters and fiber patch panels are often seen. Repeaters are optical amplifiers that receive attenuating light pulses traveling long distances and restore them to their original shapes, strengths, and timings. The restored signals can then be sent on along the journey to the receiver at the far end of the fiber. Fiber patch panels similar to the patch panels used with copper cable. These panels increase the flexibility of an optical network by allowing quick changes to the connection of devices like switches or routers with various available fiber runs, or cable links.

3.4 Wireless Media

The extraordinary convenience of wireless communications has placed an increased emphasis on wireless networks in recent years. Technology is expanding rapidly and will continue to expand into the near future, offering more and better options for wireless networks. Presently, you can subdivide wireless networking technology into three basic types corresponding to three basic networking scenarios:

- Local Area Networks (LANs). Occasionally, you will see a fully wireless LAN, but more typically, one or more wireless machines will function as members of a cable-based LAN. A LAN with both wireless and cable-based components is called a hybrid.

- Extended Local Networks. A wireless connection serves as a backbone between two LANs. For instance, a company with office networks in two nearby but separate buildings could connect those networks using a wireless bridge.
- Mobile Computing. A mobile machine connects to the home network using cellular or satellite technology. The main advantage that wireless networks have over copper and fiber optic is that you don't have to run and connect cables to the computers.

The three major types of wireless networks today are:

- Infrared (IR)
- Microwave
- Radio Frequency (RF)

3.5 Exercise

1- List properties of (UTP, SCTP, Coaxial Cables, Single-Mode fiber optic)

2- Explain Screened UTP (SCTP):

3- Show the T568B color code found in the EIA/TIA-568-B.1 standard.

4- Explain one type of copper cable

5- List properties of (UTP, SCTP, Coaxial Cables, Single-Mode fiber optic).

CHAPTER 4

Network Models and Layers

4.1 Introduction

The information that travels on a network is generally referred to as data or a packet. A packet is a logically grouped unit of information that moves between computer systems. The network models are describing this movement of the packets. The OSI and TCP/IP models have layers that explain how data is communicated from one computer to another. The models differ in the number and function of the layers. However, each model can be used to help describe and provide details about the flow of information from a source to a destination.

4.2 Using layers to describe data communication

For traveling data packets from a source to a destination on a network, it is important that all the devices on the network speak the same language or protocol. A protocol is a set of rules that make communication on a network more efficient. For example, while flying an airplane, pilots obey very specific rules for communication with other airplanes and with air traffic control.

A data communications protocol is a set of rules or an agreement that determines the format and transmission of data. Layer 4 on the source computer communicates with Layer 4 on the destination computer.

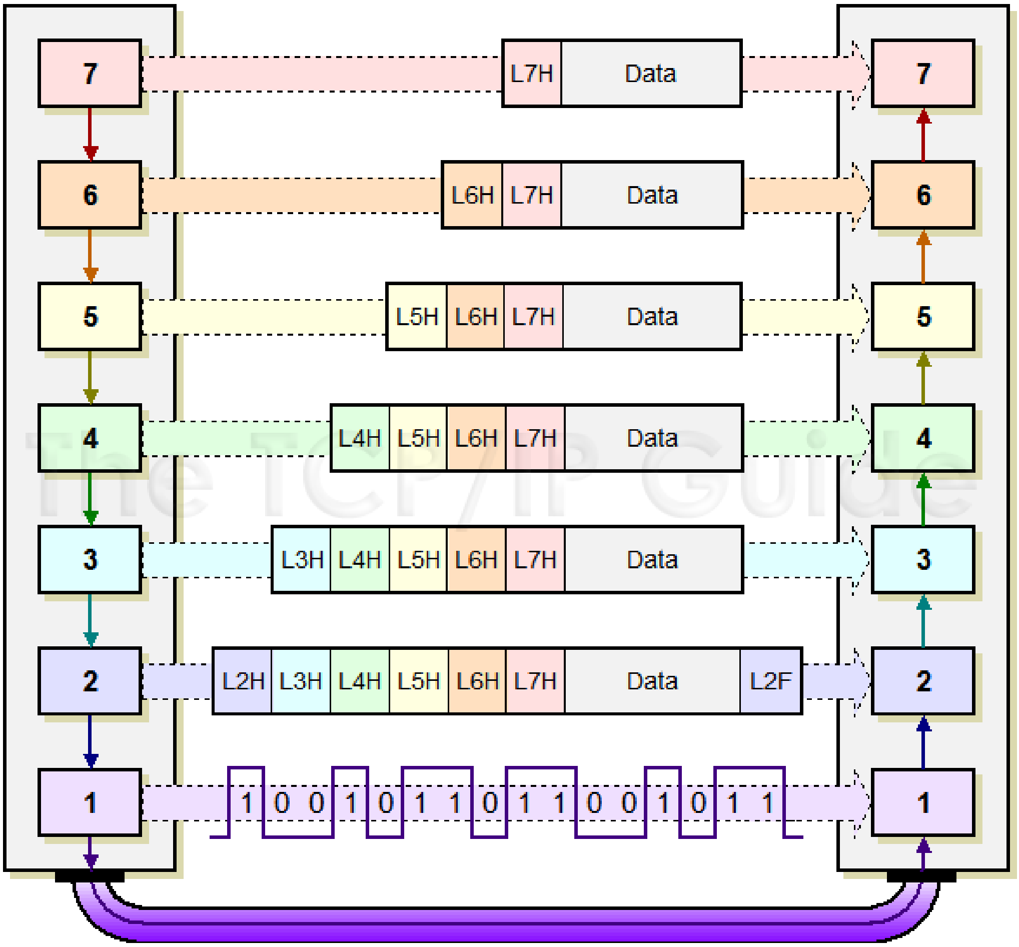


Figure 4-1 Data Operation

The rules and conventions used for this layer are known as Layer 4 protocols. It is important to remember that protocols linearly prepare data. A protocol in one layer **performs a certain set of operations on data as it prepares the data to be sent over the network**. The *data is then passed to the next layer* where another protocol *performs a different set of operations*. Once the packet has been sent to the destination, the protocols **undo the construction** of the packet that was done on the source site. This is done in reverse order.

The protocols for each layer on the destination return the information to its original form, so the application can properly read.

4.3 OSI model

The early development of networks was disorganized in many ways. The early 1980s saw tremendous increases in the number and size of networks. As companies realized the advantages of using networking technology, networks were added or expanded almost as rapidly as new network technologies were introduced.

By the mid-1980s, these companies began to experience problems from rapid expansion. Just as people that do not speak the same language have difficulty communicating with each other, it was difficult for networks that used different specifications and implementations to exchange information. The same problem occurred with companies that developed private or proprietary networking technologies. Proprietary means that one or a small group of companies controls all usage of the technology. Networking technologies strictly following proprietary rules could not communicate with technologies that followed different proprietary rules.

To address the problem of network incompatibility, the International Organization for Standardization (ISO) researched networking models like Digital Equipment Corporation net (DECnet), Systems Network Architecture (SNA), and TCP/IP to find a generally applicable set of rules for all networks. Using this research, the ISO created a network model that helps vendors to create networks that are compatible with other networks. The Open System Interconnection (OSI) reference model released in 1984 was the descriptive network model that the ISO created. It provided vendors with a set of standards that ensured greater compatibility and interoperability among various network technologies produced by companies around the world.

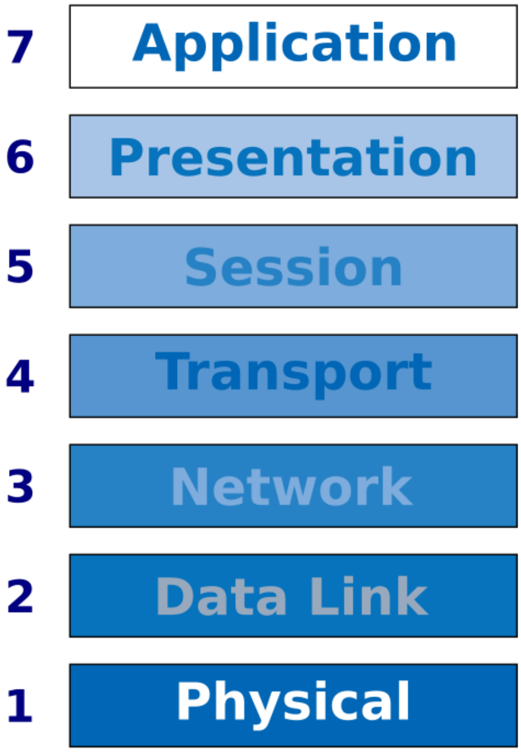


Figure 4-2 OSI Layers

The OSI reference model has become the primary model for network communications. Although there are other models in existence, most network vendors relate their products to the OSI reference model. This is especially true when they want to educate users on the use of their products. It is considered the best tool available for teaching people about sending and receiving data on a network. In the Interactive Media Activity, students will identify the benefits of the OSI model.

Benefits of the OSI Model:

- Reduce Complexity.
- Standardizes Interfaces.
- Facilitates Modular Engineering.
- Ensures Interoperable Technology.
- Accelerates Evolution.
- Simplifies Teaching and Learning.

The OSI reference model is a framework that is used to understand how information travels throughout a network. The OSI reference model explains how packets travel through the various layers to another device on a network, even if the sender and destination have different types of network media. In the OSI reference model, there are seven numbered layers, each of which illustrates a particular network function. Dividing the network into seven layers provides the following advantages:

- It breaks network communication into smaller, more manageable parts.
- It standardizes network components to allow multiple vendor development and support.
- It allows different types of network hardware and software to communicate with each other.
- It prevents changes in one layer from affecting other layers.
- It divides network communication into smaller parts to make learning it easier to understand.

4.4 OSI layers

Each layer has a set of functions that it must perform for data packets to travel from a source to a destination on a network. Below is a brief description of each layer in the OSI reference model.

4.4.1 Layer 7: The Application Layer

The application layer is the OSI layer that is closest to the user; it provides network services to the user’s applications. It differs from the other layers in that it does not provide services to any other OSI layer, but rather, only to applications outside the OSI model. Examples of such applications are spreadsheet programs, word processing programs, and bank terminal programs. The application layer establishes the availability of intended communication partners synchronizes and establishes agreement on procedures for error recovery and control of data integrity. *If you want to remember layer seven in as few words as possible, think of browsers.*

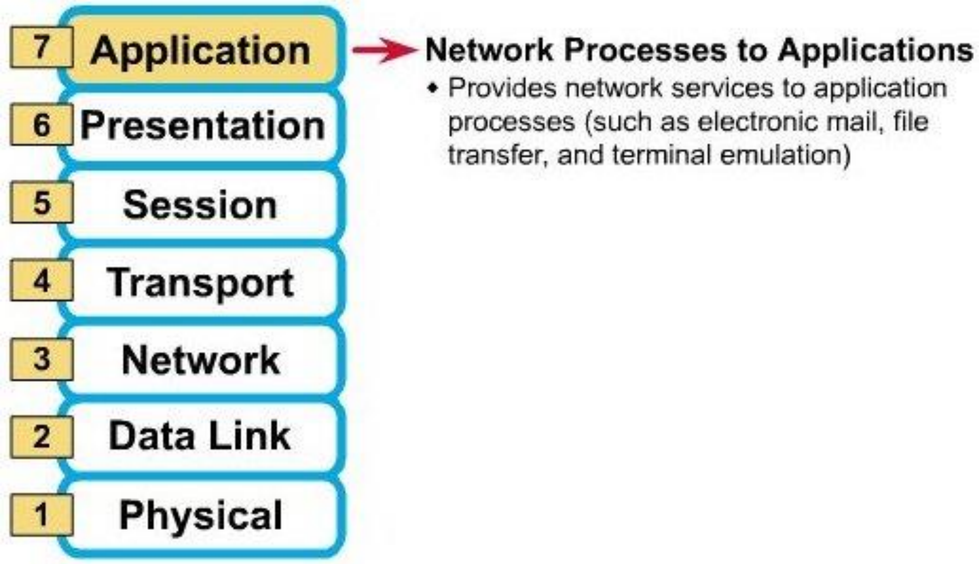

7 Application
6 Presentation
5 Session
4 Transport
3 Network
2 Data Link
1 Physical
Network Processes to Applications
• Provides network services to application processes (such as electronic mail, file transfer, and terminal emulation)

Figure 4-3 Application Layer

4.4.2 Layer 6: The Presentation Layer

The presentation layer ensures that the information that the application layer of one system sends out is readable by the application layer of another system. If necessary, the presentation layer translates between multiple data formats by using a common format. *If you want to think of layer 6 in a few words as possible, think of a common data format.*

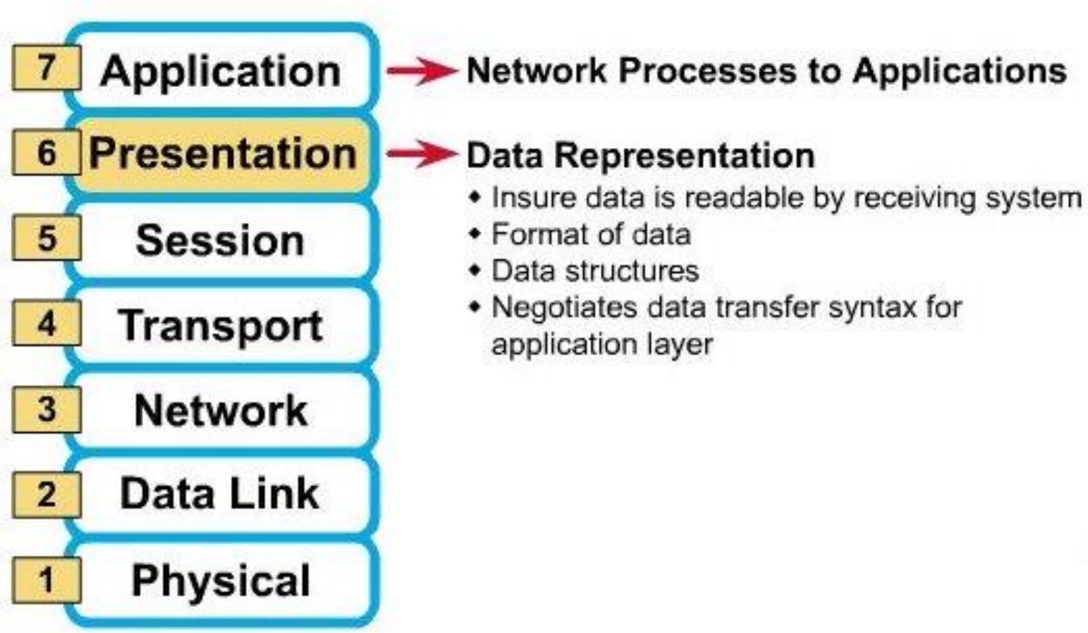

7
Application
6
Presentation
5
Session
4
Transport
3
Network
2
Data Link
1
Physical
Network Processes to Applications
Data Representation
• Insure data is readable by receiving system
• Format of data
• Data structures
• Negotiates data transfer syntax for application layer

Figure 4-4 Presentation Layer

4.4.3 Layer 5: The Session Layer

As its name implies, the session layer establishes, manages, and terminates sessions between two communicating hosts. The session layer provides its services to the presentation layer. It also synchronizes dialogue between the two hosts' presentation layers and manages their data exchange. In addition to session regulation, the session layer offers provisions for efficient data transfer, class of service, and exception reporting of session layer, presentation layer, and application layer problems. *If you want to remember layer 5 in as few words as possible, think of dialogues and conversations.*

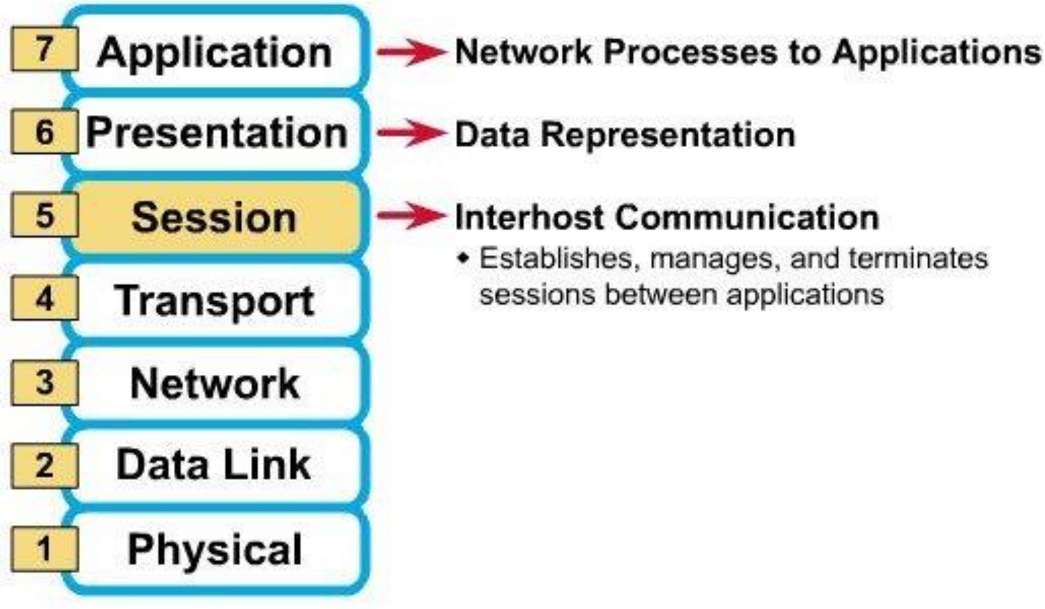


Figure 4-5 Session Layer

4.4.4 Layer 4: The Transport Layer

The transport layer segments data from the sending host’s system and reassembles the data into a data stream on the receiving host’s system. The boundary between the media-layer and transport layer can be thought of as the boundary between media-layer protocols and host-layer protocols. Whereas the application, presentation, and session layers are concerned with application issues, the lower three layers are concerned with data transfer issues.

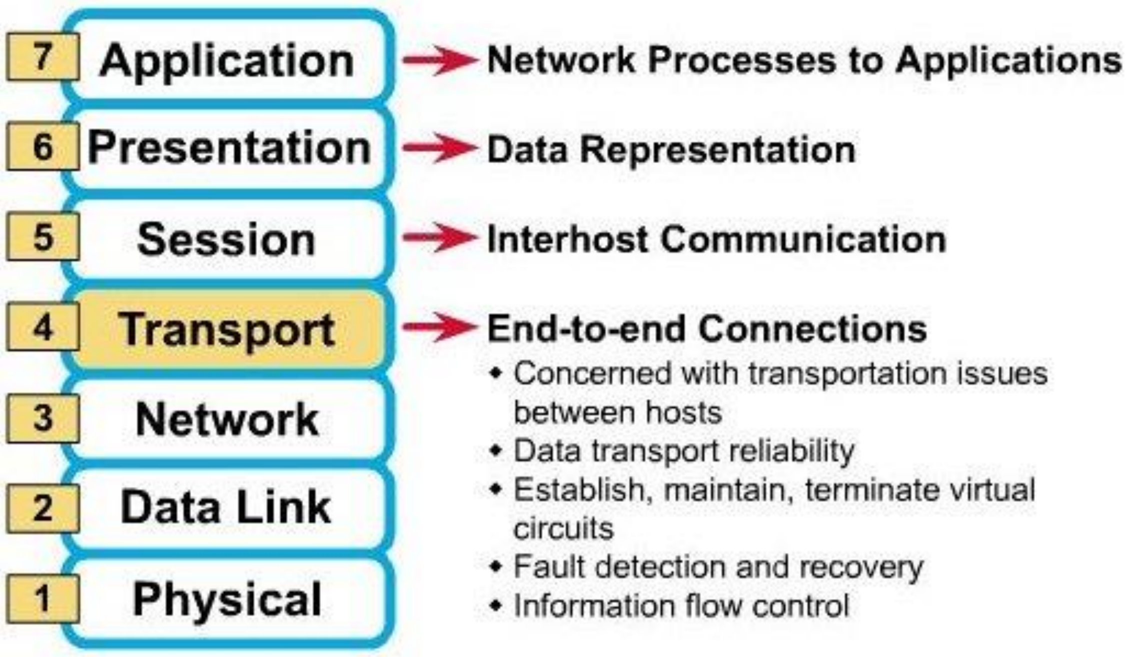

7 Application
6 Presentation
5 Session
4 Transport
3 Network
2 Data Link
1 Physical
Network Processes to Applications
Data Representation
Interhost Communication
End-to-end Connections
• Concerned with transportation issues between hosts
• Data transport reliability
• Establish, maintain, terminate virtual circuits
• Fault detection and recovery
• Information flow control

Figure 4-6 Transport Layer

The transport layer attempts to provide a data transfer service that shields the upper layers from transport implementation details. Specifically, issues such as how reliable transport between two hosts is accomplished are the concern of the transport layer. In providing communication service, the transport layer establishes, maintains, and properly terminates virtual recovery and information flow control is used. *If you want to remember layer 4 in as few words as possible, think of the quality of service, and reliability.*

4.4.5 Layer 3: The Network Layer

The network layer is a complex layer that provides connectivity and path selection between two host systems that may be located on geographically separated networks. *If you want to remember layer 3 in* *as few words as possible, think of path selection, routing, and addressing.*

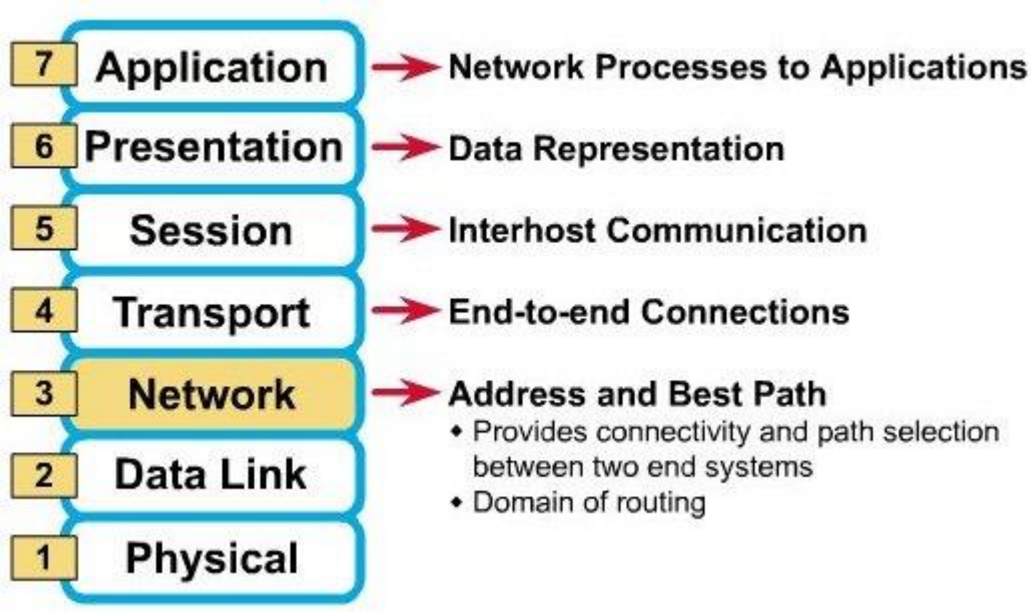


Figure 4-7 Network Layer

4.4.6 Layer 2: The Data Link Layer

The data link layer provides reliable transmit of data across a physical link in so doing, the data link layer is concerned with physical (as opposed to logical) addressing, network topology, network access, error notification, ordered delivery of frames, and media access control.

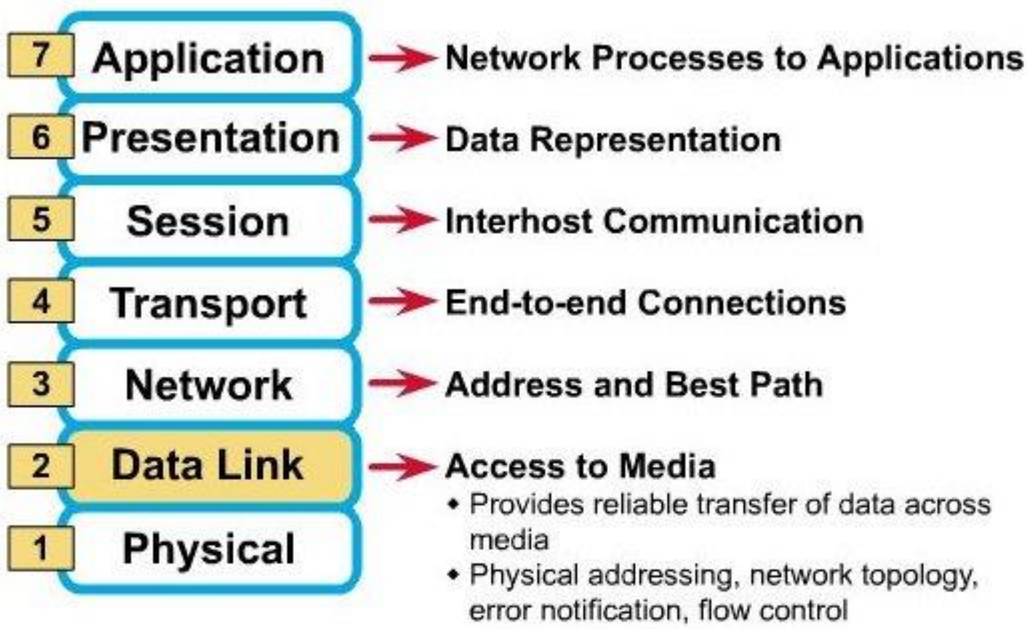


Figure 4-8 Data Link Layer

4.4.7 Layer 1: The Physical Layer

The physical layer defines the electrical, mechanical, procedural, and functional specifications for activating, maintaining, and deactivating the physical link between end systems. Such characteristics as voltage levels, the timing of voltage changes, physical data rates, maximum transmission distances, physical connectors, and other, similar, attributes are defined by physical layer specifications. *If you want to remember layer 1 in as few words as possible, think of signals and media.*

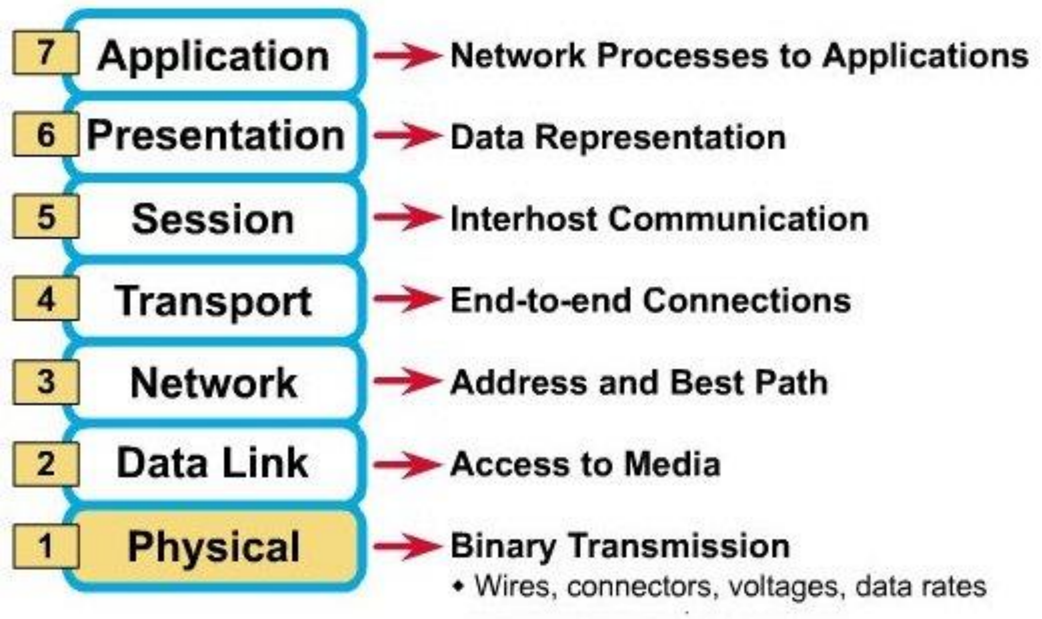

7 Application → Network Processes to Applications
6 Presentation → Data Representation
5 Session → Interhost Communication
4 Transport → End-to-end Connections
3 Network → Address and Best Path
2 Data Link → Access to Media
1 Physical → Binary Transmission
• Wires, connectors, voltages, data rates

Figure 4-9 Physical Layer

To help remember them in the correct order a common mnemonic is often used from 7 to 1 (top to bottom):

All

People

Seem

To

Need

Data

Processing

For those of you who like the Domino's or Pappa John's pies, try from 1 to 7 (bottom to top):

Please

Do

Not

Throw

Sausage

Pizza

Away

4.5 Encapsulation

You know that all communications on a network originate at a source, and are sent to a destination and that the information that is sent on a network is referred to as data or data packets. If one computer (host A) wants to send data to another (host B), the data must first be packaged by a process called encapsulation. Encapsulation wraps data with the necessary protocol information before network transit. Therefore, as the data packet moves down through the layers of the OSI model, it receives headers, trailers, and other information. (Note: The word "header" means that address information has been added). To see how encapsulation occurs, let's examine how data travels through the layers. Once the data is sent from the source, it travels through the application layer down through the other layers. As you can see, the packaging and flow of the data that is exchanged goes through changes as the networks perform their services for end-users.

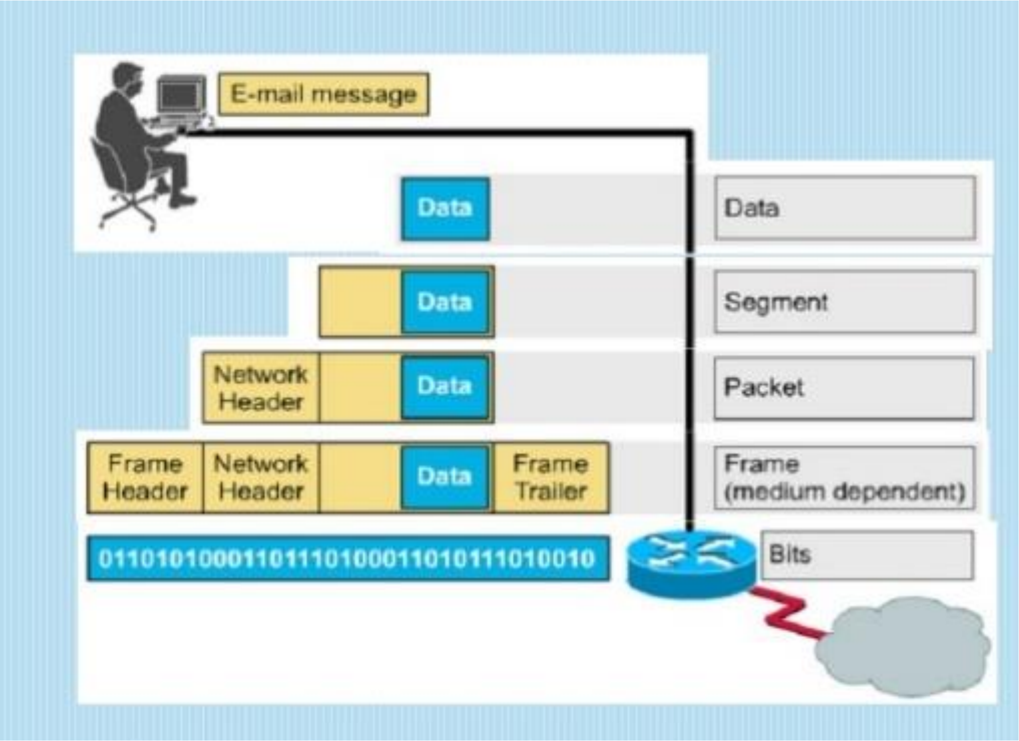


Figure 4-10 Encapsulation example: E-mail

Networks must perform the following five conversion steps to encapsulate data:

1- **Build the data (application layer):** As a user sends an e-mail message, its alphanumeric characters are converted to data that can travel across the internetwork.

2- **Package the data for end-to-end transport (transport layer):** The data is packaged for internetwork transport. By using segments, the transport function ensures that the message hosts at both ends of the e-mail system can reliably communicate.

3- **Append (add) the network address to the header (network layer):** The data is put into a packet or datagram that contains a network header with source and destination logical addresses. These addresses help network devices send the packets across the network along a chosen path.

4- **Append (add) the local address to the data link header (data link layer):** Each network device must put the packet into a frame. The frame allows connection to the next directly-connected network device on the link. Each device in the chosen network path requires framing for it to connect to the next device.

5- **Convert to bits for transmission (physical layer):** The frame must be converted into a pattern of 1s and 0s (bits) for transmission on the medium (usually a wire). A clocking function enables the devices to distinguish these bits as they travel across the medium. The medium on the physical internetwork can vary along the path used. For example, the e-mail message can originate on a LAN, cross a campus backbone, and go out a WAN link until it reaches its destination on another remote LAN. Headers and trailers are added as data moves down through the layers of the OSI model.

4.6 Peer-to-peer communications

For data to travel from the source to the destination, each layer of the OSI model at the source must communicate with its peer layer at the destination. This form of communication is referred to as peer-to-peer. During this process, the protocols of each layer exchange information, called protocol data units (PDUs). Each layer of communication on the source computer communicates with a layer-specific PDU, and with its peer layer on the destination computer as illustrated in the figure.

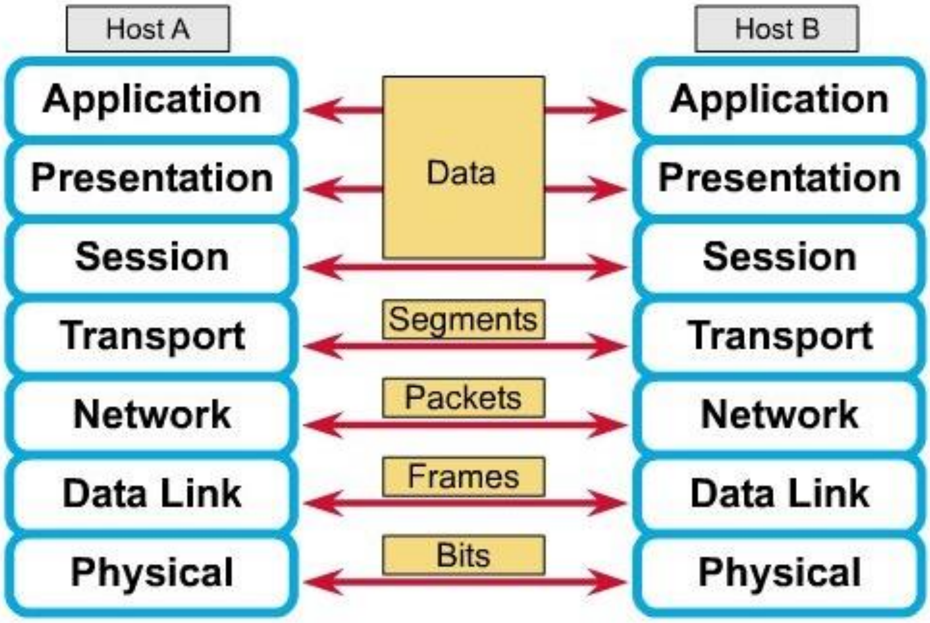


Figure 4-11 Peer-to-peer communications

Data packets on a network originate at a source and then travel to a destination. Each layer depends on the service function of the OSI layer below it. To provide this service, the lower layer uses encapsulation to put the PDU from the upper layer into its data field. Then it adds whatever headers and trailers the layer needs to perform its function. Next, as the data moves down through the layers of the OSI model, additional headers and trailers are added. After Layers 7, 6, and 5 have added their information, Layer 4 adds more information. This grouping of data, the Layer 4 PDU, is called a segment.

The network layer provides a service to the transport layer, and the transport layer presents data to the internetwork subsystem. The network layer has the task of moving the data through the internetwork. It accomplishes this task by encapsulating the data and attaching a header creating a packet (the Layer 3 PDU). The header contains information required to complete the transfer, such as source and destination logical addresses. The data link layer provides a service to the network layer. It encapsulates the network layer information in a frame (the Layer 2 PDU). The frame header

contains information (for example, physical addresses) required to complete the data link functions. The data link layer provides a service to the network layer by encapsulating the network layer information in a frame. The physical layer also provides a service to the data link layer. The physical layer encodes the data link frame into a pattern of 1s and 0s (bits) for transmission in the medium (usually a wire) at layer 1.

4.7 TCP/IP model

The U.S. Department of Defense (DoD) created the TCP/IP reference model because it wanted to design a network that could survive any conditions, including a nuclear war. In a world connected by different types of communication media such as copper wires, microwaves, optical fibers, and satellite links, the DoD wanted transmission of packets every time and under any conditions. This very difficult design problem brought about the creation of the TCP/IP model. Unlike the proprietary networking technologies mentioned earlier, TCP/IP was developed as an open standard. This meant that anyone was free to use TCP/IP. This helped speed up the development of TCP/IP as a standard. The TCP/IP model has the following four layers:

1- Application layer
2- Transport layer

3- Internet layer

4- Network access layer

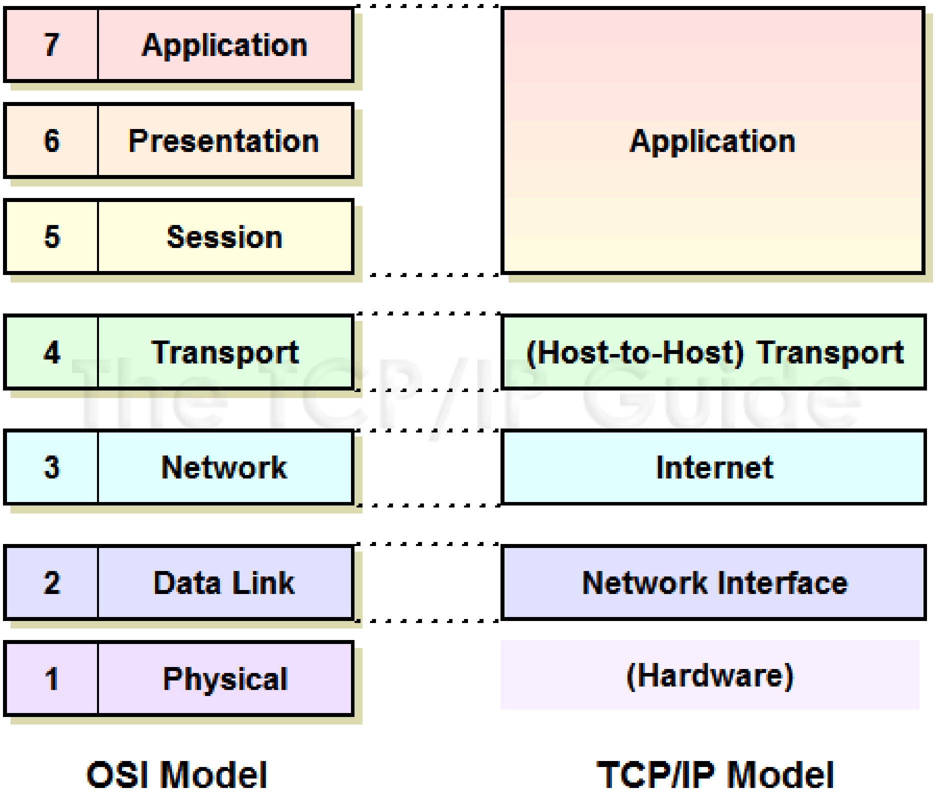


Figure 4-12 TCP/IP model vs OSI Model

Although some of the layers in the TCP/IP model have the same name as layers in the OSI model, the layers of the two models do not correspond exactly. Most notably, the application layer has different functions in each model. The designers of TCP/IP felt that the application layer should include the OSI session and presentation layer details. They created an application layer that handles issues of representation, encoding, and dialog control. The transport layer deals with the quality of service issues of reliability, flow control, and error correction. One of its protocols, the transmission control protocol

(TCP), provides excellent and flexible ways to create reliable, well flowing, low-error network communications. TCP is a connection-oriented protocol. It maintains a dialogue between source and destination while packaging application layer information into units called segments. Connection-oriented does not mean that a circuit exists between the communicating computers. It does mean that Layer 4 segments travel back and forth between two hosts to acknowledge the connection exists logically for some period. The purpose of the Internet layer is to divide TCP segments into packets and send them from any network. The packets arrive at the destination network independent of the path they took to get there. The specific protocol that governs this layer is called the Internet Protocol (IP). Best path determination and packet switching occur at this layer. The relationship between IP and TCP is an important one. IP can be thought to point the way for the packets, while TCP provides reliable transport. The name of the network access layer is very broad and somewhat confusing. It is also known as the host-to-network layer. This layer is concerned with all of the components, both physical and logical, that is required to make a physical link. It includes the networking technology details, including all the details in the OSI physical and data link layers.

The following figure illustrates some of the common protocols specified by the TCP/IP reference model layers.

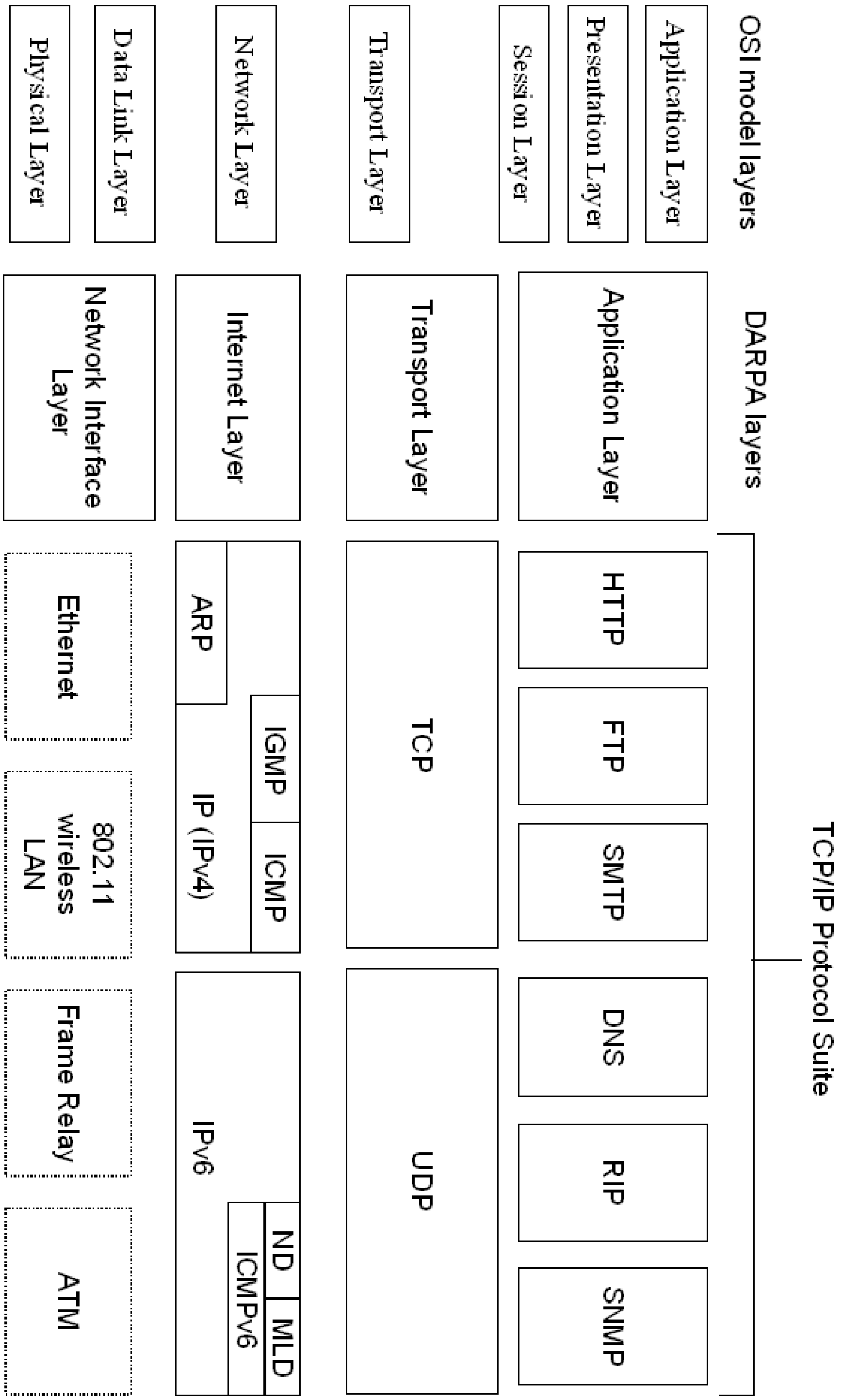


Figure 4-13 TCP/IP Protocol

Some of the most commonly used application layer protocols include the following:

1. File Transfer Protocol (FTP)
2. Hypertext Transfer Protocol (HTTP)
3. Simple Mail Transfer Protocol (SMTP)
4. Domain Name System (DNS)
5. Trivial File Transfer Protocol (TFTP)

The common transport layer protocols include:

1. Transport Control Protocol (TCP)
2. User Datagram Protocol (UDP)

The primary protocol of the Internet layer is:

1. Internet Protocol (IP)

The network access layer refers to any particular technology used on a specific network. Regardless of which network application services are provided and which transport protocol is used, there is only one Internet protocol, IP. This is a deliberate design decision. IP serves as a universal protocol that allows any computer anywhere to communicate at any time. A comparison of the OSI model and the TCP/IP model will point out some similarities and differences.

Similarities include:

1. Both have layers.
2. Both have application layers, though they include very different services.
3. Both have comparable transport and network layers.

4. Both models need to be known by networking professionals.
5. Both assume packets are switched. This means that individual packets mat take different paths to reach the same destination. This is contrasted with circuit-switched networks where all the packets take the same path.

Differences include:

1. TCP/IP combines the presentation and session layer issues into its application layer.
2. TCP/IP combines the OSI data link and physical layers into the network access layer.
3. TCP/IP appears simpler because it has fewer layers.
4. TCP/IP protocols are the standards around which the Internet developed, so the TCP/IP model gains credibility just because of its protocols. In contrast, networks are not usually built on the OSI protocol, even though the OSI model is used as a guide.

Although TCP/IP protocols are the standards with which the Internet has grown, this curriculum will use the OSI model for the following **reasons**:

1. It is a generic, protocol independent standard.
2. It has more details, which make it more helpful for teaching and learning.
3. It has more details, which can be helpful when troubleshooting. Networking professionals differ in their opinions on which model to use.

Due to the nature of the industry, it is necessary to become familiar with both. Both the OSI and TCP/IP models will be referred to throughout the curriculum. The focus will be on the following:

1. TCP as an OSI layer 4 protocol
2. IP as an OSI Layer 3 protocol
3. Ethernet as a Layer 2 and Layer 1 technology

Remember that there is a difference between a model and an actual protocol that is used in networking. The OSI model will be used to describe TCP/IP protocols.

Transmission Control Protocol (TCP)

Transmission Control Protocol, TCP, is a connection-oriented protocol that functions on the Transport layer of the OSI model. When two computers on a network need to communicate, TCP opens a connection between the computers. When the data packet is ready to be sent, TCP adds to the packet header information that contains flow control and error checking.

Internet Protocol (IP):

The Internet protocol, IP, is a connectionless protocol that operates at the Network layer of the OSI model. When data packets ate sent over the network, IP is responsible for addressing the packets and routing them through the network. Attached to each packet is an IP header that contains the sending address and receiving address. When the packets reach their final destination, the IP puts all the packets together again in the correct order.

User Datagram Protocol (UDP):

The User Datagram Protocol (UDP) provides a datagram service. A datagram is a way of sending messages with a minimum of overhead. Delivery is not guaranteed. No checking for missing or out-of-sequence packet is performed, and no acknowledgments are sent.

File Transfer Protocol (FTP):

File Transfer Protocol, or FTP, is used for file sharing between computers that use TCP/IP to communicate. FTP allows users to log on to a remote computer on a network and see that files are on the computer. It allows users to also upload and download files between the two computers. FTP is a widely used Application layer protocol because an FTP service exists for almost every operating system.

Simple Mail Transfer Protocol (SMTP):

Simple Mail Transfer Protocol (SMTP) makes sure that e-mail is delivered from the sender’s service to the intended recipient’s e-mail server. It does not handle the delivery to the final e-mail desktop location. SMTP is an Application layer protocol.

4.8 Exercise

1. What layer converts data into frames?
2. Which layers convert data into segments.
3. What is the purpose of the TCP protocol?
4. What layer converts data into packets?
5. Explain the TCP/IP model
6. What is the protocol name that resolves domain into IP addresses?
7. What layer converts data into bits?
8. What is the purpose of the TCP protocol?
9. How many layers TCP/IP model has?
10. Which OSI layer responsible for mail and file transfers?
11. What are the similarities and differences between TCP/IP and OSI model?
12. List all steps need for networks to encapsulate data.
13. What are the benefits of the OSI model?

CHAPTER 5

Internet Protocols

5.1 Introduction

IP is the transmission mechanism used by the TCP/IP protocols. It is an unreliable and connectionless datagram protocol a best-effort (IP provides no error checking or tracking) delivery service. IP assumes the unreliability of the underlying layers and does its best to get a transmission through to its destination, but with no guarantees. The IP address is a 32-bit integer, composed of 4-octets, and that from 1 to 3 of the leading octets specify the network address; the remaining one (s) specify the host ID within that network.

5.2 Assignment of IP Addresses

In addition to the physical addresses (contained on NICs) that identify individual devices, the Internet requires an additional addressing convention; an address that identifies the connection of the host to its network. The IP address is globally unique. A central authority, the Network Information Center (NIC), is responsible for handing out blocks of IP addresses; also it has delegated that authority to other organizations, each one of which “owns” a top-level domain (e.g. EDU=Educational Institutions, COM=Commercial Enterprises, GOV=Governmental Organizations, MIL=Military Organizations, NET=Network Organizations, and ORG=Miscellaneous Organizations). There are separate domains for countries (e.g. UK=United Kingdom, and CA=Canada).

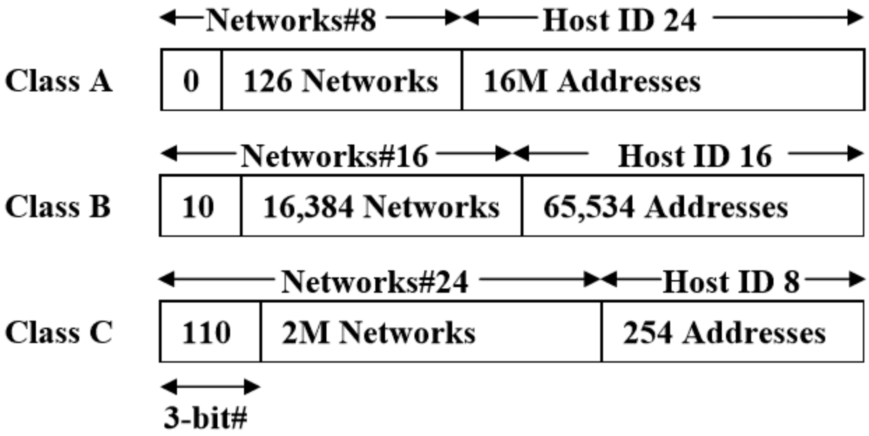
5.3 IP Address Format

Each Internet address consists of four bytes (32-bits), defining three fields: **class type**, **Net ID**, and **Host ID**. These parts are varying lengths, depending on the class of the address. The classes meet the needs of large, medium, and small sub-networks of the Internet. A state university might have a class B address and a small company may have a class C address. Also, class A addresses are numerically the lowest and accommodate more hosts than class B, or class C networks. A full address is available in class C only. The remaining unassigned octets of the four are assigned locally by the network administrator (master).

Table (1) Class A, B & C IP Addresses

Cl.	**w**	**N. ID**	**H. ID**	**No. Net**	**No. Host**
A	1-126	w	x.y.z	126	256^3-2=16777214
B	128-191	w.x	y.z	64*256=16384	256^2 -2= 65534
C	192-223	w.x.y	z	32*256^2 = 2097152	256-2 = 254

5.4 IP Address Class Identification



Network Address Range	IP Address Range
A=1.0.0.0 → 126.0.0.0	A=1.0.0.1 → 126.255.255.254
B=128.0.0.0 → 191.255.0.0	B=128.0.0.1 → 191.255.255.254
C=192.0.0.0 → 233.255.255.0	C=192.0.0.1 → 233.255.255.254

Figure (1) Class A, B & C network addresses

5.4.1 Class A Address

There are only 126 networks because network numbers of 0 and 127 are reserved for a special purpose. So the octets range from 0000 0001 to 0111 1110, which are the decimal values of 1 to 126. The IP address obtained by allowing the host ID octets to range from 0 to 255, with the exception that no network number or host ID may be all 0’s or all 1’s.

5.4.2 Class B Address

The most significant 2-bits (10) are interpreted as the network address. The first octets range from 1000 0000 to 1011 1111, yielding decimal values of 128 to191, and the second octet can range from 0000 0000 to 1111 1111, that is 0 to 255 decimal.

5.4.3 Class C Address

The first octet of this class is range from 1100 0000 to 1101 1111, which is 192 to 223 decimal.

Example: Consider the network node with IP address 185.121.9.12, decipher an IP address.

Solution:

185=1011 1001

∴ The leading bits are (10) and so the signature of a class B address.

The network address is 185.121.0.0

The host ID is 9.12

Note: any device connected to more than one network (e.g. any router) must have more than one Internet address (a device has a different address for each network connected to it).

5.4.4 Broadcast Address

If a packet is directed to all hosts in the network the host field of the destination IP is to be replaced by all-ones bit. The broadcast address is used in some special uses, e.g. in dynamic address assignment protocols.

Example: What is the broadcast address for the network number 148.19.0.0? **Solution**:

Since the network is class B which means that the 3rd and 4th octets are the host field.

Then broadcast **IP** is: 148.19.255.255

Note: All ones make the value $(255)_{10}$= $(1111\ 1111)_2$

The following figure shows the IP addresses distribution for a different type of LAN topologies.

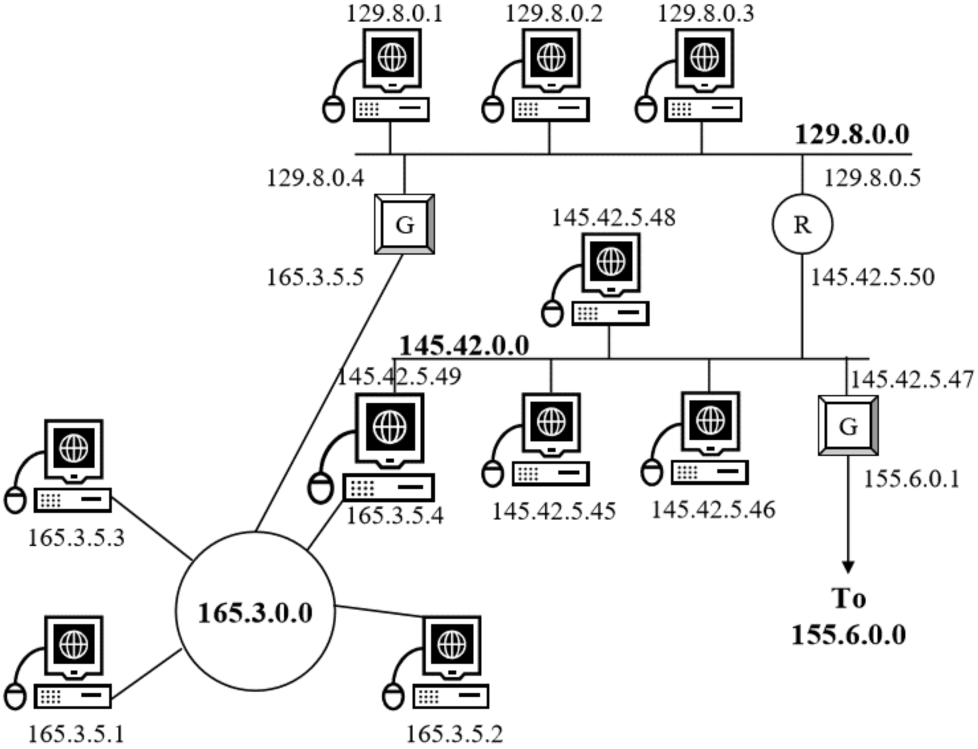


Figure (2) Network and host addresses on the Internet.

Homework: Draw a network with the following specifications:

(a) Two ring networks with four hosts (class A).

(b) Two bus networks with four hosts (class C).

(c) The 1st ring is connected to the 1st bus by a router and the 2nd bus by a gateway.

(d) The 2nd ring is connected to the 1st bus by a gateway and the 2nd bus by a router.

(e) The 1st ring is connected to the 2nd ring by a gateway. Show all the hosts (computers), with their addresses and connections. The address selection is up to you.

5.5 Subnets

With too many hosts to have on a single LAN, the users begin to notice a slowdown in LAN performance. So, network administrators with many hosts interconnecting the LANs by the router. This partitioning of the domain reduces overall network traffic within it because routers isolate local LAN traffic within the local LAN.

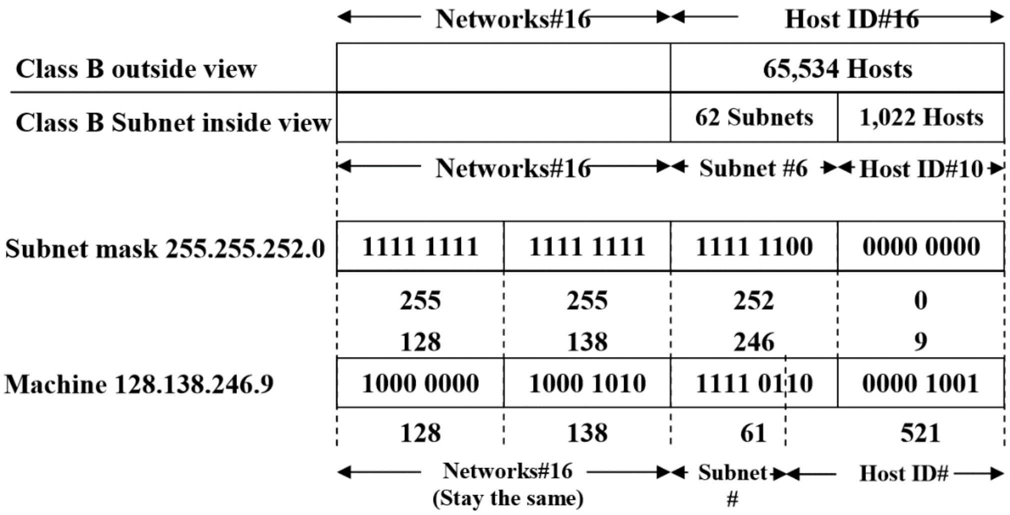


Figure (3) Example of a class B network with a 6-bit subnet.

5.6 Network and Sub Network Masks

In the routing section, routers used a network mask to isolate the **network#** from the **host ID#**. That mask will be 255.0.0.0 for class A address, 255.255.0.0 for class B, and 255.255.255.0 for class C. With subnetting, the network administrator creates a subnet mask for use within the LAN routers of the administrated network that includes both the network mask bits and the subnet mask bits. This creates more networks within the domain and allows the routers to route to the subnetworks within the main network.

Notice the following points:

1- The IP address does not change! It remains (128.138.246.9) regardless of the subnetting scheme. This is because in dotted decimal notation the dots separate octets, and the bit pattern of the assigned address does not change.

2- What changes is the subnet mask? It enlarges to include the subnet bits, and in so doing, it generates a subnet number and a new host ID number.

3- To a router inside the 128.138 domain, the machine resides on subnet 61 and has a host ID of 521, but this is normally of concern only to the network system administration personnel.

Example: Consider the network node with IP address 148.62.191.1, decipher an IP address, then find the subnet number and host ID number with network administrator of 6-bits.

Solution: 148=1001 0100

The leading bits are (10) and so the signature of a class B address.

The network address is 148.62.0.0

The host ID is 191.1

Machine 148.62.191.1

148	62	191	1
1001 0100	0011 1110	1011 1111	0000 0001
148	62	47	769
		Subnet#	Host ID#

Example: Consider the network node with IP address 182.85.201.12, decipher an IP address, and then find the subnet number and host ID number with network administrator of 7-bits.

Solution:

182=1011 0110

The leading bits are (10) and so the signature of a class B address.

The network address is 182.85.0.0

The host ID is 201.12

Machine 148.62.191.1

182	85	201	12
1011 0110	0101 0101	1100 1001	0000 1100
182	85	100	268
		Subnet#	Host ID#

5.7 More Subnetting Masks Ways for Class B

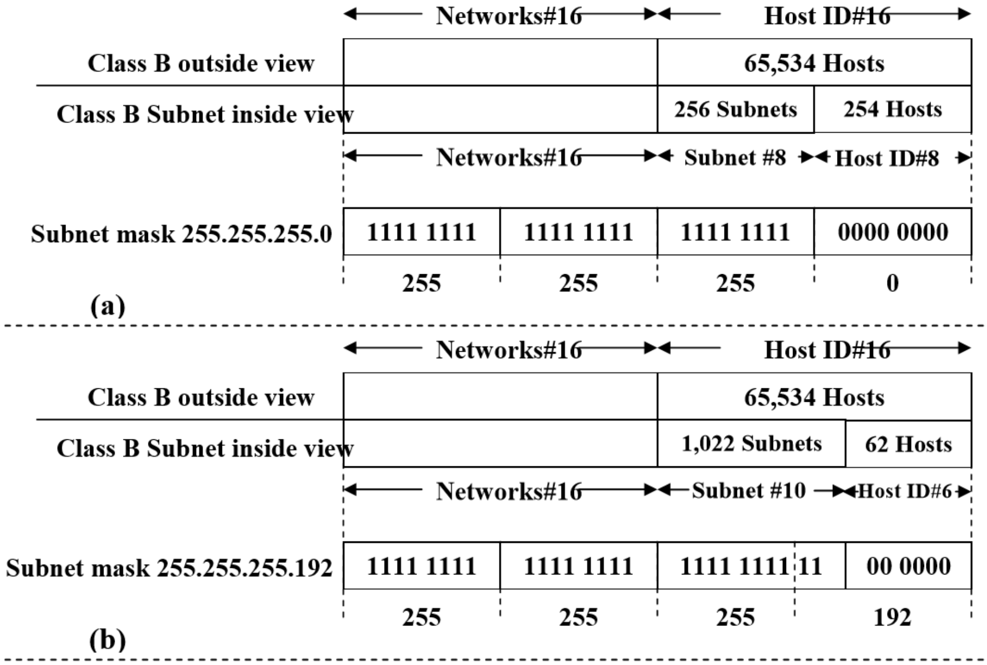


Figure (4) Subnetting class B network: (a) an 8-bit subnet address. (b) a 10-bit subnet address

Q: What is the mask that provides 27 hosts?

- 255.255.255.0
- 255.255.255.192
- 255.255.255.224
- 255.255.224.0

5.8 Exercise

1- Given the IP address, what class of address is it?

a. 126.110.16.7

b. 209.123.32.212

c. 10.14.16.12

d. 172.15.42.34

2- What is the binary number represents 10.12.16.6?

3- According to RFC 1918 this range of Class A IP addresses are reserved for private intranets and are not supposed to be used on the internet (where x is any number from 1 to 254)?

A. 10.x.x.x

B. 20.x.x.x

C. 30.x.x.x

4- IP address is ____bit binary number

CHAPTER 6

Assigning IP Address

6.1 Public and Private IP Addresses

The stability of the Internet depends directly on the uniqueness of publicly used network addresses. In Figure 6-1 Required Unique Addresses, there is an issue with the network addressing scheme. In looking at the networks, both have a network address of 198.150.11.0. The router in this illustration will not be able to forward the data packets correctly. Duplicate network IP addresses prevent the router from performing its job of best-path selection. Unique addresses are required for each device on a network.

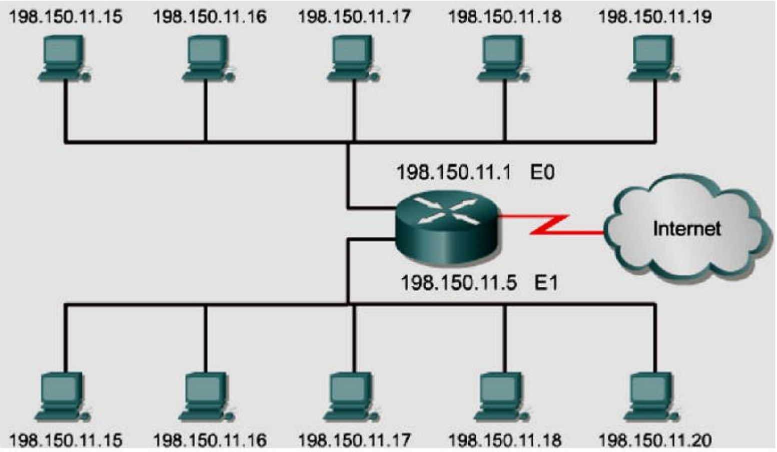


Figure 6-1 Required Unique Addresses

A procedure was needed to make sure that addresses were unique. Originally, an organization known as the Internet Network Information Center (InterNIC) handled this procedure. InterNIC no longer exists and has been succeeded by the Internet Assigned Numbers Authority (IANA). IANA carefully manages the remaining supply of IP addresses to ensure that duplication of publicly used addresses does not occur. Duplication would cause instability on the Internet and compromise its ability to deliver datagrams to networks. Public IP addresses are unique. No two machines that connect to a public network can have the same IP address because public IP addresses are global and standardized. All machines connected to the Internet agree to conform to the system. Public IP addresses must be obtained from an Internet service provider (ISP) or a registry at some expense. With the rapid growth of the Internet, public IP addresses were beginning to run out.

Table 2 Private IP Addresses

Class	Invisible Ranges (non routed addresses)	abbreviated
A	10.0.0.1 – 10.255.255.254 ≅ 16000000	10.0.0.0 / 8
B	172.16.0.1 – 172.31.255.254 ≅ 10000000	172.16.0.0 / 12
C	192.168.0.1 – 192.168.255.254 ≅ 65000	192.168.0.0 / 16

Private IP addresses are another solution to the problem of the impending exhaustion of public IP addresses. As mentioned, public networks require hosts to have unique IP addresses. However, private networks that are not connected to the Internet may use any host addresses, as long as each host within the private network is unique. Many private networks exist alongside public networks. However, a private network using just any address is strongly discouraged because that network might eventually be connected to the Internet. RFC 1918 sets aside three blocks of IP addresses for private, internal use.

These three blocks consist of one Class A, a range of Class B addresses, and a range of Class C addresses. Addresses that fall within these ranges are not routed on the Internet backbone. Internet routers immediately discard private addresses. If addressing a nonpublic intranet, a test lab, or a home network, these private addresses can be used instead of globally unique addresses. Private IP addresses can be intermixed, as shown in the graphic, with public IP addresses. This will conserve the number of addresses used for internal connections.

6.2 IPv4 Versus IPv6

The TCP/IP is sustaining a global network of information, commerce, and entertainment. IP Version 4 (IPv4) offered an addressing strategy that, although scalable for a time, resulted in an inefficient allocation of addresses. Unfortunately, Class C addresses are limited to 254 usable hosts. This does not meet the needs of larger organizations that cannot acquire a Class A or B address. Even if there were more Class A, B, and C addresses, too many network addresses would cause Internet routers to come to a stop under the burden of the enormous size of routing tables required to store the routes to reach each of the networks Over the past two decades, numerous extensions to IPv4 have been developed. These extensions are specifically designed to improve the efficiency with which the 32-bit address space can be used. Two of the more important of these are subnet masks and classless interdomain routing (CIDR). Meanwhile, an even more extendible and scalable version of IP, IP Version 6 (IPv6), has been defined and developed. IPv6 uses 128 bits rather than the 32 bits currently used in IPv4. IPv6 uses hexadecimal numbers to represent the 128 bits. IPv6 provides 640 six trillion addresses. This version of IP should provide enough addresses for future communication needs.

Internet Protocol Version 4 (Ipv4) 4 octets

1101000	1001110	1100100	0111000
1	0	1	1
209.	156.	201.	113

2^{32}=4,294,967,295 IP addresses (Approx.):4.3 billion

4,300,000,000

Internet Protocol Version 6 (Ipv4) 16 octets

10100101.00100100	01110010.11010011	00101100.10000000	11011101.00000010
A524:	72D3:	2C80:	DD02:
00000000.00101001	11101100.01111010	00000000.00101011	11101010.01110011
0029:	EC7A:	002B:	EA73

2^{128}=3.4x1038 IP addresses (approx.):340 Undecillion

340,000,000,000,000,000,000,000,000,000,00
0,000,000,000

Figure 6-2 Ipv4 and Ipv6 Addresses

IPv4 addresses are 32 bits long, written in decimal form, and separated by periods. IPv6 addresses are 128-bits long and are identifiers for individual interfaces and sets of interfaces. IPv6 addresses are assigned to interfaces, not nodes. Since each interface belongs to a single node, any of the unicast addresses assigned to the interfaces of the node may be used as an identifier for the node. IPv6 addresses are written in hexadecimal, and separated by colons. IPv6 fields are 16 bits long. To make the addresses easier to read, leading zeros can be omitted from each field. The field: 0003: is written: 3: I Pv6 shorthand representation of the 128 bits use eight 16-bit numbers, shown as four hexadecimal digits.

6.3 Obtaining an Internet Address

A network host needs to obtain a globally unique address to function on the Internet. The physical or MAC address that a host has is only locally significant, identifying the host within the local area network. Since this is a Layer 2 address, the router does not use it to forward outside the LAN. IP addresses are the most commonly used addresses for Internet communications. This protocol is a hierarchical addressing scheme that allows individual addresses to be associated together and treated as groups. These groups of addresses allow efficient transfer of data across the Internet.

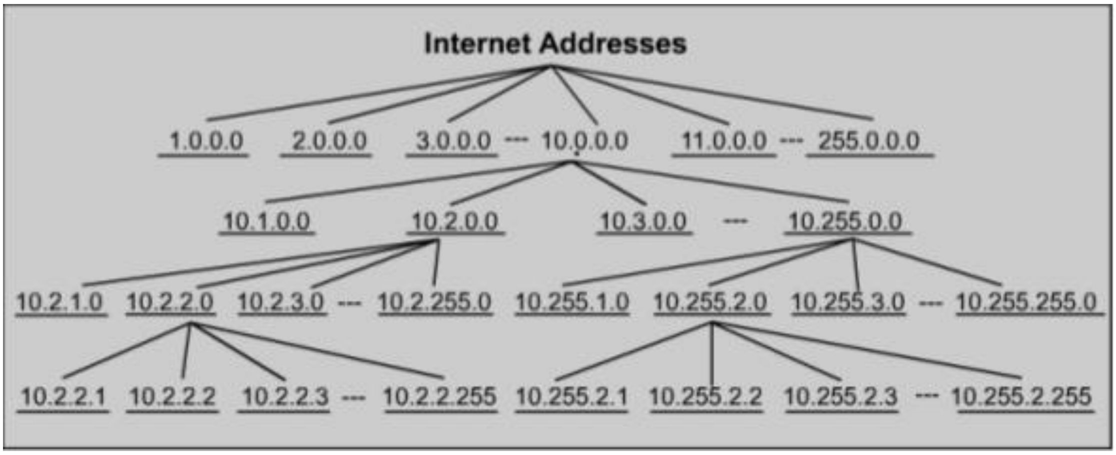


Figure 6-3 Internet Addresses

Network administrators use two methods to assign IP addresses. These methods are static and dynamic. Later in this lesson, static addressing and three variations of dynamic addressing will be covered. Regardless of which addressing scheme is chosen, no two interfaces can have the same IP address. Two hosts that have the same IP address could create a conflict that might cause both of the hosts involved not to operate properly. As shown in Figure 6-4 Assigning IP Addresses, the hosts have a physical address by having a network interface card that allows connection to the physical medium. The figure will focus on static IP address assignments.

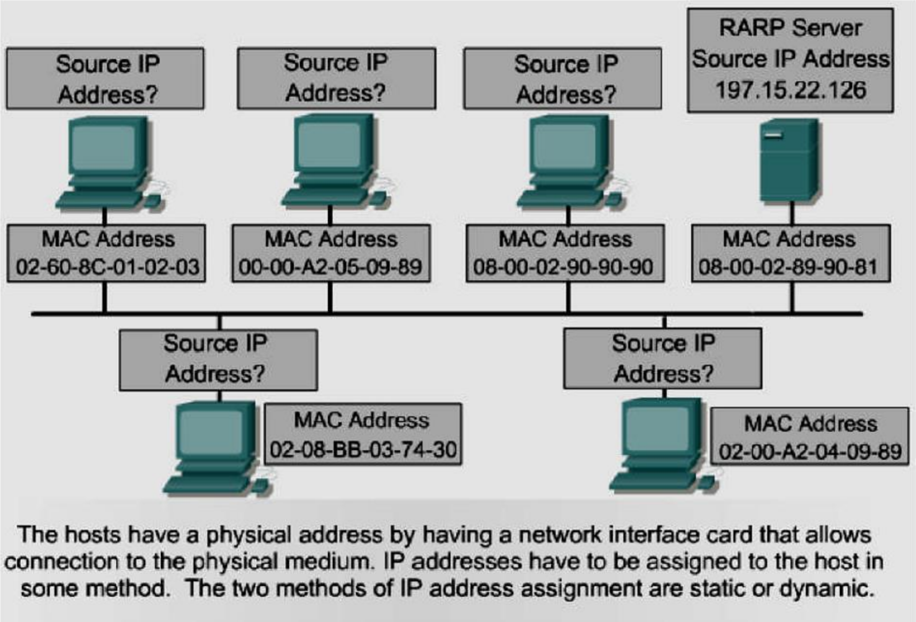
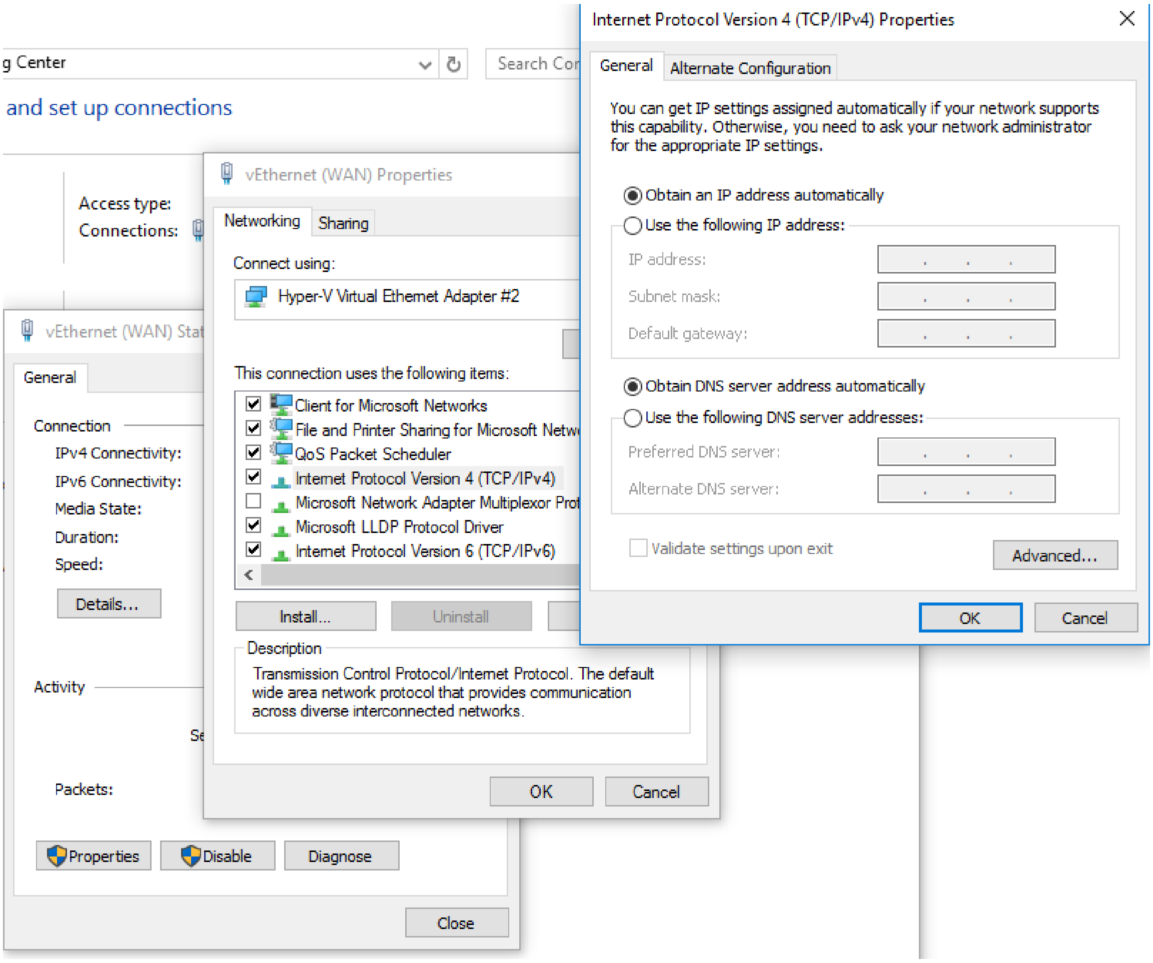

RARP Server
Source IP Address
197.15.22.126
Source IP Address?
Source IP Address?
Source IP Address?
MAC Address 02-60-8C-01-02-03
MAC Address 00-00-A2-05-09-89
MAC Address 08-00-02-90-90-90
MAC Address 08-00-02-89-90-81
Source IP Address?
Source IP Address?
MAC Address 02-08-BB-03-74-30
MAC Address 02-00-A2-04-09-89
The hosts have a physical address by having a network interface card that allows connection to the physical medium. IP addresses have to be assigned to the host in some method. The two methods of IP address assignment are static or dynamic.

Figure 6-4 Assigning IP Addresses

6.4 Static Assignment of an IP

Address Static assignment works best on small, infrequently changing networks. The system administrator manually assigns and tracks IP addresses for each computer, printer, or server on the intranet. Good recordkeeping is critical to prevent problems that occur with duplicate IP addresses. This is possible only when there are a small number of devices to track.



Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically
○ Use the following IP address:
IP address:
Subnet mask:
Default gateway:

● Obtain DNS server address automatically
○ Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:

□ Validate settings upon exit

vEthernet (WAN) Properties

Connect using:
Hyper-V Virtual Ethernet Adapter #2

This connection uses the following items:
☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Netw
☑ QoS Packet Scheduler
☑ Internet Protocol Version 4 (TCP/IPv4)
□ Microsoft Network Adapter Multiplexor Prot
☑ Microsoft LLDP Protocol Driver
☑ Internet Protocol Version 6 (TCP/IPv6)

Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

vEthernet (WAN) Stat
Connection
IPv4 Connectivity:
IPv6 Connectivity:
Media State:
Duration:
Speed:
Activity
Packets:

Figure 6-5 TCP/IP Configuration for Windows

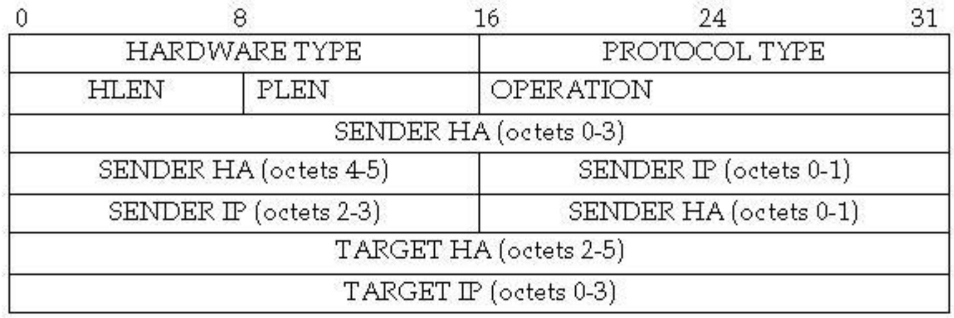
Servers should be assigned a static IP address so workstations and other devices will always know how to access needed services. Consider how difficult it would be to phone a business that changed its phone number every day. Other devices that should be assigned static IP addresses are network printers, application servers, and routers.

6.5 RARP IP Address Assignment

Reverse Address Resolution Protocol (RARP) associates a known MAC address with an IP address. This association allows network devices to encapsulate data before sending the data out on the network. A network device, such as a diskless workstation, might know its MAC address but not its IP address. RARP allows the device to request to learn its IP address. Devices using RARP require that a RARP server be present on the network to answer RARP requests.

Consider an example where a source device wants to send data to another device. In this example, the source device knows its own MAC address but is unable to locate its IP address in the ARP table. The source device must include both its MAC address and IP address for the destination device to retrieve data, pass it to higher layers of the OSI model, and respond to the originating device. Therefore, the source initiates a process called a RARP request. This request helps the source device-detect its IP address.

RARP requests are broadcast onto the LAN and are responded to by the RARP server which is usually a router. RARP uses the same packet format as ARP. However, in a RARP request, the MAC headers and operation code are different from an ARP request.



0 8 16 24 31

<table>
<tr><td colspan="2">HARDWARE TYPE</td><td colspan="2">PROTOCOL TYPE</td></tr>
<tr><td>HLEN</td><td>PLEN</td><td colspan="2">OPERATION</td></tr>
<tr><td colspan="4">SENDER HA (octets 0-3)</td></tr>
<tr><td colspan="2">SENDER HA (octets 4-5)</td><td colspan="2">SENDER IP (octets 0-1)</td></tr>
<tr><td colspan="2">SENDER IP (octets 2-3)</td><td colspan="2">SENDER HA (octets 0-1)</td></tr>
<tr><td colspan="4">TARGET HA (octets 2-5)</td></tr>
<tr><td colspan="4">TARGET IP (octets 0-3)</td></tr>
</table>

Figure 6-6 ARP/RARP Message Structure

The RARP packet format contains places for MAC addresses of both the destination and source devices. The source IP address field is empty. The broadcast goes to all devices on the network. Figure 6-8 Figure 6-9, and depict the destination MAC address as FF:FF:FF:FF:FF: FF. Workstations running RARP have codes in ROM that direct them to start the RARP process. A step-by-step layout of the RARP process is illustrated in Figure 6-7 through Figure 6-14.

- *Hardware Type*: (*16-bits*) - the type of interface the sender seeks an answer for.
- *Protocol Type*: (*16-bits*) - the high-level software address type provided.
- *HLEN*: (*8-bits*) – Hardware address length.
- *PLEN*: (*8-bits*) - Protocol address length.
- *OPERATION*: (*16-bits*) - the specific type of operation requested.
  - 1 ARP.request
  - 2 ARP.response
  - 3 RARP request
  - 4 RARP response
  - 5 Dynamic RARP request
  - 6 Dynamic RARP reply
  - 7 Dynamic RARP error
  - 8 InARP request
  - 9 InARP reply
- *SENDER HA*: (*6-octets*) - the sender's actual hardware address, scalable up to six bytes.
- *SENDER IP*: (*4-octets*) - the sender's IP address, always 32-bits.
- *TARGET HA*: (*6-octets*) - the destination node's hardware address, scalable up to six bytes.
- *TARGET IP*: (*4-octets*) - the destination node's IP address, always 32-bits.

Computer FE:ED:F9:23:44:EF needs to get its IP address for internal operation.

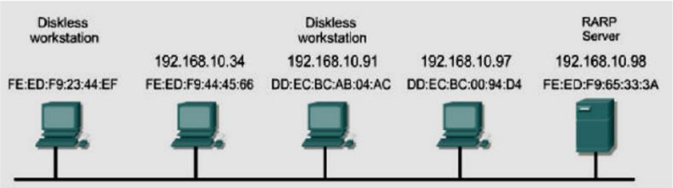
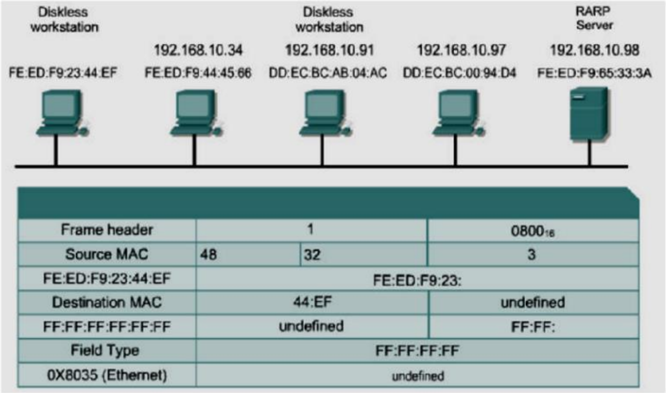


Figure 6-7 RARP: Network Segment

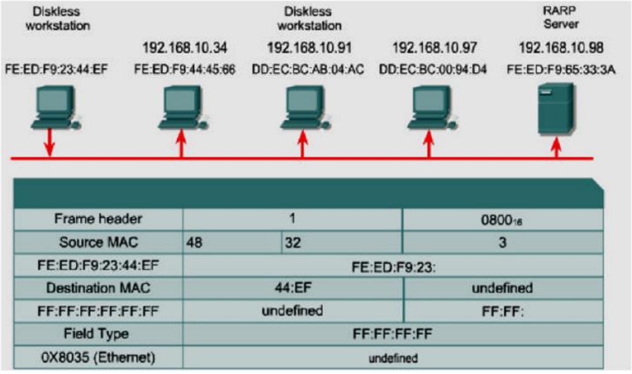
Computer FE:ED:F9:23:44:EF generates a RARP request.



Frame header	1		0800$_{16}$
Source MAC	48	32	3
FE:ED:F9:23:44:EF	FE:ED:F9:23:		
Destination MAC	44:EF		undefined
FF:FF:FF:FF:FF:FF	undefined		FF:FF:
Field Type	FF:FF:FF:FF		
0X8035 (Ethernet)	undefined		

Figure 6-8 RARP: Request Generation

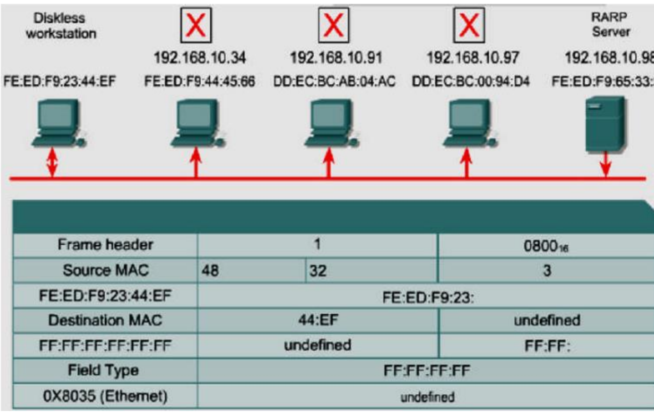
Computer FE:ED:F9:23:44:EF transmits RARP request.



Frame header	1		0800$_{16}$
Source MAC	48	32	3
FE:ED:F9:23:44:EF	FE:ED:F9:23:		
Destination MAC	44:EF		undefined
FF:FF:FF:FF:FF:FF	undefined		FF:FF:
Field Type	FF:FF:FF:FF		
0X8035 (Ethernet)	undefined		

Figure 6-9 RARP: Request Transmission

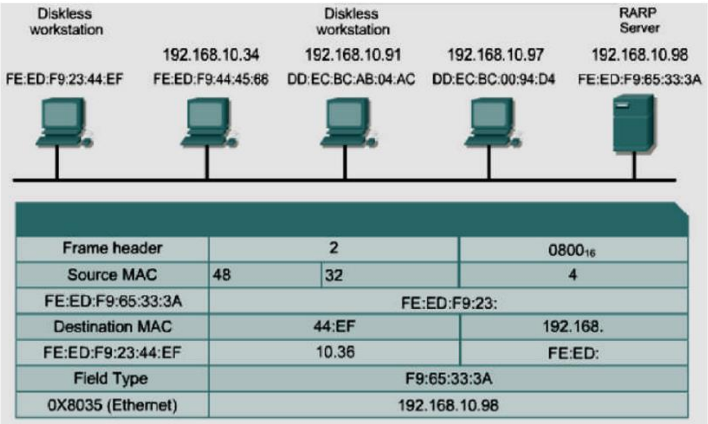
All computers pass the packet up to the network layer. If IP numbers do not match, the packet is discarded except for the RARP server, which detects the RARP request field.



Frame header	1		0800$_{16}$
Source MAC	48	32	3
FE:ED:F9:23:44:EF	FE:ED:F9:23:		
Destination MAC	44:EF		undefined
FF:FF:FF:FF:FF:FF	undefined		FF:FF:
Field Type	FF:FF:FF:FF		
0X8035 (Ethernet)	undefined		

Figure 6-10 RARP: Request Verification

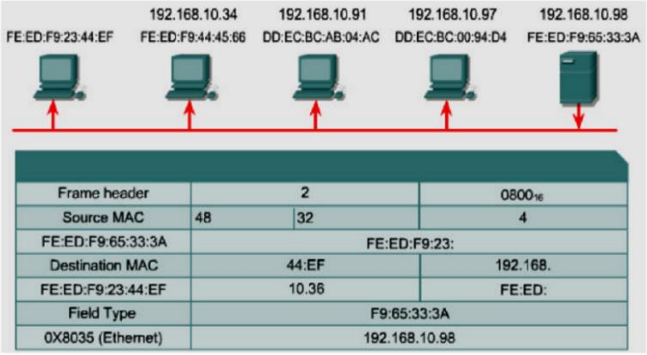
The RARP server creates a RARP reply message for the requesting client.



Frame header	2		0800_{16}
Source MAC	48	32	4
FE:ED:F9:65:33:3A	FE:ED:F9:23:		
Destination MAC	44:EF		192.168.
FE:ED:F9:23:44:EF	10.36		FE:ED:
Field Type	F9:65:33:3A		
0X8035 (Ethernet)	192.168.10.98		

Figure 6-11 RARP: Reply Generation

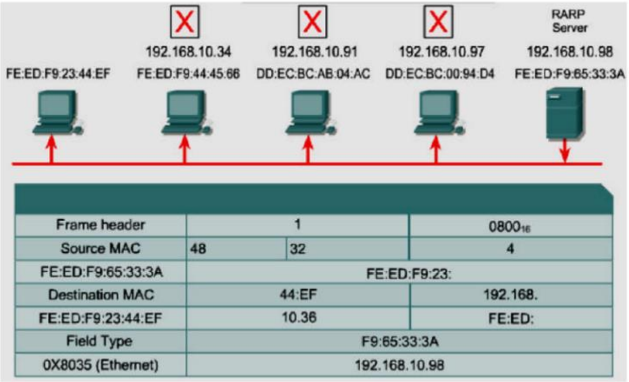
All computers copy the frame and examine it.



Frame header	2		0800_{16}
Source MAC	48	32	4
FE:ED:F9:65:33:3A	FE:ED:F9:23:		
Destination MAC	44:EF		192.168.
FE:ED:F9:23:44:EF	10.36		FE:ED:
Field Type	F9:65:33:3A		
0X8035 (Ethernet)	192.168.10.98		

Figure 6-12 RARP: Reply Transmission

If MAC addresses do not match, the packet is discarded.



Frame header	1		0800_{16}
Source MAC	48	32	4
FE:ED:F9:65:33:3A	FE:ED:F9:23:		
Destination MAC	44:EF		192.168.
FE:ED:F9:23:44:EF	10.36		FE:ED:
Field Type	F9:65:33:3A		
0X8035 (Ethernet)	192.168.10.98		

Figure 6-13 RARP: Reply Evaluation

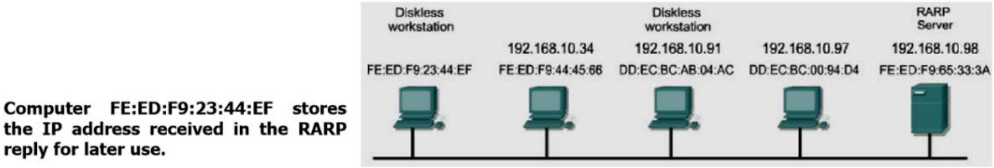
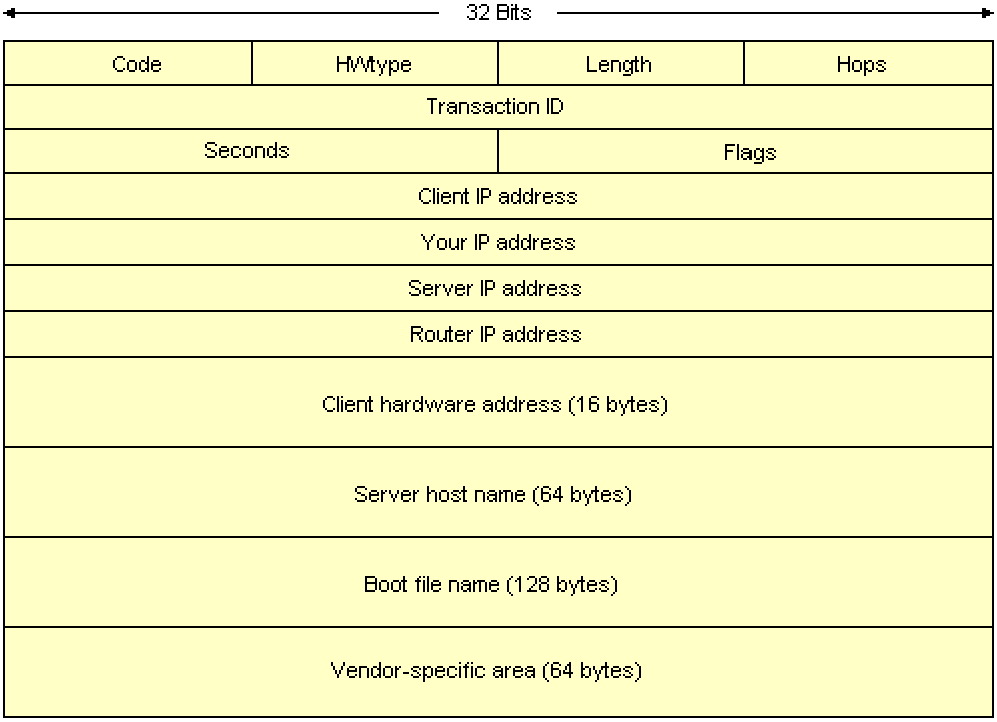

Computer FE:ED:F9:23:44:EF stores the IP address received in the RARP reply for later use.

Figure 6-14 RARP: Data Storage

6.6 BOOTP IP Address

Assignment The bootstrap protocol (BOOTP) operates in a client-server environment and only requires a single packet exchange to obtain IP information. However, unlike RARP, BOOTP packets can include the IP address, as well as the address of a router, the address of a server, and vendor-specific information.


32 Bits

Code	HWtype	Length	Hops
Transaction ID			
Seconds		Flags	
Client IP address			
Your IP address			
Server IP address			
Router IP address			
Client hardware address (16 bytes)			
Server host name (64 bytes)			
Boot file name (128 bytes)			
Vendor-specific area (64 bytes)			

Figure 6-15 BOOTP Message Structure

One problem with BOOTP, however, is that it was not designed to provide a dynamic address assignment. With BOOTP, a network administrator creates a configuration file that specifies the parameters for each device. The administrator must add hosts and maintain the BOOTP database. Even though the addresses are dynamically assigned, there is still a one to one relationship between the number of IP addresses and the number of hosts. This means that for every host on the network there must be a BOOTP profile with an IP address assignment in it. No two profiles can have the same IP address. Those profiles might be used at the same time and that would mean that two hosts have the same IP address.

A description of the BOOTP message fields is given below.

Code - an operation code that specifies the message type (1 = BOOTREQUEST, 2 = BOOTREPLY)

HW:- type - the type of hardware (for example, 1 = Ethernet)

Length - specifies the length of the hardware address in bytes

Hops - set to 0 by the client, and incremented by each router which relays the

Transaction ID - a 32-bit randomly generated number used to match the boot request with the response generated

Seconds - set by the client - the time elapsed in seconds since the client started its boot process

Flags - the first bit of the Flags field is used as a broadcast flag - all other bits are reserved for future use and must be set to zero

Client IP address - set by the client (either its known IP address or 0.0.0.0)

Your IP address - set by the server if the Client IP address field was 0.0.0.0

Server IP address - the IP address of the BOOTP server sending a BOOTREPLY message

Router IP address - set by the forwarding router if BOOTP forwarding is used

Client hardware address - set by the client and used by the server to identify which registered client is booting

Server hostname - optional server hostname (a null-terminated string)

Boot file name - the client leaves this null or specifies a generic name indicating the type of boot file to be used - the server returns the fully qualified filename of a suitable boot file (a null-terminated string)

Vendor-specific Area - optional hardware or vendor-specific configuration information

A device uses BOOTP to obtain an IP address when starting up. BOOTP uses UDP to carry messages. The UDP message is encapsulated in an IP packet. A computer uses BOOTP to send a broadcast IP packet using a destination IP address of all 1s, 255.255.255.255 in dotted decimal notation. A BOOTP server receives the broadcast and then sends back a broadcast. The client receives a frame and checks the MAC address. If the client finds its own MAC address in the destination address field and broadcast in the IP destination field, it takes and stores the IP address and other information supplied in the BOOTP reply message. A step-by-step description of the process is shown in Figures (16) through (23).

Computer FE:ED:F9:23:44:EF needs to obtain its IP address for Internet and Internet operation.

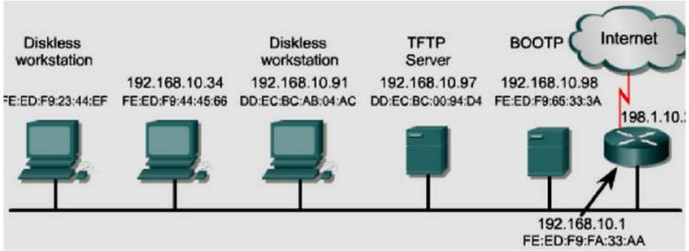
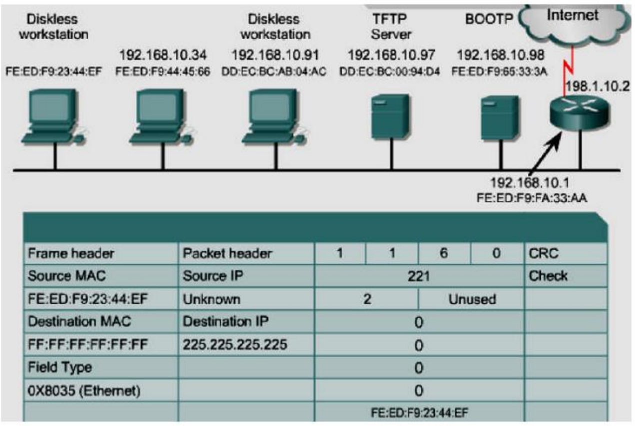


Figure 6-16 BOOTP: Network Segment

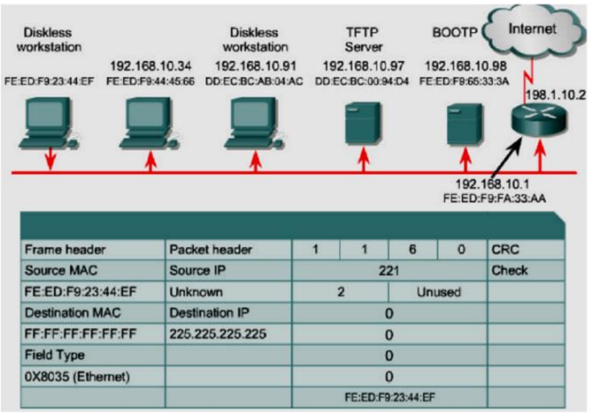
Workstation FE:ED:F9:23:44:EF generates a BOOTP request.



Frame header	Packet header	1	1	6	0	CRC
Source MAC	Source IP	221				Check
FE:ED:F9:23:44:EF	Unknown	2		Unused		
Destination MAC	Destination IP	0				
FF:FF:FF:FF:FF:FF	225.225.225.225	0				
Field Type		0				
0X8035 (Ethernet)		0				
		FE:ED:F9:23:44:EF				

Figure 6-17 BOOTP: Request Creation

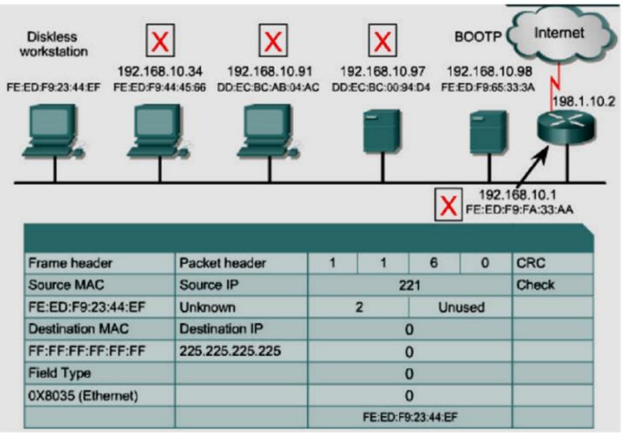
Workstation FE:ED:F9:23:44:EF encapsulates the request in a packet header. The header contains an unknown source IP address and a broadcast destination IP address. For the frame header the workstation uses its MAC address as the source and a broadcast for the destination as it does not know the address of the BOOTP server. The workstation then transmits a BOOTP request frame.



Frame header	Packet header	1	1	6	0	CRC
Source MAC	Source IP	221				Check
FE:ED:F9:23:44:EF	Unknown	2		Unused		
Destination MAC	Destination IP	0				
FF:FF:FF:FF:FF:FF	225.225.225.225	0				
Field Type		0				
0X8035 (Ethernet)		0				
		FE:ED:F9:23:44:EF				

Figure 6-18 BOOTP: Request Transmission

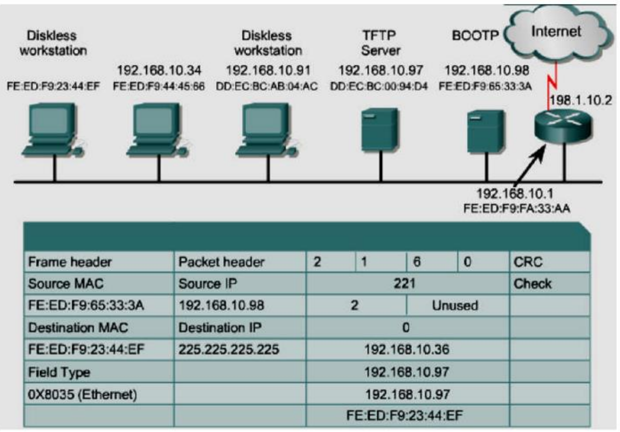
All devices pick up a copy of the frame, detect a broadcast MAC destination, strip off the frame header, and pass the packet up to the network layer. The devices detect that the IP destination is a broadcast IP address, strip off the packet header, and pass the reply data to the transport layer. All of the devices detect the BOOTP request field as being a BOOTP request. All devices except for the BOOTP server discard it.



Frame header	Packet header	1	1	6	0	CRC
Source MAC	Source IP	221				Check
FE:ED:F9:23:44:EF	Unknown	2		Unused		
Destination MAC	Destination IP	0				
FF:FF:FF:FF:FF:FF	225.225.225.225	0				
Field Type		0				
0X8035 (Ethernet)		0				
		FE:ED:F9:23:44:EF				

Figure 6-19 BOOTP: Request Verification

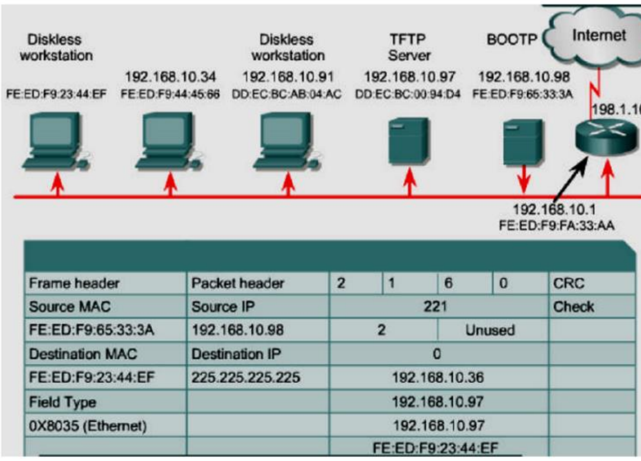
The server prepares a BOOTP response from its database to send back to the requesting device. This includes client IP address. TFTP server address, and default Gateway address (other fields are omitted for this example). In the frame header, source and destination addresses are reversed. In the packet header, the BOOTP server places its IP address in the source field and a broadcast address in the destination field. This is done to get the BOOTP response packet back up to the transport layer to be processed. Only a broadcast will be passed since the client still does not know its IP address.



Frame header	Packet header	2	1	6	0	CRC
Source MAC	Source IP	221				Check
FE:ED:F9:65:33:3A	192.168.10.98	2		Unused		
Destination MAC	Destination IP	0				
FE:ED:F9:23:44:EF	225.225.225.225	192.168.10.36				
Field Type		192.168.10.97				
0X8035 (Ethernet)		192.168.10.97				
		FE:ED:F9:23:44:EF				

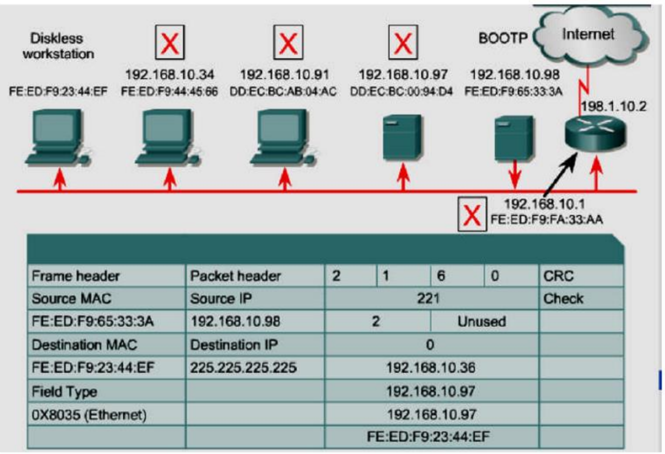
Figure 6-20 BOOTP: Reply Creation

The BOOTP server then sends the BOOTP reply frame back to the requesting device. All devices pick up the packet and examine it.



Frame header	Packet header	2	1	6	0	CRC
Source MAC	Source IP	221				Check
FE:ED:F9:65:33:3A	192.168.10.98	2		Unused		
Destination MAC	Destination IP	0				
FE:ED:F9:23:44:EF	225.225.225.225	192.168.10.36				
Field Type		192.168.10.97				
0X8035 (Ethernet)		192.168.10.97				
		FE:ED:F9:23:44:EF				

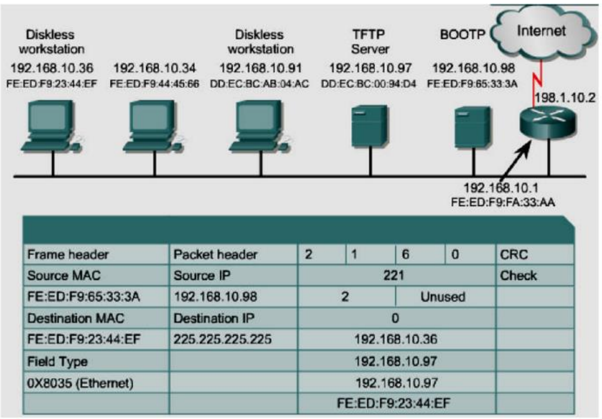
Figure 6-21 BOOTP: Reply Transmission



Frame header	Packet header	2	1	6	0	CRC
Source MAC	Source IP	221				Check
FE:ED:F9:65:33:3A	192.168.10.98	2		Unused		
Destination MAC	Destination IP	0				
FE:ED:F9:23:44:EF	225.225.225.225	192.168.10.36				
Field Type		192.168.10.97				
0X8035 (Ethernet)		192.168.10.97				
		FE:ED:F9:23:44:EF				

The destination MAC address is not theirs and not a broadcast, so they discard the packet. The MAC address is matched on the requesting client device, so the source IP and MAC address of the BOOTP server are stored in the ARP table of the diskless workstation. The frame header is stripped off and discarded.

Figure 6-22 BOOTP: Reply Verified



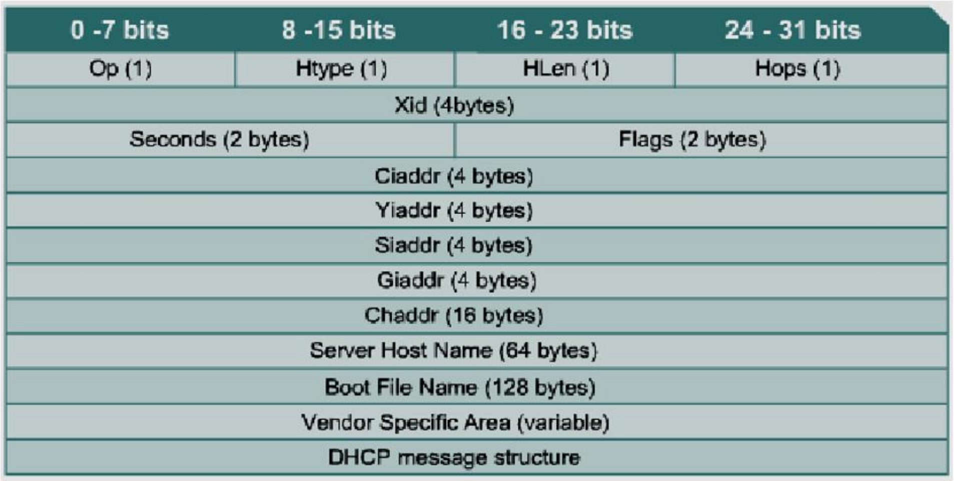
Frame header	Packet header	2	1	6	0	CRC
Source MAC	Source IP	221				Check
FE:ED:F9:65:33:3A	192.168.10.98	2		Unused		
Destination MAC	Destination IP	0				
FE:ED:F9:23:44:EF	225.225.225.225	192.168.10.36				
Field Type		192.168.10.97				
0X8035 (Ethernet)		192.168.10.97				
		FE:ED:F9:23:44:EF				

The packet destination IP is a broadcast, so the packet header is stripped off and the BOOTP reply data is passed up to the transport layer, where the OP field data says that this is a BOOTP reply. The reply data is stored in the appropriate memory locations in the workstation. The workstation now has access to the TFTP server for further operating system downloads and to the default Gateway as well as having its own IP address. It can now fully function on the network and the Internet.

Figure 6-23 BOOTP: Data Storage

6.7 DHCP IP Address Management

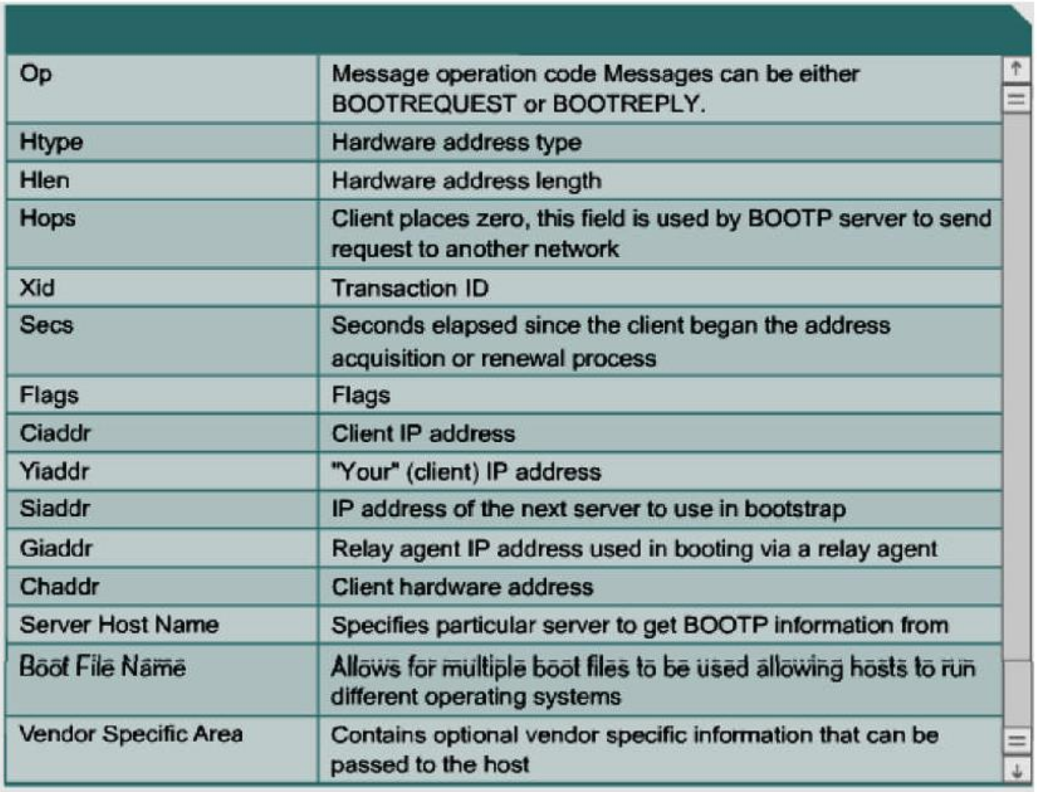
Dynamic host configuration protocol (DHCP) is the successor to BOOTP. Unlike BOOTP, DHCP allows a host to obtain an IP address dynamically without the network administrator having to set up an individual profile for each device. All that is required when using DHCP is a defined range of IP addresses on a DHCP server. As hosts come online, they contact the DHCP server and request an address. The DHCP server chooses an address and leases it to that host. With DHCP, the entire network configuration of a computer can be obtained in one message. This includes all of the data supplied by the BOOTP message, plus a leased IP address and a subnet mask.



0 -7 bits	8 -15 bits	16 - 23 bits	24 - 31 bits
Op (1)	Htype (1)	HLen (1)	Hops (1)
Xid (4bytes)			
Seconds (2 bytes)		Flags (2 bytes)	
Ciaddr (4 bytes)			
Yiaddr (4 bytes)			
Siaddr (4 bytes)			
Giaddr (4 bytes)			
Chaddr (16 bytes)			
Server Host Name (64 bytes)			
Boot File Name (128 bytes)			
Vendor Specific Area (variable)			
DHCP message structure			

Figure 6-24 DHCP Message Structure

The major advantage that DHCP has over BOOTP is that it allows users to be mobile. This mobility allows users to freely change network connections from location to location. It is no longer required to keep a fixed profile for every device attached to the network as was required with the BOOTP system. The importance of this DHCP advancement is its ability to lease an IP address to a device and then reclaim that IP address for another user after the first user releases it. This means that DHCP offers a one to many ratios of IP addresses and that an address is available to anyone who connects to the network. A step-by-step description of the process is shown in Figures (26) through (40).



Op	Message operation code Messages can be either BOOTREQUEST or BOOTREPLY.
Htype	Hardware address type
Hlen	Hardware address length
Hops	Client places zero, this field is used by BOOTP server to send request to another network
Xid	Transaction ID
Secs	Seconds elapsed since the client began the address acquisition or renewal process
Flags	Flags
Ciaddr	Client IP address
Yiaddr	"Your" (client) IP address
Siaddr	IP address of the next server to use in bootstrap
Giaddr	Relay agent IP address used in booting via a relay agent
Chaddr	Client hardware address
Server Host Name	Specifies particular server to get BOOTP information from
Boot File Name	Allows for multiple boot files to be used allowing hosts to run different operating systems
Vendor Specific Area	Contains optional vendor specific information that can be passed to the host

Figure 6-25 DHCP Message Structure Field Descriptions

Laptop AA:EC:F9:23:44:19 is connected to the network.

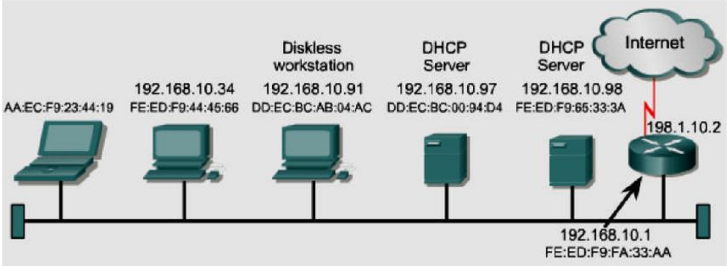
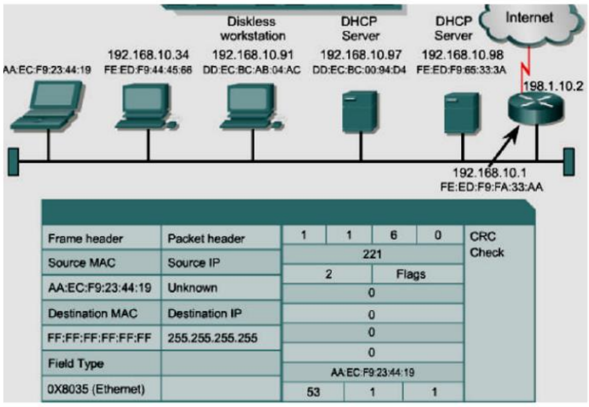


Figure 6-26 DHCP: Host Boots

Laptop AA:EC:F9:23:44:19 generates a DHCP request.

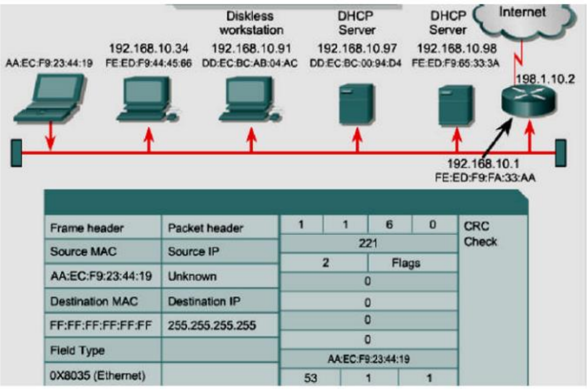


Frame header	Packet header
Source MAC	Source IP
AA:EC:F9:23:44:19	Unknown
Destination MAC	Destination IP
FF:FF:FF:FF:FF:FF	255.255.255.255
Field Type	
0X8035 (Ethernet)	

1	1	6	0	CRC Check
221				
2	Flags			
0				
0				
0				
0				
AA:EC:F9:23:44:19				
53	1	1		

Figure 6-27 DHCP: Message Structure Field Descriptions

The DHCP request is transmitted by the laptop computer.

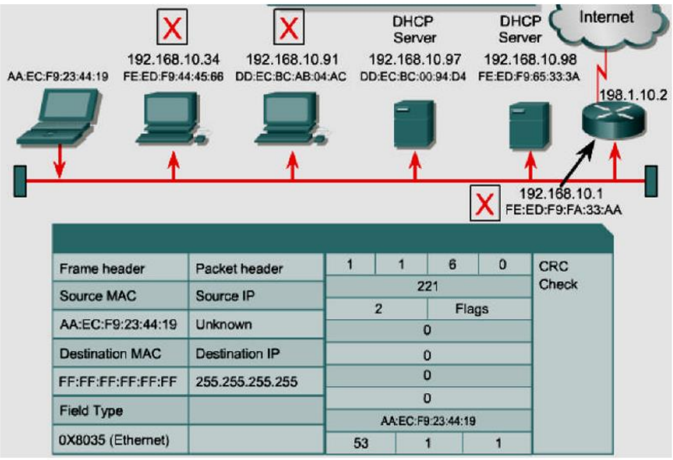


Frame header	Packet header
Source MAC	Source IP
AA:EC:F9:23:44:19	Unknown
Destination MAC	Destination IP
FF:FF:FF:FF:FF:FF	255.255.255.255
Field Type	
0X8035 (Ethernet)	

1	1	6	0	CRC Check
221				
2	Flags			
0				
0				
0				
0				
AA:EC:F9:23:44:19				
53	1	1		

Figure 6-28 DHCP: Request Transmitted

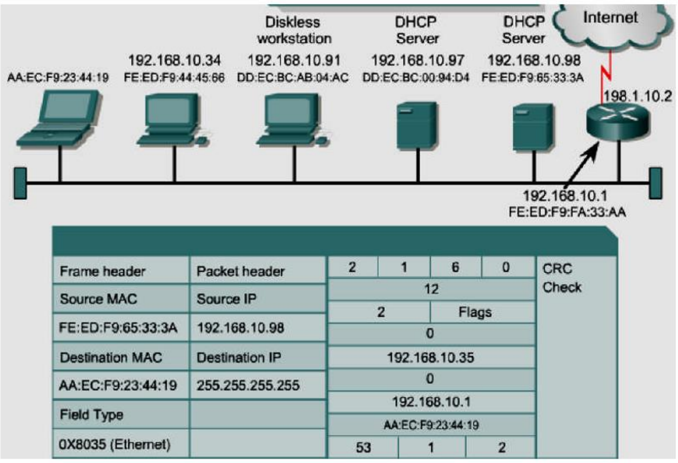
All devices pick up a copy of the frame, detect a broadcast MAC destination, strip off the frame header, and pass the packet up to the network layer. The devices detect that the IP destination is a broadcast IP address, strip off the packet header, and pass the reply data to the transport layer. All of the devices detect the DHCP request field as being a DHCP request. All devices except for the DHCP servers discard the request.



Frame header	Packet header	1 1 6 0	CRC Check
Source MAC	Source IP	221 2 Flags	
AA:EC:F9:23:44:19	Unknown	0	
Destination MAC	Destination IP	0	
FF:FF:FF:FF:FF:FF	255.255.255.255	0	
Field Type		0	
0X8035 (Ethernet)		AA:EC:F9:23:44:19 53 1 1	

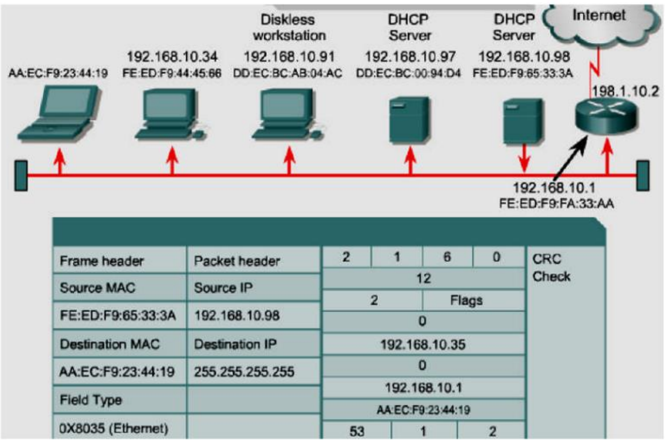
Figure 6-29 DHCP: Request Evaluated

The server prepares a DHCP offer to send back to the requesting device. This includes client IP address. DHCP server address, and default Gateway address. In the frame header, source and destination addresses are reversed. In the packet header, the DHCP server places its IP address in the source field and a broadcast address in the destination field. This is done to get the DHCP response packet back up to the transport layer to be processed. Only a broadcast will be passed since the client still does not know its IP address.



Frame header	Packet header	2 1 6 0	CRC Check
Source MAC	Source IP	12 2 Flags	
FE:ED:F9:65:33:3A	192.168.10.98	0	
Destination MAC	Destination IP	192.168.10.35	
AA:EC:F9:23:44:19	255.255.255.255	0	
Field Type		192.168.10.1	
0X8035 (Ethernet)		AA:EC:F9:23:44:19 53 1 2	

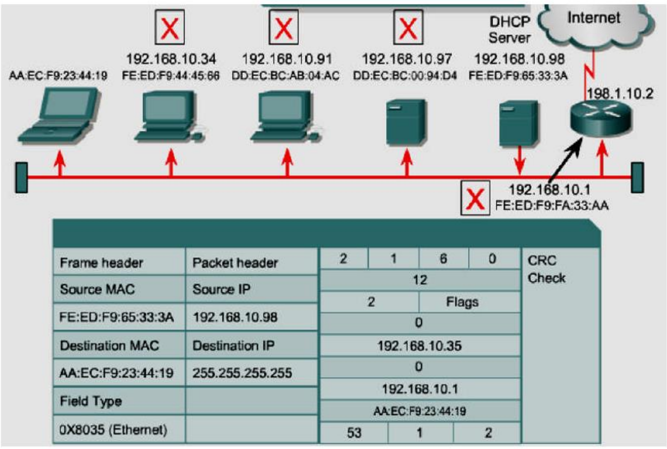
Figure 6-30 DHCP: Offer Prepared



Frame header	Packet header	2 1 6 0	CRC Check
Source MAC	Source IP	12	
		2 Flags	
FE:ED:F9:65:33:3A	192.168.10.98	0	
Destination MAC	Destination IP	192.168.10.35	
AA:EC:F9:23:44:19	255.255.255.255	0	
Field Type		192.168.10.1	
		AA:EC:F9:23:44:19	
0X8035 (Ethernet)		53 1 2	

The DHCP server sends the DHCP reply frame back to the requesting device. All devices pick up the packet and examine it.

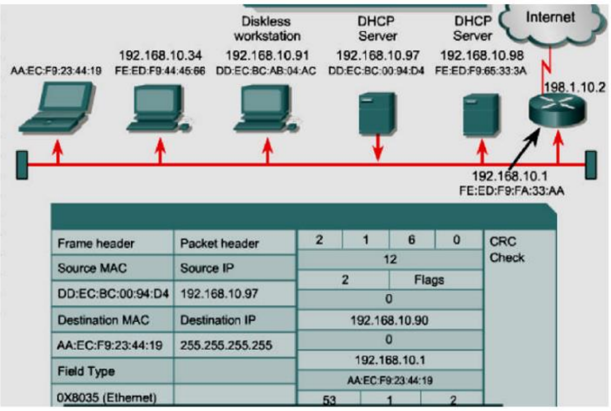
Figure 6-31 DHCP: Offer Transmitted



Frame header	Packet header	2 1 6 0	CRC Check
Source MAC	Source IP	12	
		2 Flags	
FE:ED:F9:65:33:3A	192.168.10.98	0	
Destination MAC	Destination IP	192.168.10.35	
AA:EC:F9:23:44:19	255.255.255.255	0	
Field Type		192.168.10.1	
		AA:EC:F9:23:44:19	
0X8035 (Ethernet)		53 1 2	

The destination MAC address is not theirs and not a broadcast, so they discard the packet. The MAC address is matched on the requesting client device, and so the source IP and MAC address of the DHCP server are stored in the ARP table of the laptop. The frame header is stripped off and discarded.

Figure 6-32 DHCP: Offer Evaluated



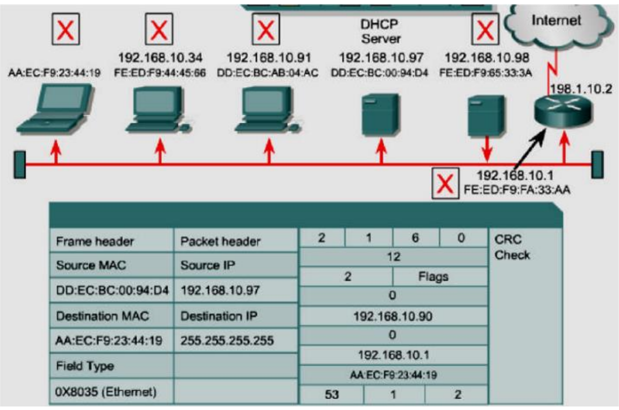
Frame header	Packet header
Source MAC	Source IP
DD:EC:BC:00:94:D4	192.168.10.97
Destination MAC	Destination IP
AA:EC:F9:23:44:19	255.255.255.255
Field Type	
0X8035 (Ethernet)	

2 1 6 0
12
2 Flags
0
192.168.10.90
0
192.168.10.1
AA:EC:F9:23:44:19
53 1 2

CRC Check

The second DHCP server sends the DHCP reply frame back to the requesting device. All devices pick up the packet and examine it.

Figure 6-33 DHCP: Offer Transmitted



Frame header	Packet header
Source MAC	Source IP
DD:EC:BC:00:94:D4	192.168.10.97
Destination MAC	Destination IP
AA:EC:F9:23:44:19	255.255.255.255
Field Type	
0X8035 (Ethernet)	

2 1 6 0
12
2 Flags
0
192.168.10.90
0
192.168.10.1
AA:EC:F9:23:44:19
53 1 2

CRC Check

The destination MAC address is not theirs and not a broadcast, so they discard the packet. The MAC address is matched on the requesting client device, and so the source IP and MAC address of the DHCP server are stored in the ARP table of the laptop. The frame header is stripped off and discarded. Since the laptop has already received a DHCP offer from another server, this offer is discarded.

Figure 6-34 DHCP: Offer Evaluated

The laptop computer now sends a DHCP request addressed to the specific DHCP server that sent the accepted offer.

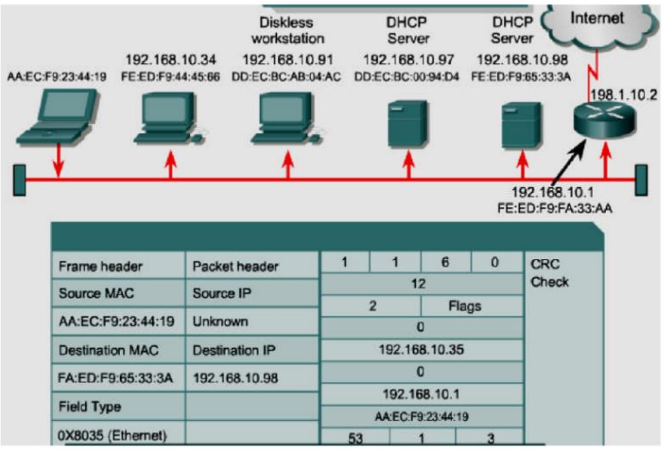


Figure 6-35 DHCP: Request Generated

All devices pick up a copy of the frame and compare the MAC destination to their own. If there is no match, the devices discard the frame.

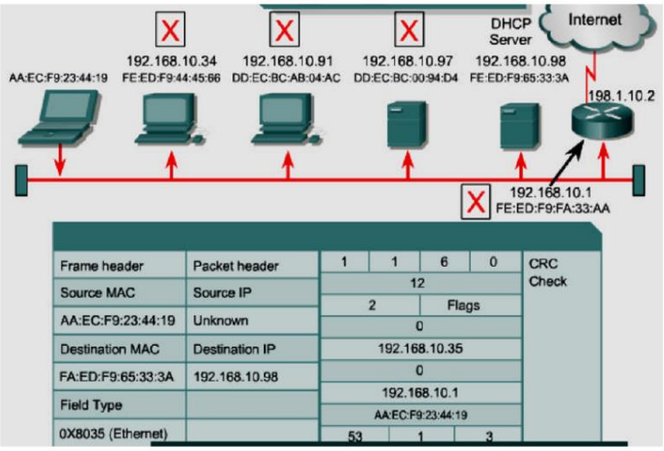
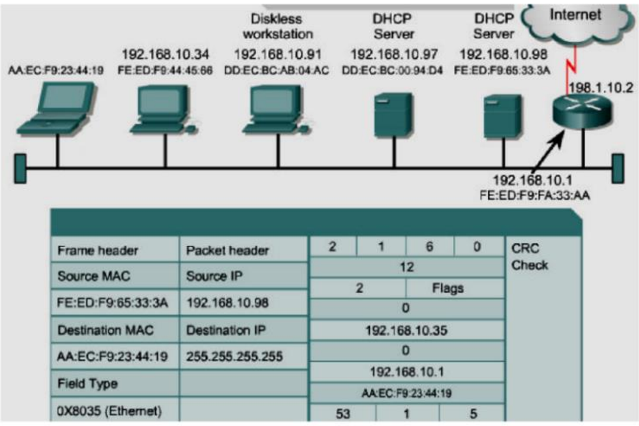


Figure 6-36 DHCP: Request Transmitted

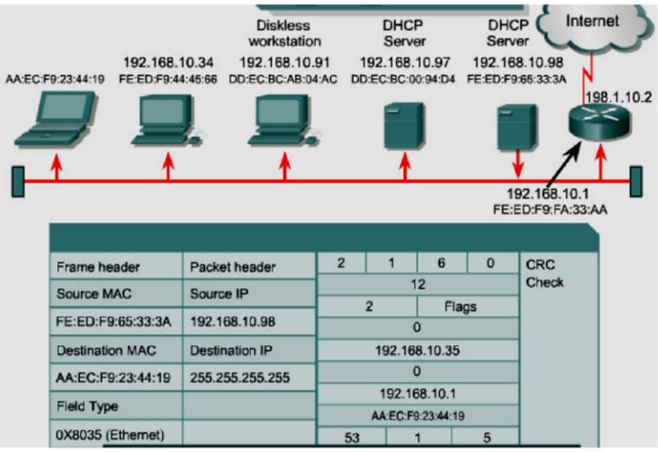
The DHCP selected server creates a DHCPACK.



Frame header	Packet header	2 1 6 0	CRC Check
Source MAC	Source IP	12	
		2 Flags	
FE:ED:F9:65:33:3A	192.168.10.98	0	
Destination MAC	Destination IP	192.168.10.35	
AA:EC:F9:23:44:19	255.255.255.255	0	
Field Type		192.168.10.1	
		AA:EC:F9:23:44:19	
0X8035 (Ethernet)		53 1 5	

Figure 6-37 DHCP: DHCPACK Created

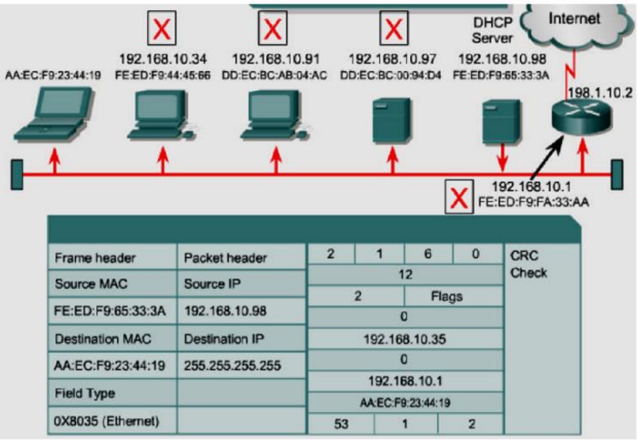
The DHCP server sends the DHCPACK frame back to the requesting device. All devices pick up the packet and examine it.



Frame header	Packet header	2 1 6 0	CRC Check
Source MAC	Source IP	12	
		2 Flags	
FE:ED:F9:65:33:3A	192.168.10.98	0	
Destination MAC	Destination IP	192.168.10.35	
AA:EC:F9:23:44:19	255.255.255.255	0	
Field Type		192.168.10.1	
		AA:EC:F9:23:44:19	
0X8035 (Ethernet)		53 1 5	

Figure 6-38 DHCP: DHCPACK Transmitted

The destination MAC address is not theirs and not a broadcast, so they discard the packet. The MAC address is matched on the requesting client device, and so the source IP and MAC address of the DHCP server are stored in the ARP table of the laptop. The frame header is stripped off and discarded.



Frame header	Packet header	2 | 1 | 6 | 0	CRC Check
Source MAC	Source IP	12 2 | Flags	
FE:ED:F9:65:33:3A	192.168.10.98	0	
Destination MAC	Destination IP	192.168.10.35	
AA:EC:F9:23:44:19	255.255.255.255	0 192.168.10.1	
Field Type		AA:EC:F9:23:44:19	
0X8035 (Ethernet)		53 | 1 | 2	

Figure 6-39 DHCP: DHCPACK Evaluated

The laptop computer now goes into the bound mode and starts to use the assigned IP address and other data passed with the DHCP offer message.

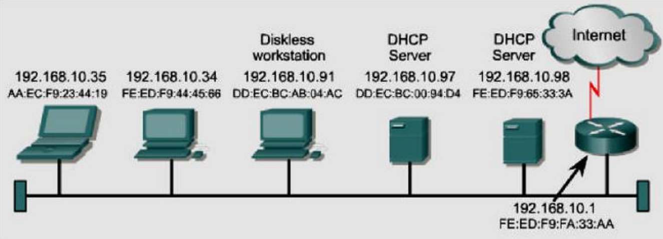
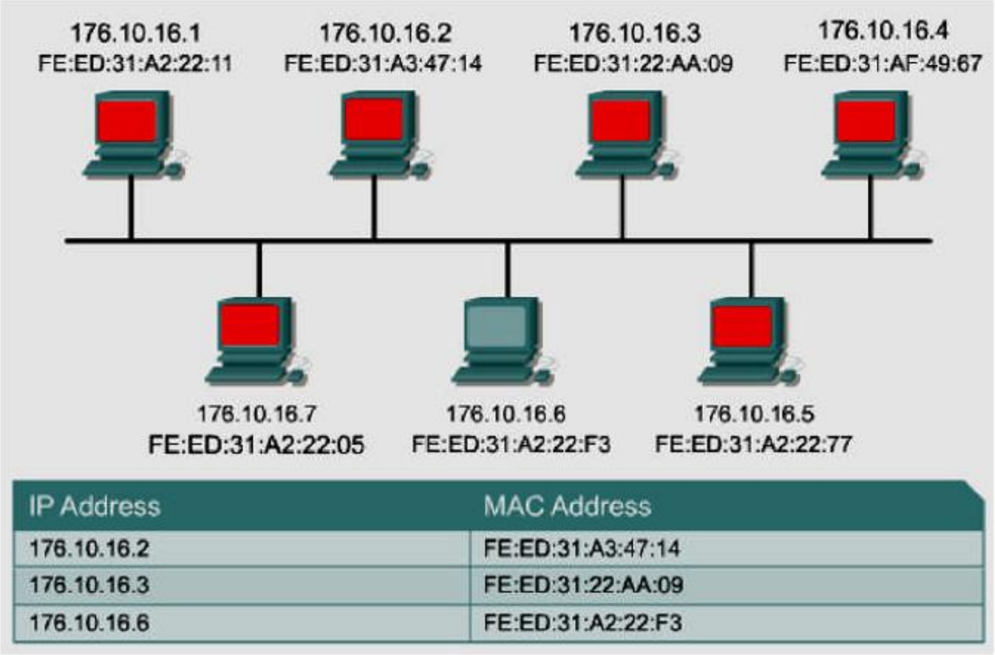


Figure 6-40 DHCP: DHCPACK Created

6.8 Problems in Address Resolution

One of the major problems in networking is how to communicate with other network devices.



IP Address	MAC Address
176.10.16.2	FE:ED:31:A3:47:14
176.10.16.3	FE:ED:31:22:AA:09
176.10.16.6	FE:ED:31:A2:22:F3

Figure 6-41 LAN Transmission Address Resolution Issues

- Computer 176.10.16.1 is monitoring the Ethernet segment to update its ARP table with IP-MAC address pairs so that it can send data to other hosts on the LAN.
- Computer 176.10.16.2 prepares the data for transmission. To do that it checks the network cable to see if another computer is using it. If another station is using the cable, computer 176.10.16.2 will have to wait, as only one computer can transmit at a time. The cable is clear so computer 176.10.16.2 can transmit.
- Computer 176.10.16.2 transmits the data frames through the network cable segment.
- All computers on the Ethernet segment analyze the incoming data frames to determine if the transmission is for them. Part of this process adds the IP-MAC source addresses to the ARP

table. All devices except the one that the data was sent discard the data frame.

- Computer 176.10.16.3 prepares the data for transmission. It follows all the preparation steps.
- Computer 176.10.16.3 transmits its data frames through the Ethernet segment.
- Again all hosts on the segment analyze the incoming frames. Adding data to their ARP tables and discarding the frame if they were not the specified destination of the data.
- Computer 176.10.16.6 prepares the data for transmission.
- Computer 176.10.16.6 transmits its data frames through the Ethernet segment.
- All hosts on the segment analyze the incoming frames. They add data to their ARP tables and discard the frames if they were not the specified destination of the data. This shows the automatic process that is used on a normal Ethernet LAN for maintaining address associations.
- Computer 176.10.16.1 wants to send data to 176.10.16.4. It has its IP address, but data transmission also requires the MAC address of 176.10.16.4. How does it get that MAC address to perform the data transmission?

In TCP/IP communications, a datagram on a LAN must contain both a destination MAC address and a destination IP address. These addresses must be correct and match the destination MAC and IP addresses of the host device. If it does not match, the datagram will be discarded by the destination host. Communications within a LAN segment require two addresses. There needs to be a way to automatically map IP to

MAC addresses. It would be too time-consuming for the user to create the maps manually. The TCP/IP suite has a protocol, called Address Resolution Protocol (ARP), which can automatically obtain MAC addresses for local transmission. Different issues are raised when data is sent outside of the local area network.

Computer 192.168.10.34 needs to communicate with computer 192.168.1.1. How does it get the MAC address for 192.168.1.1, and would it do any good if it was able to get the MAC address? Remember that MAC addresses are only useful in a LAN. They will not be any help outside of the 192.168.10.0 network. So the MAC address of the router is needed to get the data out of the LAN and on to the WAN system.

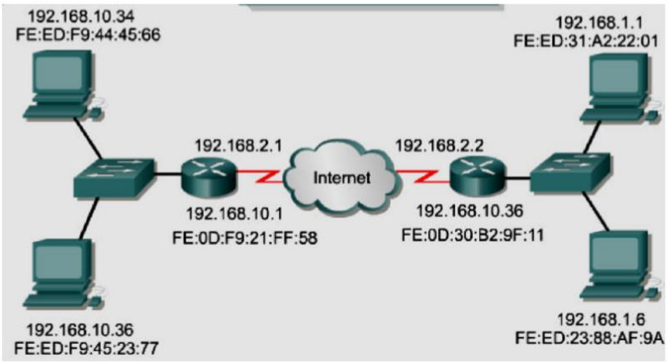
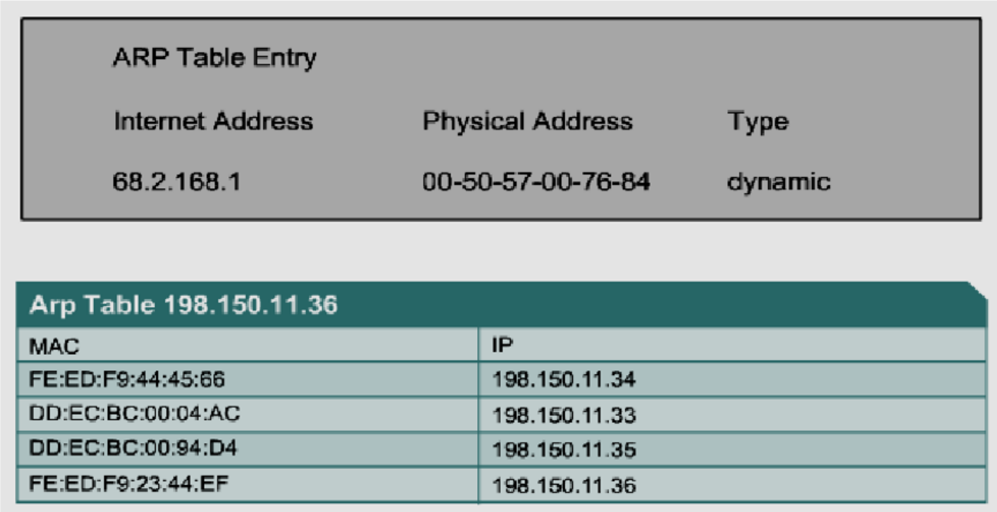


Figure 6-42 Non-Local Address Resolution Issues

Communications between two LAN segments have an additional task. Both the IP and MAC addresses are needed for both the destination host and the intermediate routing device. TCP/IP has a variation on ARP called Proxy ARP that will provide the MAC address of an intermediate device for transmission outside the LAN to another network segment.

6.9 Address Resolution Protocol (ARP)

With TCP/IP networking, a data packet must contain both a destination MAC address and a destination IP address. If the packet is missing either one, the data will not pass from Layer 3 to the upper layers. In this way, MAC addresses and IP addresses act as checks and balances for each other. After devices determine the IP addresses of the destination devices, they can add the destination MAC addresses to the data packets. Some devices will keep tables that contain MAC addresses and IP addresses of other devices that are connected to the same LAN. These are called Address Resolution Protocol (ARP) tables. ARP tables are stored in RAM, where the cached information is maintained automatically on each of the devices. It is very unusual for a user to have to make an ARP table entry manually. Each device on a network maintains its own ARP table. When a network device wants to send data across the network, it uses information provided by the ARP table. When a source determines the IP address for a destination, it then consults the ARP table to locate the MAC address for the destination. If the source locates an entry in its table, the destination IP address to destination MAC address, it will associate the IP address to the MAC address and then uses it to encapsulate the data. The data packet is then sent out over the networking media to be picked up by the destination device.



ARP Table Entry

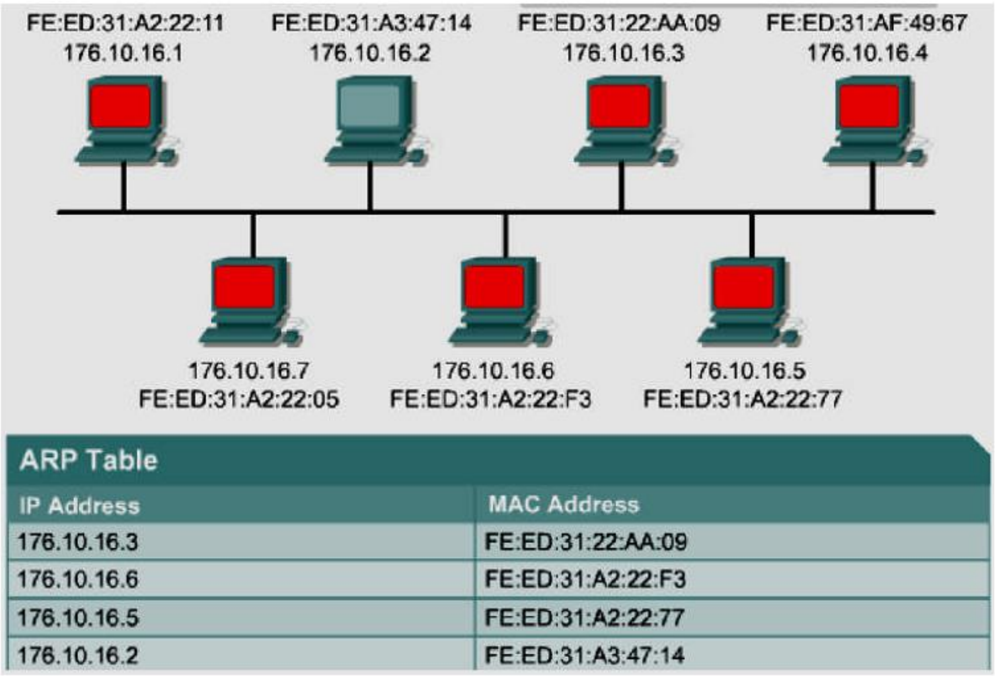
Internet Address	Physical Address	Type
68.2.168.1	00-50-57-00-76-84	dynamic

Arp Table 198.150.11.36

MAC	IP
FE:ED:F9:44:45:66	198.150.11.34
DD:EC:BC:00:04:AC	198.150.11.33
DD:EC:BC:00:94:D4	198.150.11.35
FE:ED:F9:23:44:EF	198.150.11.36

Figure 6-43 ARP Table Entry

There are two ways that devices can gather MAC addresses that they need to add to the encapsulated data. One way is to monitor the traffic that occurs on the local network segment. All stations on an Ethernet network will analyze all traffic to determine if the data is for them. Part of this process is to record the source IP and MAC address of the datagram to an ARP table. So as data is transmitted on the network, the address pairs populate the ARP table. Another way to get an address pair for data transmission is to broadcast an ARP request.



ARP Table

IP Address	MAC Address
176.10.16.3	FE:ED:31:22:AA:09
176.10.16.6	FE:ED:31:A2:22:F3
176.10.16.5	FE:ED:31:A2:22:77
176.10.16.2	FE:ED:31:A3:47:14

Figure 6-44ARP Table Functions

- Computer 176.10.16.1 is monitoring the Ethernet segment to update its ARP table.
- Computer 176.10.16.2 prepares the data for transmission. To do that it checks the network cable to see if another computer is using it. If another station is

using the cable, computer 176.10.16.2 will have to wait, as only one computer can transmit at a time. The cable is clear so computer 176.10.16.2 can transmit.

- Computer 176.10.16.2 transmits the data frames through the network cable segment.
- All computers on the Ethernet segment analyze the incoming data frames to determine if the transmission is for them. Part of this process is to add the IP-MAC source addresses from the data to the ARP table.
- Computer 176.10.16.3 prepares the data for transmission. It follows all the preparation steps.
- Computer 176.10.16.3 transmits its data frames through the Ethernet segment.
- Again all hosts on the segment analyze the incoming frames and add data to their ARP tables.
- Computer 176.10.16.6 prepares the data for transmission.
- Computer 176.10.16.6 transmits its data frames through the Ethernet segment.
- All hosts on the segment analyze the incoming frames.
- Computer 176.10.16.5 prepares the data for transmission. Notice the first pair in the ARP table, it is reaching its timeout value. If a computer does not transmit data for a certain length of time, their IPMAC pair is dropped from the ARP table.
- Computer 176.10.16.3 transmits its data frames through the Ethernet segment. The first value in the ARP table exceeded the timeout value so it is removed. The ARP

table is dynamically updated. It adds and removes entire based on segment activity and timeout values.

- Again all hosts on the segment analyze the incoming frames. New values are added to the ARP table.
- Computer 176.10.16.2 prepares the data for transmission.
- Computer 176.10.16.1 transmits the data frames through the network cable segment.
- All computers on the Ethernet segment analyze the incoming data frames to determine if the transmission is for them. The IP-MAC pair for 176.10.16.2 is added back into the table. If this transmission had come before the timeout value was exceeded, the pair would not have been removed from the table, the timeout value would have just been reset.

The computer that requires an IP and MAC address pair broadcasts an ARP request. All the other devices on the LAN analyze this request. If one of the local devices matches the IP address of the request, it sends back an ARP reply that contains its IP-MAC pair. If the IP address is for the LAN and the computer does not exist or is turned off, there is no response to the ARP request. In this situation, the source device reports an error. If the request is for a different IP network, there is another process that can be used.

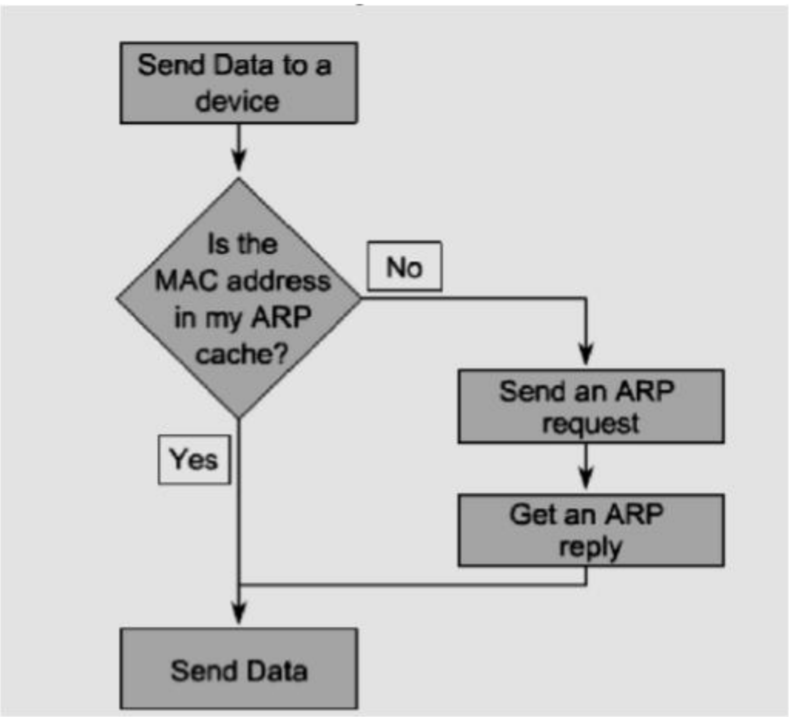
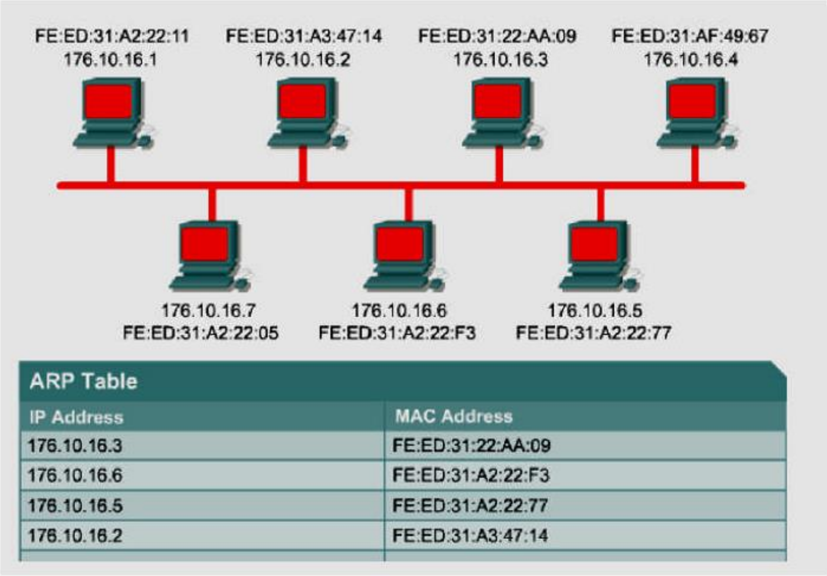


Figure 6-45 The ARP Process



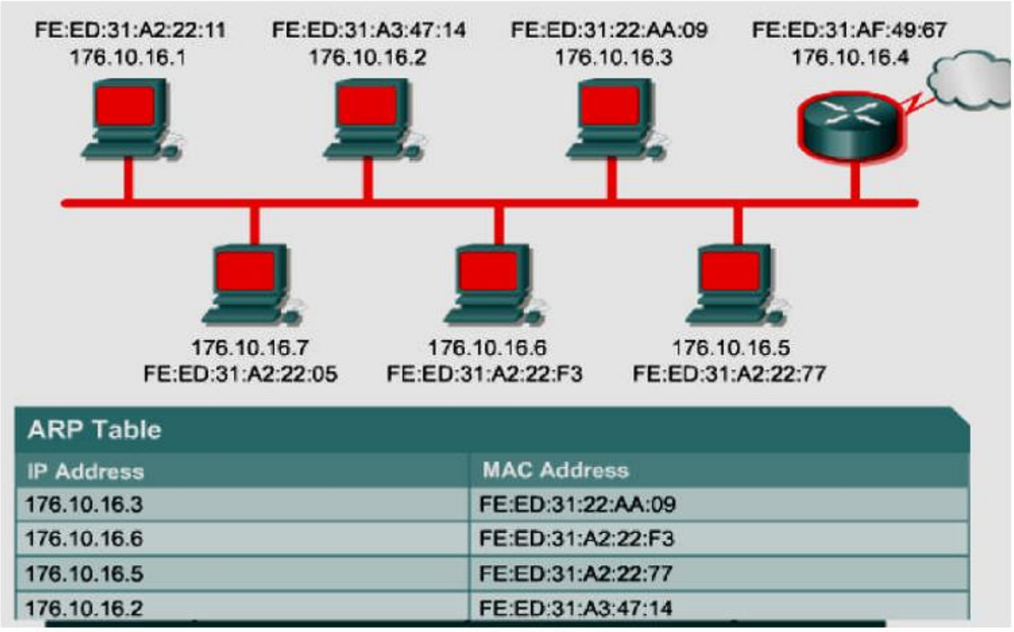
ARP Table

IP Address	MAC Address
176.10.16.3	FE:ED:31:22:AA:09
176.10.16.6	FE:ED:31:A2:22:F3
176.10.16.5	FE:ED:31:A2:22:77
176.10.16.2	FE:ED:31:A3:47:14

Figure 6-46ARP Request

- Computer 176.10.16.1 needs to send a data transmission to the computer 176.10.16.4.
- Computer 176.10.16.1 prepares the data for transmission to computer 176.10.16.4. As it is building the frame for transmission. It finds that the IP-MAC pair for 176.10.16.4 is not in its ARP table. Computer 176.10.16.1 needs this pair, so it must do an ARP request to get it.
- Computer 176.10.16.1 discards the process of encapsulation for the data transmission and instead creates an ARP request to get the MAC address of computer 176.10.16.4.
- Computer 176.10.16.1 transmits the data frames through the network cable segment.
- All computers on the Ethernet segment analyze the incoming data frames to determine if the transmission is for them.
- All computers except computer 176.10.16.4 drop the frames because they do not match the destination IP address of the incoming frames.
- Computer 176.10.16.4 prepares the ARP reply data for transmission.
- Computer 176.10.16.4 transmits its data frames through the Ethernet segment.
- Again all hosts on the segment analyze the incoming frames and add data to their ARP tables.
- Computer 176.10.16.1 prepares the data for transmission.

- Computer 176.10.16.1 transmits its data frames through the Ethernet segment.
- All hosts on the segment analyze the incoming frames.
- All computers except computer 176.10.16.4 drop the frames because they do not match the destination MAC address of the incoming frames.
- Computer 176.10.16.2 prepares the data for transmission.
- Computer 176.10.16.4 processes data transmission.



ARP Table

IP Address	MAC Address
176.10.16.3	FE:ED:31:22:AA:09
176.10.16.6	FE:ED:31:A2:22:F3
176.10.16.5	FE:ED:31:A2:22:77
176.10.16.2	FE:ED:31:A3:47:14

Figure 6-47 Proxy ARP Request

- Computer 176.10.16.1 needs to send a data transmission to the computer 176.10.16.4.
- Computer 176.10.16.1 prepares the data for transmission to computer 176.10.16.4. As it is building the frame for

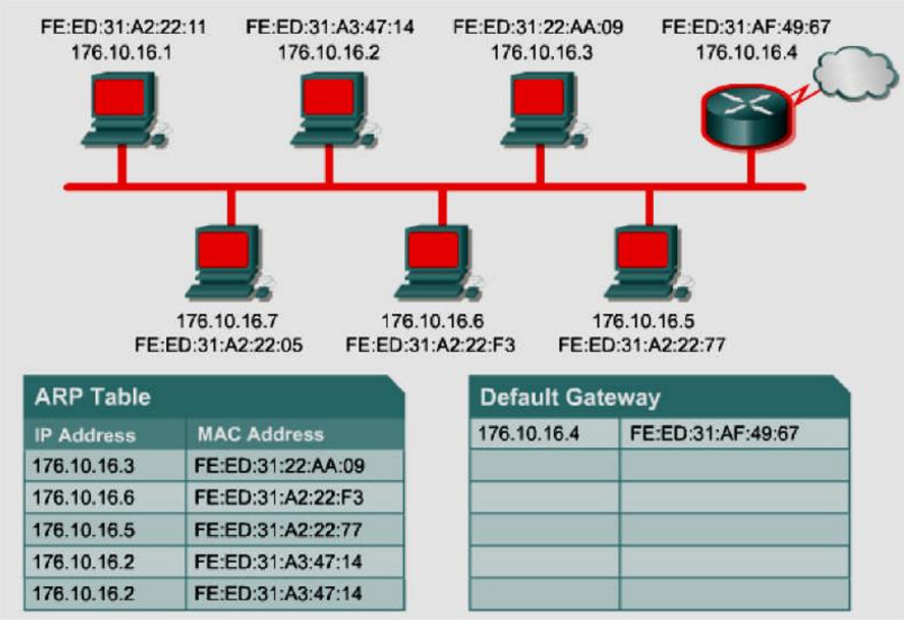
transmission. It finds that the IP-MAC pair for 176.10.16.4 is not in its ARP table. Computer 176.10.16.1 needs this pair, so it must do an ARP request to get it.

- Computer 176.10.16.1 discards the process of encapsulation for the data transmission and instead creates an ARP request to get the MAC address of computer 176.10.16.4.
- Computer 176.10.16.1 transmits the data frames through the network cable segment.
- All computers on the Ethernet segment analyze the incoming data frames to determine if the transmission is for them.
- All devices except router 176.10.16.4 drop the frames because they do not match the destination IP address of the incoming frames.
- Router 176.10.16.4 compares the address with its Ethernet interface IP address. The calculation reveals that this packet is going outside of the LAN. Since this router has proxy ARP enabled, it prepares an ARP reply to the requesting host with its MAC address and the IP address of the destination device.
- Router 176.10.16.4 transmits its data frames through the Ethernet segment.
- Again all hosts on the segment analyze the incoming frames and add data to their ARP tables.
- Computer 176.10.16.1 prepares the data for transmission.

- Computer 176.10.16.1 transmits its data frames through the Ethernet segment.
- All hosts on the segment analyze the incoming frames.
- All computers except computer 176.10.16.4 drop the frames because they do not match the destination MAC address of the incoming frames.
- Router 176.10.16.4 processes the data for transmission to forward to the next network hop.
- Computer 176.10.16.4 processes data transmission.

Routers do not forward broadcast packets. If the feature is turned on, a router performs a proxy ARP. Proxy ARP is a variation of the ARP protocol. In this variation, a router sends an ARP response with the MAC address of the interface, on which the request was received, to the requesting host. The router responds with the MAC addresses for those requests in which the IP address is not in the range of addresses of the local subnet.

Another method to send data to the address of a device that is on another network segment is to set up a default gateway. A default gateway is a host option where the IP address of the router interface is stored in the network configuration of the host. The source host compares the destination IP address and its IP address to determine if the two IP addresses are located in the same segment. If the receiving host is not on the same segment, the source host sends the data using the actual IP address of the destination and the MAC address of the router. The MAC address for the router was learned from the ARP table by using the IP address of that router. If the default gateway on the host or the proxy ARP feature on the router is not configured, no traffic can leave the LAN. One of the other is required to have a connection outside of the LAN.



ARP Table

IP Address	MAC Address
176.10.16.3	FE:ED:31:22:AA:09
176.10.16.6	FE:ED:31:A2:22:F3
176.10.16.5	FE:ED:31:A2:22:77
176.10.16.2	FE:ED:31:A3:47:14
176.10.16.2	FE:ED:31:A3:47:14

Default Gateway

176.10.16.4	FE:ED:31:AF:49:67

Figure 6-48 Default Gateway

- Computer 176.10.16.1 needs to send a data transmission to the computer 199.11.20.5.
- Computer 176.10.16.1 prepares the data for transmission to computer 199.11.20.5. As it is built the frame for transmission. It finds that the IP-MAC pair for 199.11.20.5 is not in its ARP table. With the default gateway set on this computer, the destination address is compared with the host's source address. The calculation shown that the destination is on another network. So the host builds the data frame using the destination IP address and the default gateways MAC address.

- Computer 176.10.16.1 transmits its data frames through the network cable segment.
- All hosts on the segment analyze the incoming frames.
- All computers except for router 176.10.16.4 drop the frames because they do not match the destination MAC address of the incoming frames

6.1 Exercise

1- Class A IP addresses can accommodate 16 million hosts while a Class B can accommodate ___?

   A. 254

   B. 65,534

   C. 4 million.

2- Every active IP address has a corresponding NIC card address

   A. True

   B. False

3- Using the TCP/IP protocol when is a subnet mask required?

   A. only when connecting outside the LAN

   B. only when using TCP/IP

   C. for both intranet and internet usage

4- The TCP/IP protocol used on the internet allows for approximately ___ billion unique IP addresses?

   A. 1

   B. 4

   C. 10

5- Which of the following is class B IP address?

   A. 10.14.16.12

   B. 127.0.0.1

   C. 172.15.42.34

   D. 209.123.32.212

CHAPTER 7

Error Detection and Correction

7.1 Introduction

Error detection and correction or error control are techniques that enable reliable delivery of digital data over unreliable communication channels. Many communication channels are subject to channel noise, and thus errors may be introduced during transmission from the source to a receiver. Error detection techniques allow detecting such errors, while error correction enables the reconstruction of the original data in many cases.

Networks must be able to transfer data from one device to another with complete accuracy. Data can be corrupted during transmission. For reliable communication, errors must be detected and corrected. Error detection and correction are implemented either at the data link layer or the transport layer of the OSI model.

7.2 Types of Errors

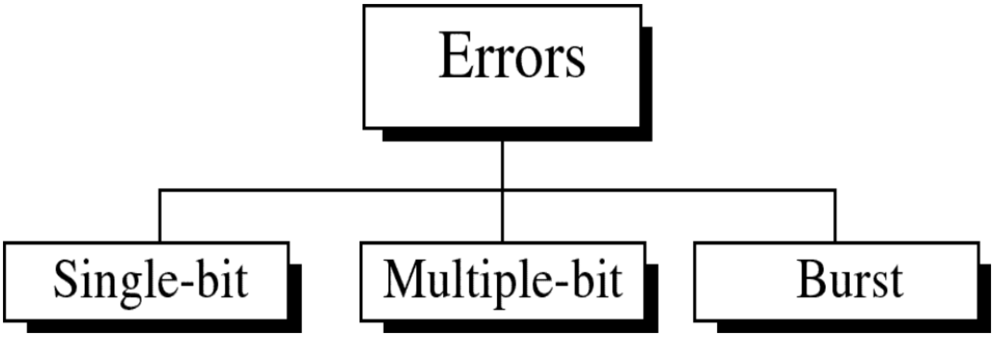


Figure 7-1 Types of Errors

7.2.1 Single-bit error

Single bit errors are the least likely type of errors in serial data transmission because the noise must have a very rare and very short duration. However, this kind of error can happen in parallel transmission.

Example:

If data is sent at 1Mbps then each bit lasts only 1/1,000,000 sec. or 1 μs.

For a single-bit error to occur, the noise must have a duration of only 1 μs, which is very rare.

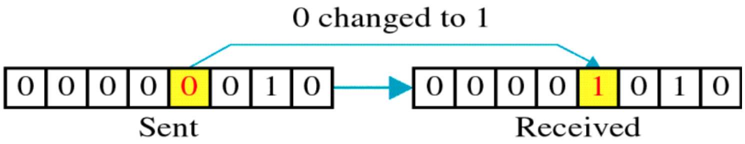


Figure 7-2 Single-bit error

7.2.2 Burst error

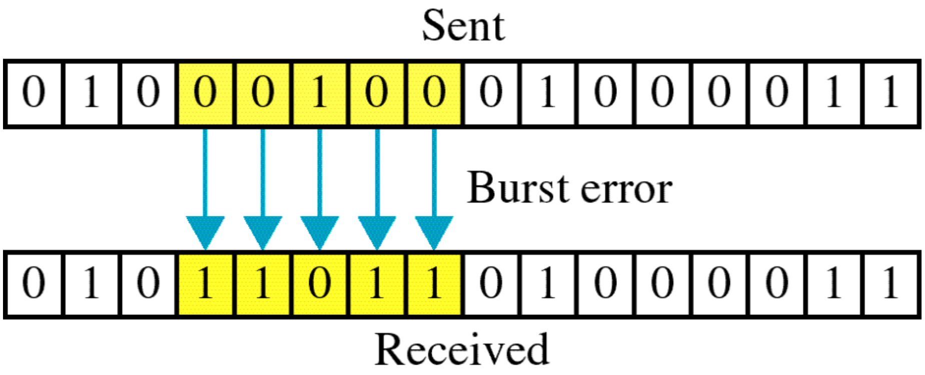


Figure 7-3 Burst Error in Parallel Transmission

The term burst error means that two or more bits in the data unit have changed from 1 to 0 or from 0 to 1.

Burst errors do not necessarily mean that the errors occur in consecutive bits, the length of the burst is measured from the first corrupted bit to the last corrupted bit. Some bits in between may not have been corrupted.

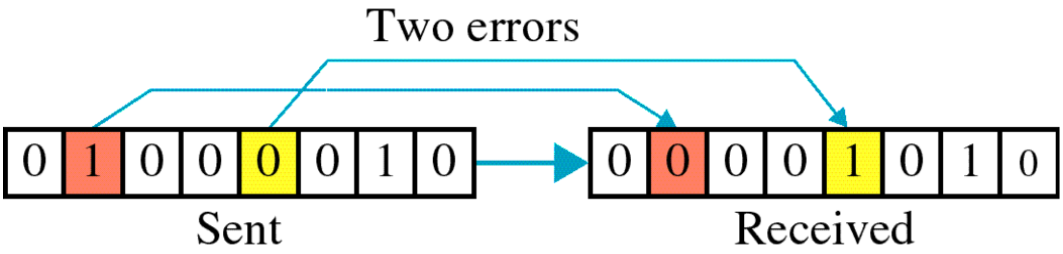


Figure 7-4 Burst Error in Serial Transmission

Burst error is most likely to happen in serial transmission since the duration of noise is normally longer than the duration of a bit.

The number of bits affected depends on the data rate and the duration of the noise.

Example:

If data is sent at rate = 1Kbps then a noise of 1/100 sec can affect 10 bits. (1/100*1000)

If the same data is sent at rate = 1Mbps then a noise of 1/100 sec can affect 10,000 bits. (1/100*10^6)

7.3 Error detection

Error detection means deciding whether the received data is correct or not without having a copy of the original message. Error detection uses the concept of **redundancy**, which means adding extra bits for detecting errors at the destination.

7.4 Redundancy

All error-detection and correction schemes add some redundancy (i.e., some extra data) to a message, which receivers can use to check the consistency of the delivered message and to recover data that has been determined to be corrupted. Error-detection and correction schemes can be either systematic or non-systematic. In a systematic scheme, the transmitter sends the original data and attaches a fixed number of check bits (or parity data), which are derived from the data bits by some deterministic algorithm. If only error detection is required, a receiver can simply apply the same algorithm to the received data bits and compare its output with the received check bits; if the values do not match, an error has occurred at some point during the transmission. In a system that uses a non-systematic code, the original message is transformed into an encoded message carrying the same information and that has at least as many bits as the original message.

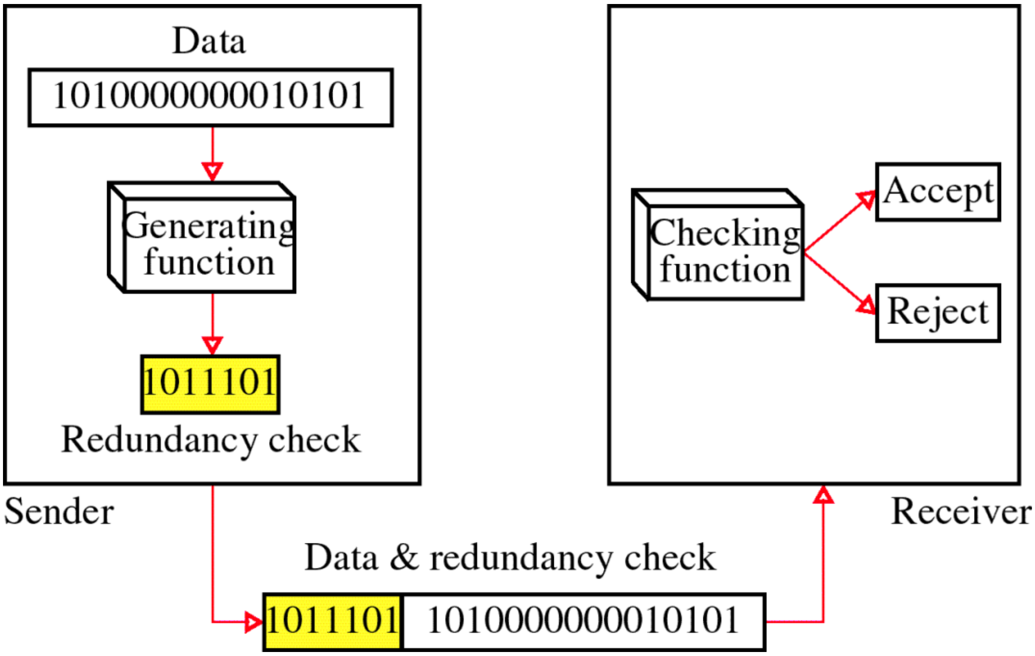


Figure 7-57.4 Redundancy Mechanism

Four types of redundancy checks are used in data communications

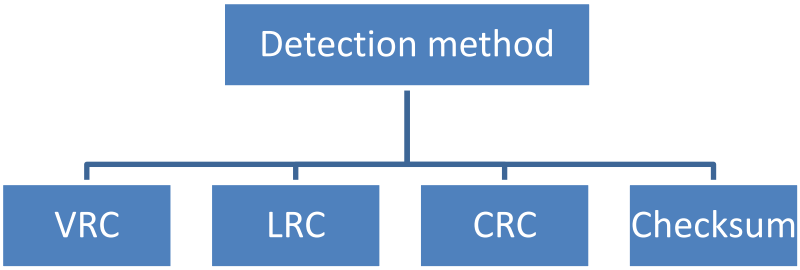


Figure 7-6 Redundancy Types

7.5 Vertical Redundancy Check VRC

Vertical redundancy check (VRC) is an error-checking method used on an eight-bit ASCII character. In VRC, a parity bit is attached to each byte of data, which is then tested to determine whether the transmission is correct. VRC is considered an unreliable error-detection method because it only works if an even number of bits is distorted.

A vertical redundancy check is also called a transverse redundancy check when used in combination with other error-controlling codes such as a longitudinal redundancy check.

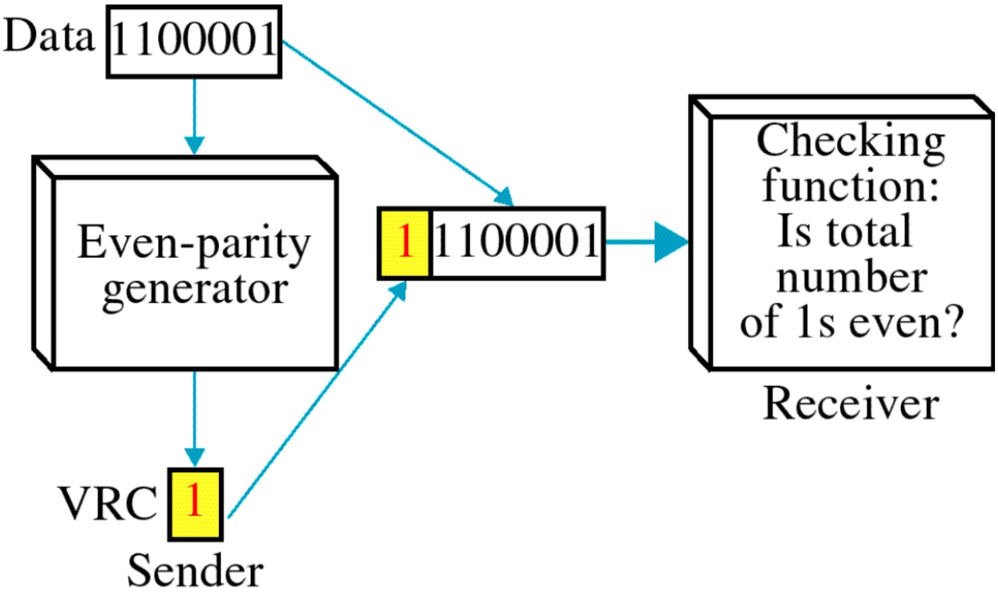


Figure 7-7 Vertical Redundancy Check

Performance

- It can detect single-bit error

- It can detect burst errors only if the total number of errors is odd.

Example

Suppose the sender wants to send the word world. In ASCII the five characters are coded as

1110111 1101111 1110010 1101100 1100100

The following shows the actual bits sent

11101110 11011110 11100100 11011000 11001001

Example

Now suppose the word world in Example 1 is received by the receiver without being corrupted in transmission.

11101110 11011110 11100100 11011000 11001001

The receiver counts the 1s in each character and comes up with even numbers (6, 6, 4, 4, 4). The data are accepted.

Example

Now suppose the word world in Example 1 is corrupted during transmission.

11111110 11011110 11101100 11011000 11001001

The receiver counts the 1s in each character and comes up with even and odd numbers (7, 6, 5, 4, 4). The receiver knows that the data are corrupted, discards them, and asks for retransmission.

7.5.1 Longitudinal Redundancy Check LRC

A longitudinal redundancy check (LRC) is an error-detection method for determining the correctness of transmitted and stored data.

LRC verifies the accuracy of stored and transmitted data using parity bits. It is a redundancy check applied to a parallel group of bitstreams. The data to be transmitted is divided into transmission blocks into which additional check data is inserted.

This term is also known as a horizontal redundancy check.

LRC generally applies to a single parity bit per bitstream. Although simple longitudinal parities only detect errors, a combination with additional error control coding, such as a transverse redundancy check, is capable of correcting errors. LRC fields consist of one byte containing an eight-bit binary value. LRC values are calculated by transmitting devices, which append LRC to messages. The device at the receiving end recalculates the LRC on receipt of the message and compares the calculated value to the actual value received in the LRC field. If the values are equal, the transmission was successful; if the values are not equal, this indicates an error.

LRC is generated through the following steps:

- Add all bytes in messages excluding the starting colon and the ending the carriage return line feed
- Add this to the eight-bit field and discard the carries
- Subtract the final field value from FF hex, producing one’s complement
- Add one, producing two’s complement

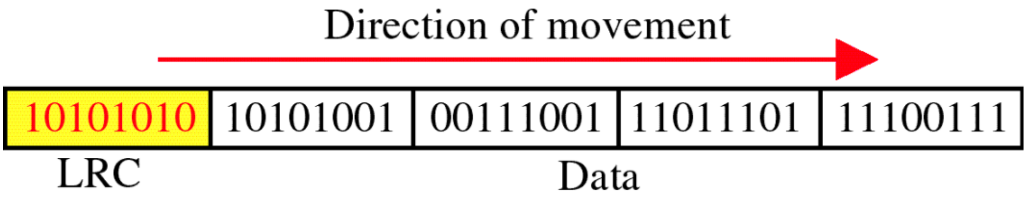
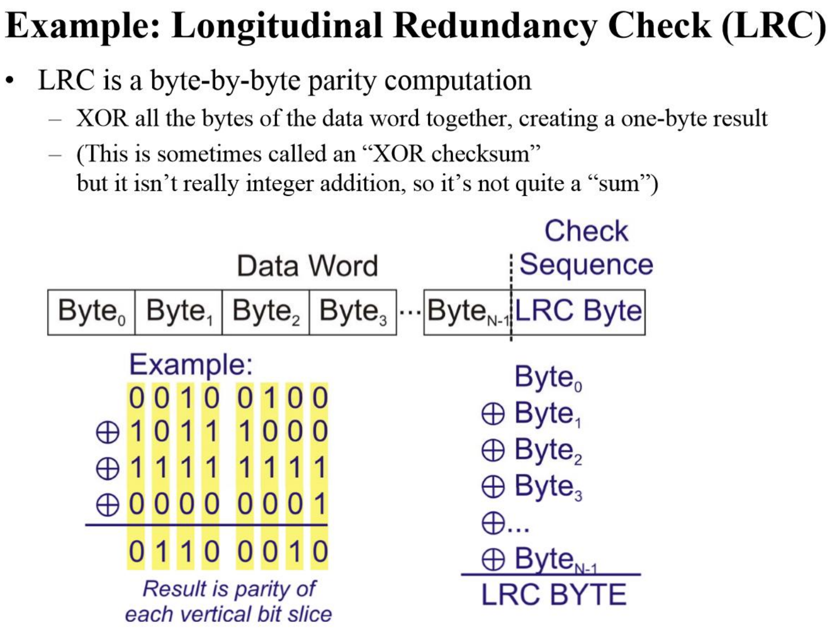


Figure 7-8 Longitudinal Redundancy Check



Example: Longitudinal Redundancy Check (LRC)

- LRC is a byte-by-byte parity computation
  - XOR all the bytes of the data word together, creating a one-byte result
  - (This is sometimes called an "XOR checksum"
    but it isn't really integer addition, so it's not quite a "sum")

Performance

- LCR increases the likelihood of detecting burst errors.
- If two bits in one data unit are damaged and two bits in the same positions in another data unit are also damaged, the LRC checker will not detect an error.

7.5.2 VRC and LRC

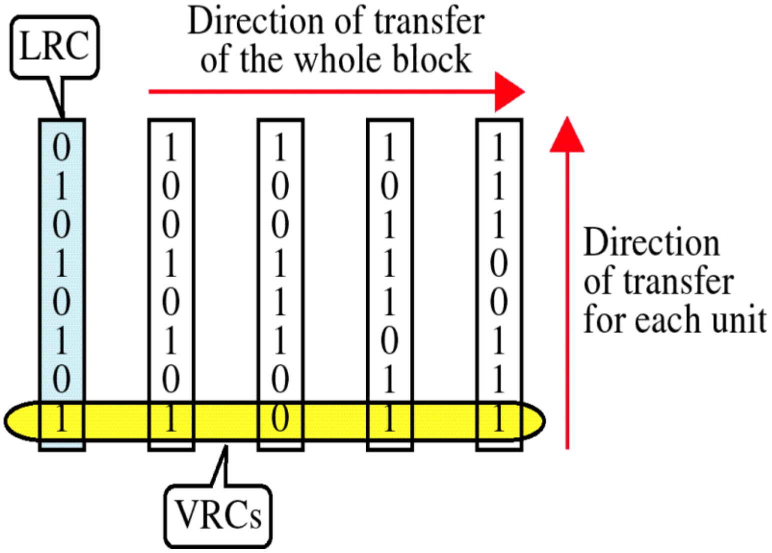


Figure 7-9 VRC & LRC

7.5.3 Two –Dimensional Parity Check

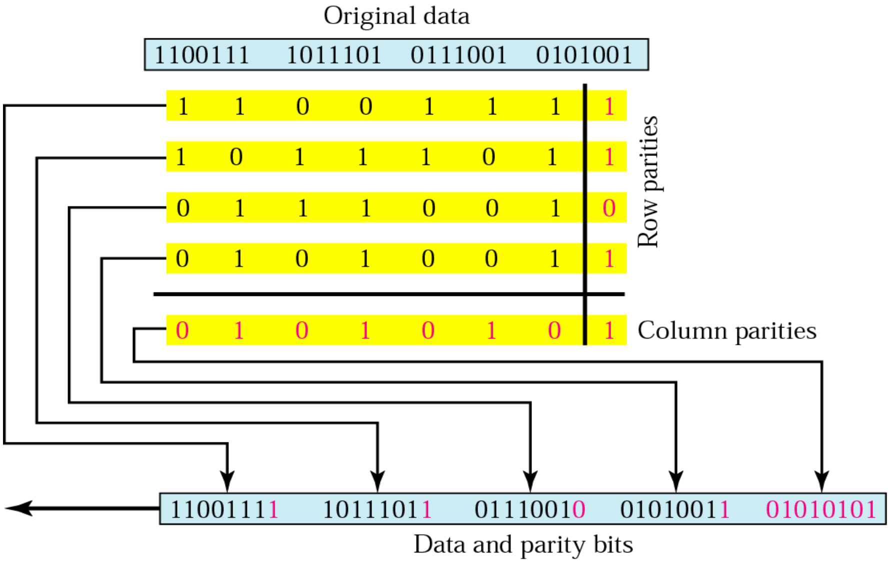


Figure 7-10 Two –Dimensional Parity Check

Example Suppose the following block is sent:

10101001 00111001 11011101 11100111 10101010

However, it is hit by a burst noise of length 8, and some bits are corrupted.

10100011 10001001 11011101 11100111 10101010

When the receiver checks the parity bits, some of the bits do not follow the even-parity rule and the whole block is discarded.

10100011 10001001 11011101 11100111 10101010

7.5.4 Cyclic Redundancy Check CRC

A cyclic redundancy check (CRC) is an error-detecting code commonly used in digital networks and storage devices to detect accidental changes to raw data. Blocks of data entering these systems get a short check value attached, based on the remainder of a polynomial division of their contents. On retrieval, the calculation is repeated and, in the event the check values do not match, corrective action can be taken against data corruption.

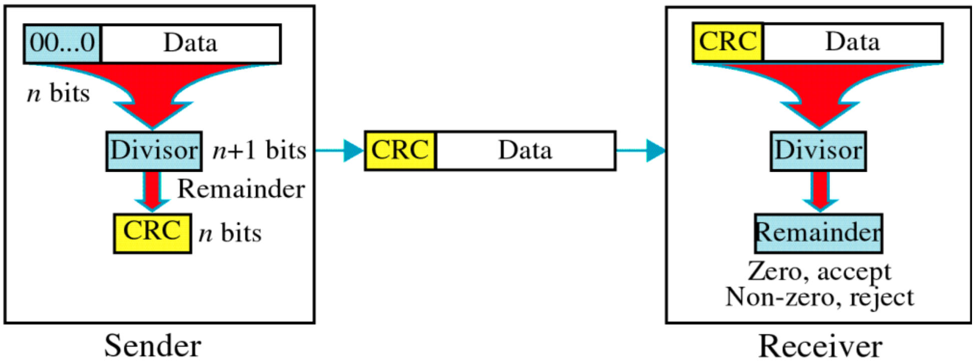


Figure 7-11 Cyclic Redundancy Check

Given a k-bit frame or message, the transmitter generates an n-bit sequence, known as a frame check sequence (FCS), so that the resulting frame, consisting of (k+n) bits, is exactly divisible by some predetermined number.

The receiver then divides the incoming frame by the same number and, if there is no remainder, assumes that there was no error.

CRC example

want:

$$D.2^r \; XOR \; R \; = \; nG$$

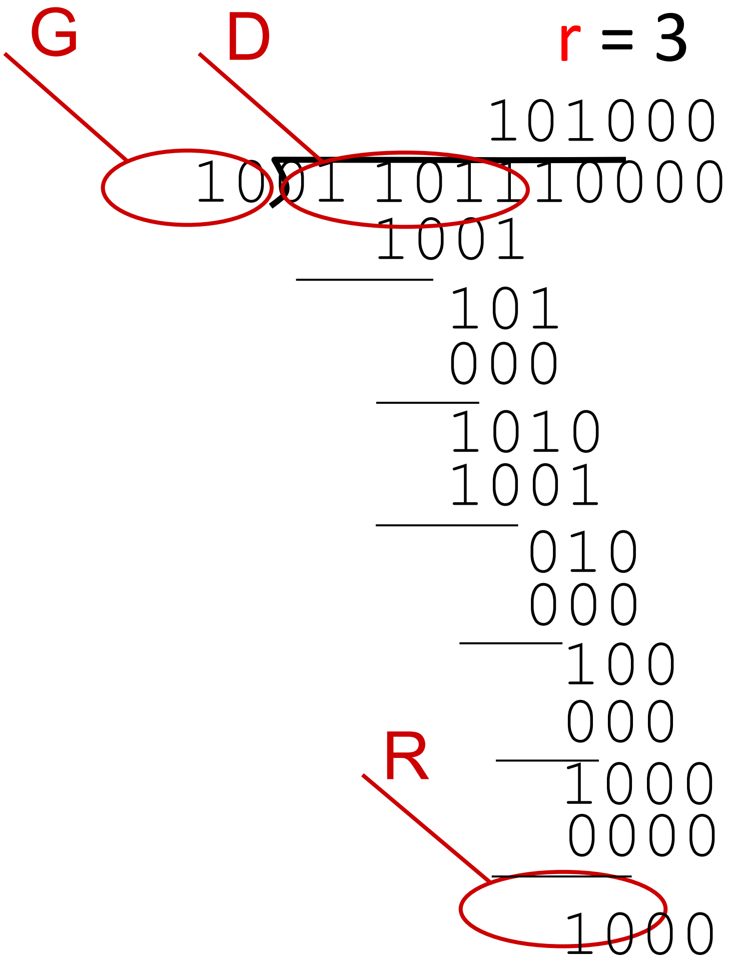
equivalently:

$$D.2^r \; = \; nG \; XOR \; R$$

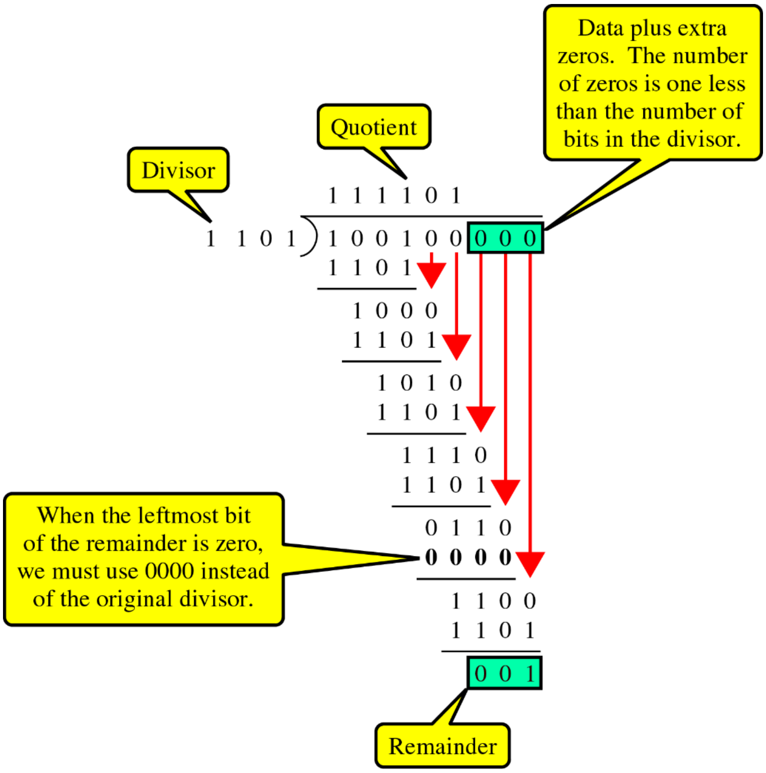
equivalently:

if we divide D.^{2}r by G, want remainder R to satisfy:

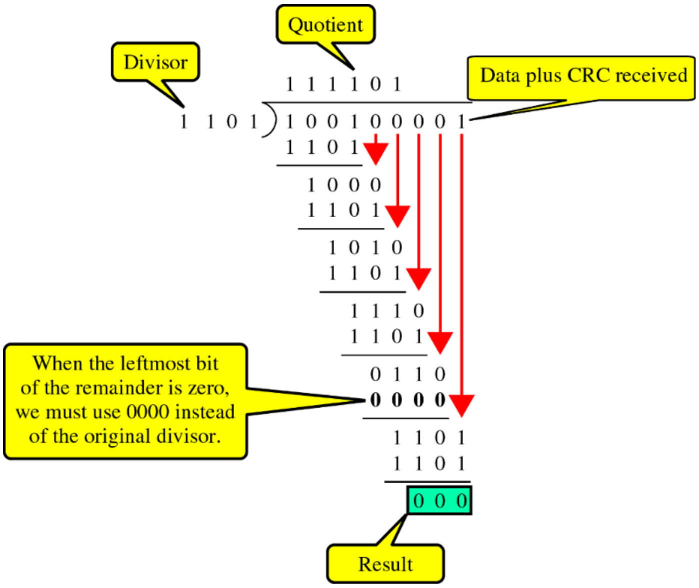
$$R = remander[\frac{D2^R}{G}]$$



```
              101000
1001 ) 101110000
       1001
          101
          000
          1010
          1001
             010
             000
              100
              000
              1000
              0000
              1000
```


Data plus extra zeros. The number of zeros is one less than the number of bits in the divisor.
Quotient
Divisor
1 1 1 1 0 1
1 1 0 1
1 0 0 1 0 0 0 0 0
1 1 0 1
1 0 0 0
1 1 0 1
1 0 1 0
1 1 0 1
1 1 1 0
1 1 0 1
0 1 1 0
0 0 0 0
1 1 0 0
1 1 0 1
0 0 1
When the leftmost bit of the remainder is zero, we must use 0000 instead of the original divisor.
Remainder

Send

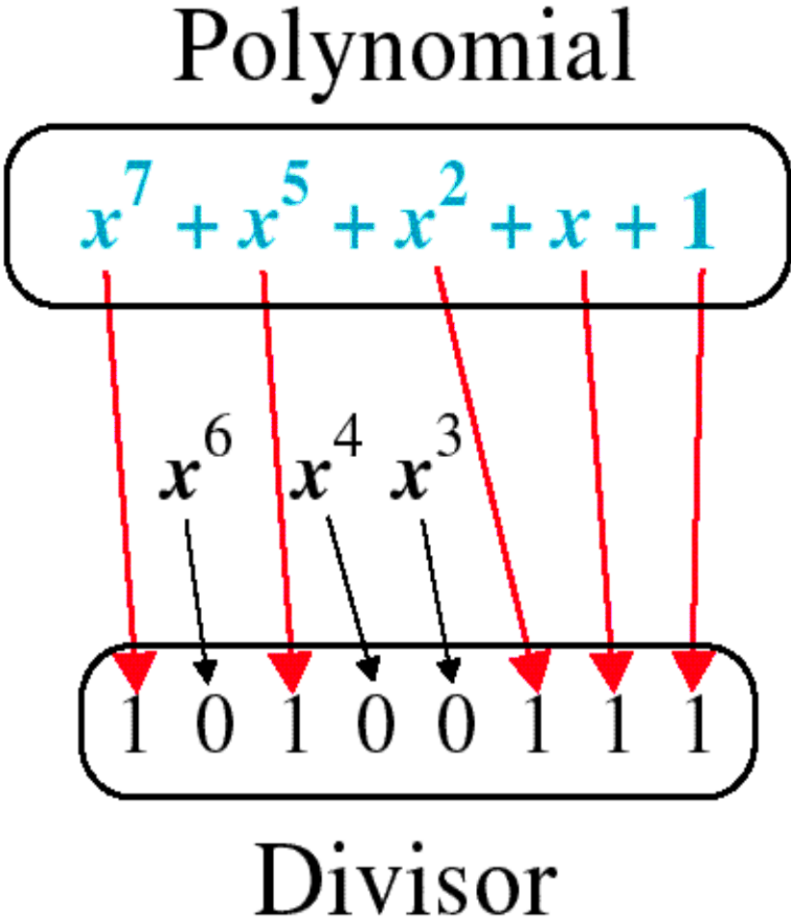


Receive

7.6 Polynomial and Divisor

CRC generator(divisor) is most often represented not as a string of 1s and 0s, but as an algebraic polynomial

$$\boxed{x^7 + x^5 + x^2 + x + 1}$$



Standard Polynomials

CRC-12

$$x^{12} + x^{11} + x^{3} + x + 1$$

CRC-16

$$x^{16} + x^{15} + x^{2} + 1$$

CRC-ITU

$$x^{16} + x^{12} + x^{5} + 1$$

CRC-32

$$x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^{8} + x^{7} + x^{5} + x^{4} + x^{2} + x + 1$$

7.7 Checksum

A checksum is a small-sized datum derived from a block of digital data to detect errors that may have been introduced during its transmission or storage. By themselves, checksums are often used to verify data integrity but are not relied upon to verify data authenticity.

The procedure which generates this checksum is called a checksum function or checksum algorithm. Depending on its design goals, a good checksum algorithm will usually output a significantly different value, even for small changes made to the input. This is especially true of cryptographic hash functions, which may be used to detect many data corruption errors and verify overall data integrity; if the computed checksum for the current data input matches the stored value of a previously computed checksum, there is a very high probability the data has not been accidentally altered or corrupted.

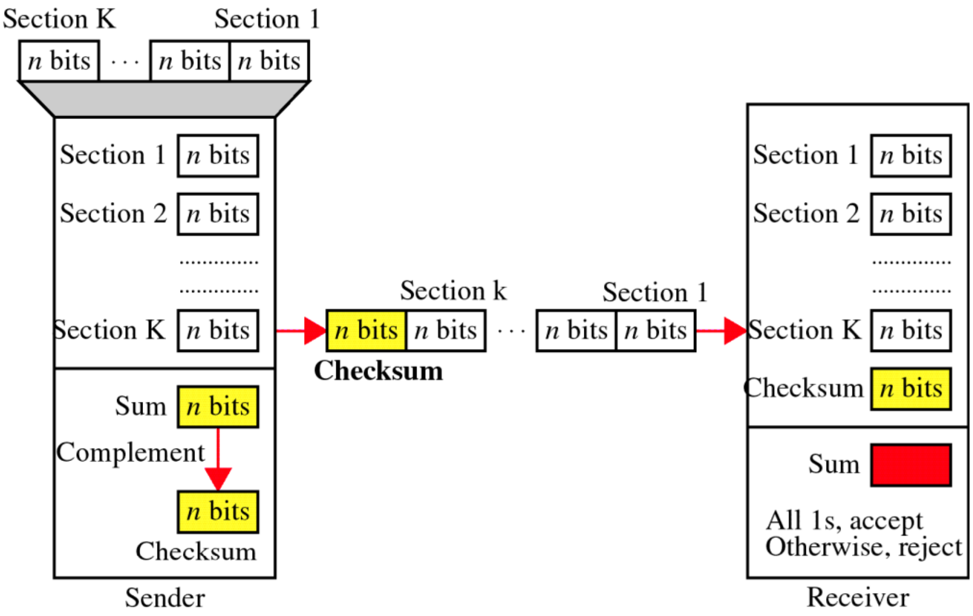


Figure 7-12 Checksum

At the sender

- The unit is divided into k sections, each of n bits.
- All sections are added together using one's complement to get the sum.
- The sum is complemented and becomes the checksum.
- The checksum is sent with the data

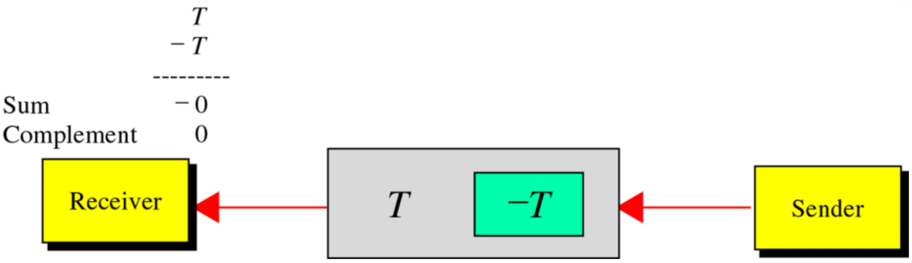
At the receiver

- The unit is divided into k sections, each of n bits.
- All sections are added together using one's complement to get the sum.
- The sum is complemented.
- If the result is zero, the data are accepted: otherwise, they are rejected.

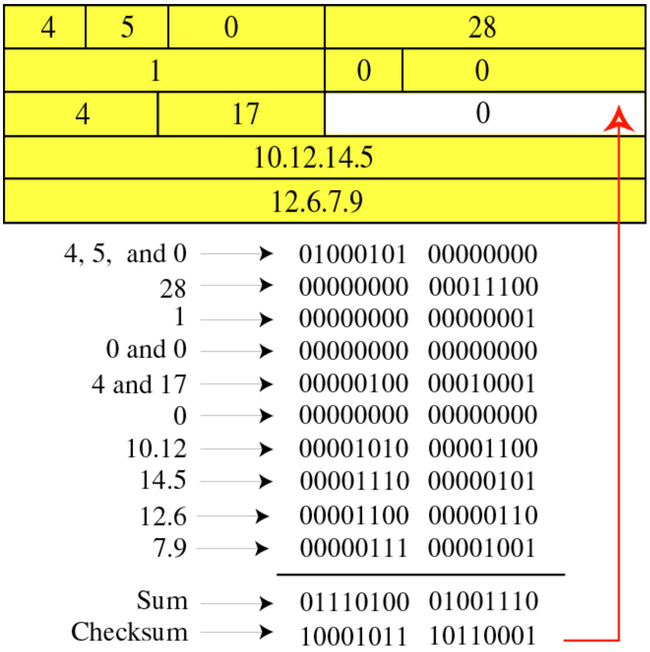
To create the checksum the sender does the following:

- The unit is divided into K sections, each of n bits.
- Sections 1 and 2 are added together using one's complement.
- Section 3 is added to the result of the previous step.
- Section 4 is added to the result of the previous step.
- The process repeats until section k is added to the result of the previous step.
- The final result is complemented to make the checksum.

The receiver adds the data unit and the checksum field. If the result is all 1s, the data unit is accepted; otherwise it is discarded.



Example:



<table>
<tr><td>4</td><td colspan="2">5</td><td>0</td><td colspan="2">28</td></tr>
<tr><td colspan="4">1</td><td>0</td><td>0</td></tr>
<tr><td colspan="2">4</td><td colspan="2">17</td><td colspan="2">0</td></tr>
<tr><td colspan="6">10.12.14.5</td></tr>
<tr><td colspan="6">12.6.7.9</td></tr>
</table>

```
4, 5,  and 0 ──➤ 01000101  00000000
          28 ──➤ 00000000  00011100
           1 ──➤ 00000000  00000001
     0 and 0 ──➤ 00000000  00000000
    4 and 17 ──➤ 00000100  00010001
           0 ──➤ 00000000  00000000
       10.12 ──➤ 00001010  00001100
        14.5 ──➤ 00001110  00000101
        12.6 ──➤ 00001100  00000110
         7.9 ──➤ 00000111  00001001
                 ──────────────────
         Sum ──➤ 01110100  01001110
    Checksum ──➤ 10001011  10110001
```

Example

(at a sender)

Original data: 10101001 00111001

10101001

00111001

11100010 Sum

00011101 Checksum

10101001 00111001 00011101 ← send

(at a receiver)

Received data: 10101001 00111001 00011101

10101001

00111001

00011101

11111111 ← Sum

00000000 ← Complement

Performance

- The checksum detects all errors involving an odd number of bits.
- It detects most errors involving an even number of bits.
- If one or more bits of a segment is damaged and the corresponding bit or bits of opposite value in a second segment are also damaged, the sums of those columns will not change and the receiver will not detect a problem.

7.8 Error Correction

Error Correction codes are used to detect and correct the errors when data is transmitted from the sender to the receiver. Error Correction can be handled in two ways: Backward error correction: Once the error is discovered, the receiver requests the sender to retransmit the entire data unit. Forward error correction: In this case, the receiver uses the error-correcting code which automatically corrects the errors. A single additional bit can detect the error, but cannot correct it. For correcting the errors, one has to know the exact position of the error. For example, if we want to calculate a single-bit error, the error correction code will determine which one of seven bits is in error. To achieve this, we have to add some additional redundant bits.

Suppose r is the number of redundant bits and d is the total number of the data bits. The number of redundant bits r can be calculated by using the formula:

$$2^r >= d + r + 1$$

The value of r is calculated by using the above formula. For example, if the value of d is 4, then the possible smallest value that satisfies the above relation would be 3.

To determine the position of the bit which is in error, a technique developed by R.W Hamming is Hamming code which can be applied to any length of the data unit and uses the relationship between data units and redundant units.

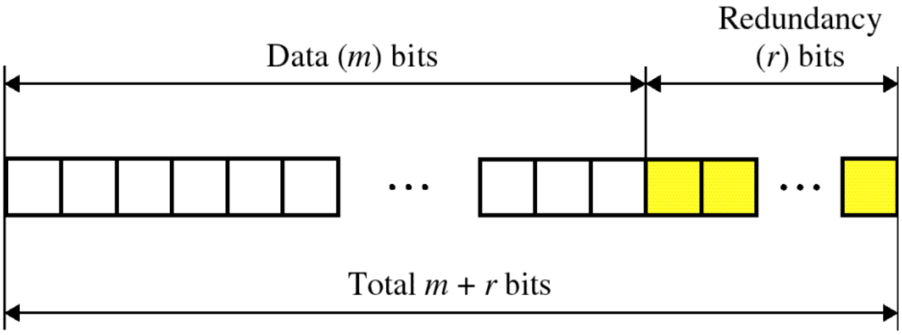


Figure 7-13 Error Correction Mechanism

7.8.1 Hamming Code

Hamming code is a block code that is capable of detecting up to two simultaneous bit errors and correcting single-bit errors. It was developed by R.W. Hamming for error correction.

In this coding method, the source encodes the message by inserting redundant bits within the message. These redundant bits are extra bits that are generated and inserted at specific positions in the message itself to enable error detection and correction. When the destination receives this message, it performs recalculations to detect errors and find the bit position that has an error.

7.8.1.1 Encoding a message by Hamming Code

The procedure used by the sender to encode the message encompasses the following steps −

Step 1 − Calculation of the number of redundant bits.

Step 2 − Positioning the redundant bits.

Step 3 − Calculating the values of each redundant bit.

Once the redundant bits are embedded within the message, this is sent to the user.

Step 1 − Calculation of the number of redundant bits.

If the message contains m$m$number of data bits, r$r$number of redundant bits are added to it so that mr can indicate at least (m + r+ 1) different states. Here, (m + r) indicates the location of an error in each of (m + r) bit positions and one additional state indicates no error. Since rr bits can indicate $2^r r$ states, $2^r r$ must be at least equal to (m + r + 1). Thus the following equation should hold $2^r \geq m + r + 1$

Step 2 − Positioning the redundant bits.

The r redundant bits placed at bit positions of powers of 2, i.e. 1, 2, 4, 8, 16, etc. They are referred to in the rest of this text as r_1 (at position 1), r_2 (at position 2), r_3 (at position 4), r_4 (at position 8), and so on.

Step 3 − Calculating the values of each redundant bit.

The redundant bits are parity bits. A parity bit is an extra bit that makes the number of 1s either even or odd. The two types of parity are −

Even Parity − Here the total number of bits in the message is made even.

Odd Parity − Here the total number of bits in the message is made odd.

Each redundant bit, r_i, is calculated as the parity, generally even parity, based upon its bit position. It covers all bit positions whose binary representation includes a 1 in the i^{th} position except for the position of ri. Thus −

- r_1 is the parity bit for all data bits in positions whose binary representation includes a 1 in the least significant position excluding 1 (3, 5, 7, 9, 11, and so on)
- r_2 is the parity bit for all data bits in positions whose binary representation includes a 1 in the position 2 from right except 2 (3, 6, 7, 10, 11, and so on)
- r_3 is the parity bit for all data bits in positions whose binary representation includes a 1 in the position 3 from right except 4 (5-7, 12-15, 20-23, and so on)

Decoding a message in Hamming Code

Once the receiver gets an incoming message, it performs recalculations to detect errors and correct them. The steps for recalculation are −

Step 1 − Calculation of the number of redundant bits.

Step 2 − Positioning the redundant bits.

Step 3 − Parity checking.

Step 4 − Error detection and correction

Step 1 − Calculation of the number of redundant bits

Using the same formula as in encoding, the number of redundant bits is ascertained.

$2^r \geq m + r + 1$ where m is the number of data bits and r is the number of redundant bits.

Step 2 − Positioning the redundant bits

The r redundant bits placed at bit positions of powers of 2, i.e. 1, 2, 4, 8, 16, etc.

Step 3 − Parity checking

Parity bits are calculated based upon the data bits and the redundant bits using the same rule as during generation of c1,c2 ,c3 ,c4 etc. Thus

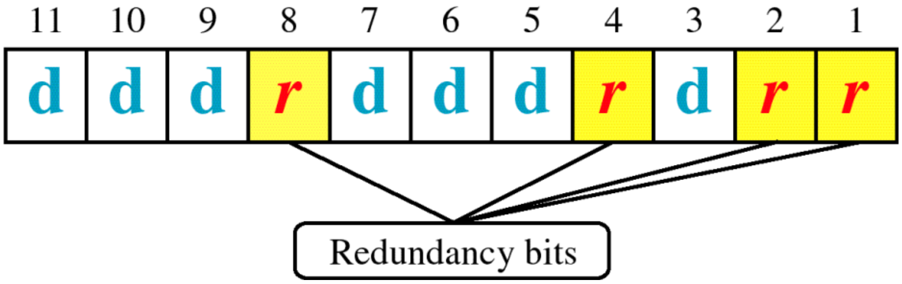
c1 = parity(1, 3, 5, 7, 9, 11 and so on)

c2 = parity(2, 3, 6, 7, 10, 11 and so on)

c3 = parity(4-7, 12-15, 20-23 and so on)

Step 4 − Error detection and correction

The decimal equivalent of the parity bits binary values is calculated. If it is 0, there is no error. Otherwise, the decimal value gives the bit position which has an error. For example, if c1c2c3c4 = 1001, it implies that the data bit at position 9, the decimal equivalent of 1001, has an error. The bit is flipped to get the correct message.



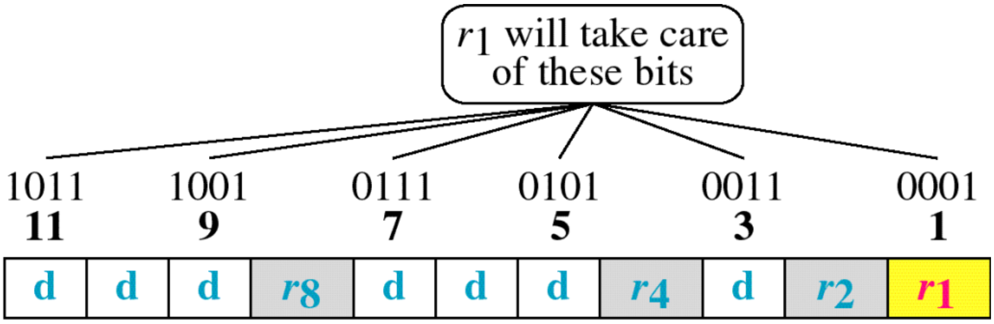
each r bit is the VRC bit for one combination of data bits

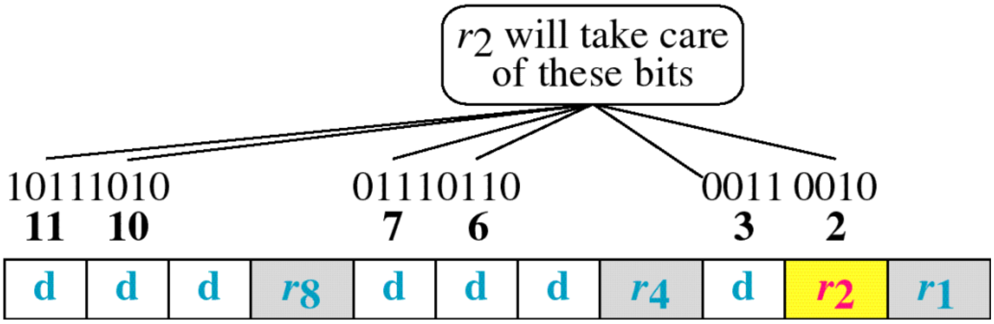
r_1 = bits 1, 3, 5, 7, 9, 11

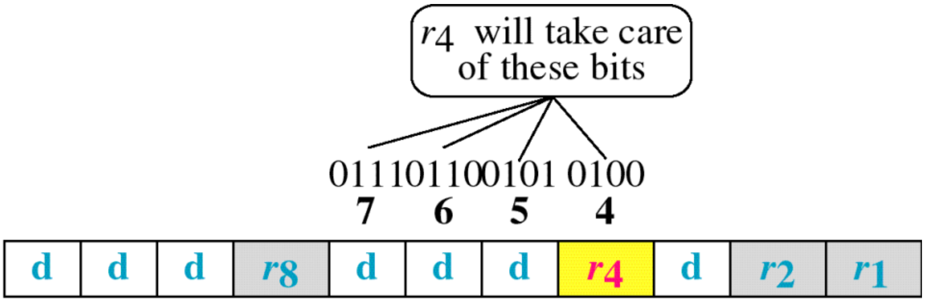
r_2 = bits 2, 3, 6, 7, 10, 11

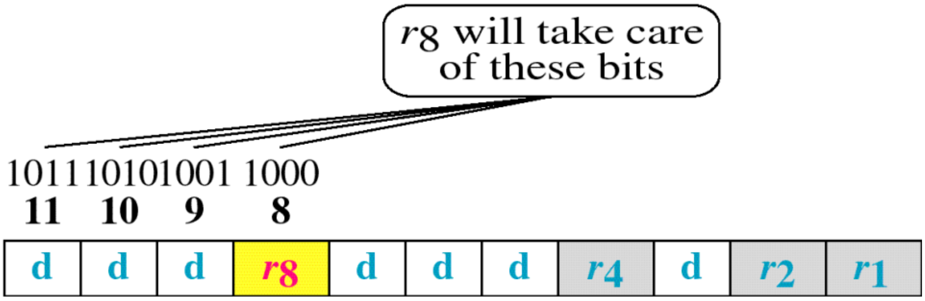
r_4 = bits 4, 5, 6, 7

r_8 = bits 8, 9, 10, 11

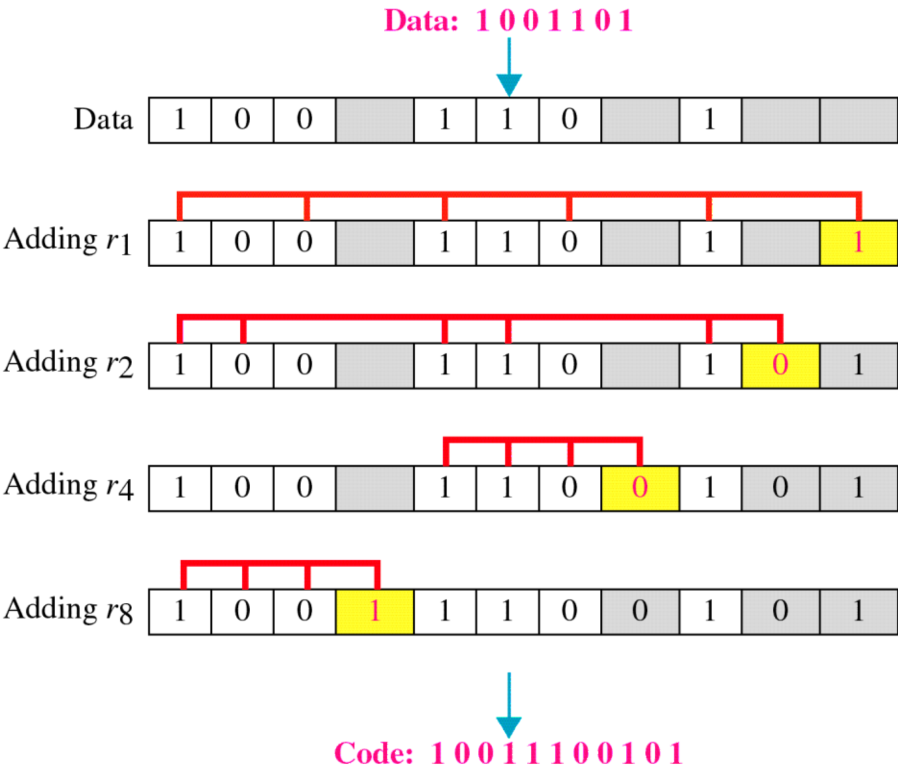




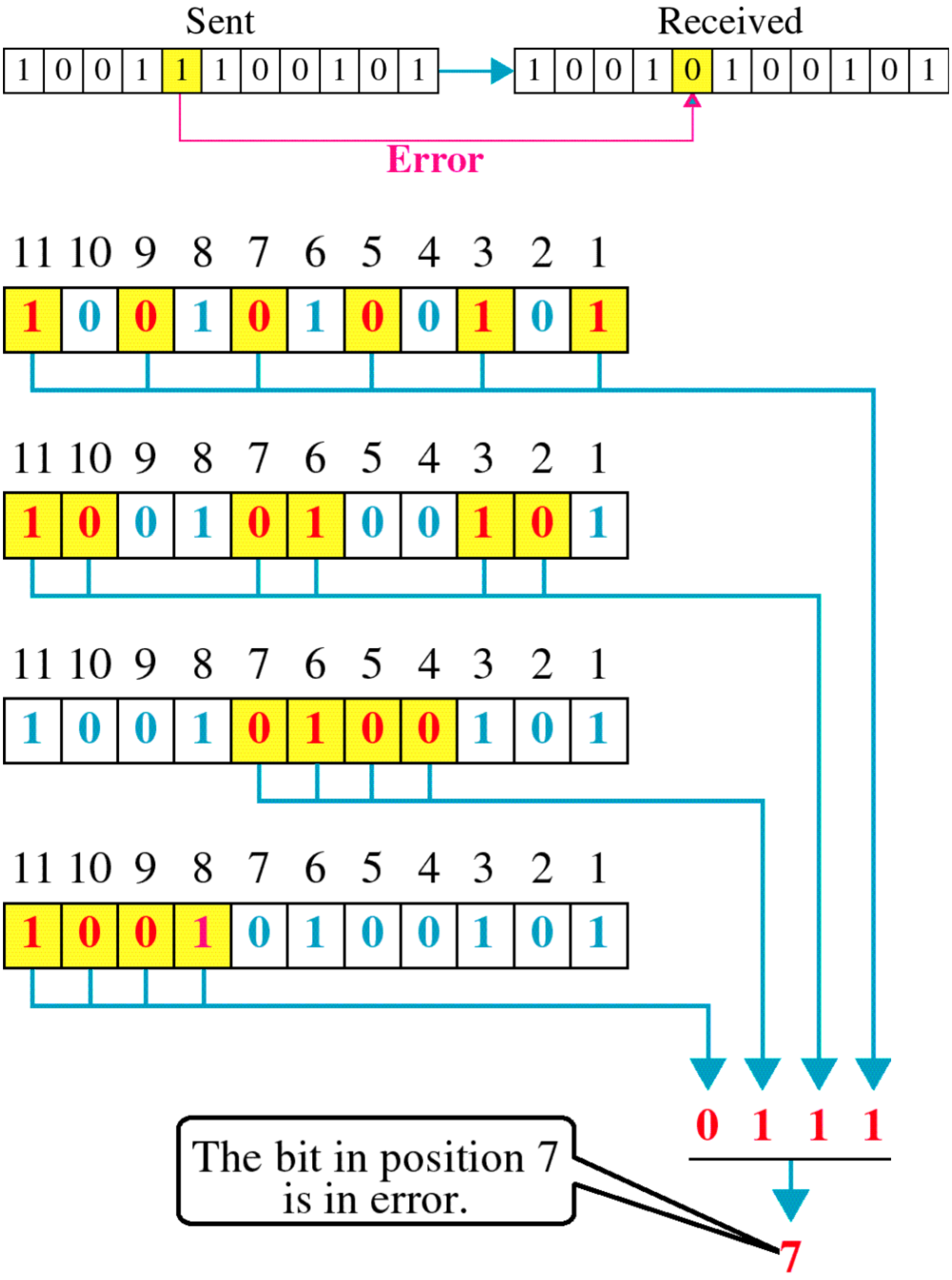




Example of Hamming Code


Data: 1 0 0 1 1 0 1
Data 1 0 0 1 1 0 1
Adding r1 1 0 0 1 1 0 1 1
Adding r2 1 0 0 1 1 0 1 0 1
Adding r4 1 0 0 1 1 0 0 1 0 1
Adding r8 1 0 0 1 1 1 0 0 1 0 1
Code: 1 0 0 1 1 1 0 0 1 0 1

Single-bit error



7.9 Exercise

1- Assume that a receiver receives the following bit sequences. An 8-bit checksum is used. Which sequences will receive correctly?

(1) 10010011 10011011 11011001

(2) 00110011 10110111 00010101

(3) 01110000 00111000 01010111

a. 1 and 2 c. 1 and 3

b. 2 and 3 d. 1,2 and 3

2- A generator of a cyclic code that contains a factor of x + 1 can detect all

a. Odd number errors

b. Single bit errors

c. Multiple bit errors

d. Even number errors

3- A 7-bit byte with binary value 0101111 is to be encoded using an even-parity Hamming code. What is the binary value after encoding?

4- Assume even parity. Then find the parity bit for the each of the following data units: 1001011 0001100 1000000 1110111

5- Find the polynomial equivalent of 100001110001.

Find the checksum of the following bit sequence. Assume a 16-bit segment size. 1001001110010011100110000100110

6- Suppose we want to transmit the message 1111001001101010 and protect it from errors using the CRC8 polynomial x8 +x2

+x1 +1. Use polynomial long division to determine the message that should be transmitted

7- How many bits in the data unit has changed in single bit error?

   a. only 1
   b. two bits
   c. three bits
   d. four bits

8- Find the parity bit for 1001011

   a. 0
   b. 1
   c. 2
   d. None

9- Given the generator function G(x) = x^4 + x + 1 and the message function M(x) = x^7 + x^6 + x^4 + x^2 + x: (a) Calculate the transmission function T(x). (b) Consider that the transmission is damaged, such that the receiver receives R(x)= x^11 + x^9 + x^8 + x^3 + x^2 + x + 1. Will this error be detected?

   a. True
   b. False

CHAPTER 8

Routing

8.1 Introduction

Routing is the process of selecting a path for traffic in a network or between or across multiple networks. Broadly, routing is performed in many types of networks, including circuit-switched networks, such as the public switched telephone network (PSTN), and computer networks, such as the Internet.

In packet switching networks, routing is the higher-level decision making that directs network packets from their source toward their destination through intermediate network nodes by specific packet forwarding mechanisms. Packet forwarding is the transit of network packets from one network interface to another. Intermediate nodes are typically networked hardware devices such as routers, gateways, firewalls, or switches. General-purpose computers also forward packets and perform routing, although they have no specially optimized hardware for the task.

The routing process usually directs forwarding based on routing tables. Routing tables maintain a record of the routes to various network destinations. Routing tables may be specified by an administrator, learned by observing network traffic, or built with the assistance of routing protocols.

Routing, in a narrower sense of the term, often refers to IP routing and is contrasted with bridging. IP routing assumes that network addresses are structured and that similar addresses imply proximity within the network. Structured addresses allow a single routing table entry to represent the route to a group of devices. In large networks, structured addressing (routing, in the narrow sense) outperforms unstructured addressing (bridging). Routing has become the dominant form of addressing on the Internet. Bridging is still widely used within local area networks.

8.2 Delivery schemes

Routing schemes differ in how they deliver messages:

A. In computer networking, unicast is a one-to-one transmission from one point in the network to another point; that is, one sender and one receiver, each identified by a network address.

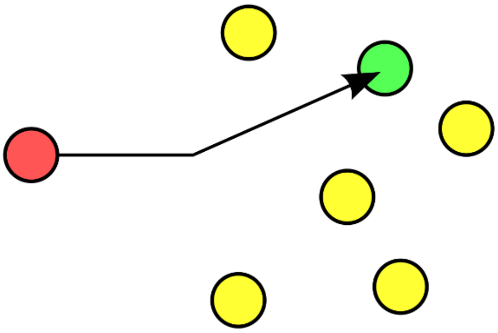


Figure 8-1 Unicast

B. Broadcasting is a method of transferring a message to all recipients simultaneously. Broadcasting can be performed as a high-level operation in a program, for example, broadcasting in Message Passing Interface, or it may be a low-level networking operation, for example broadcasting on Ethernet

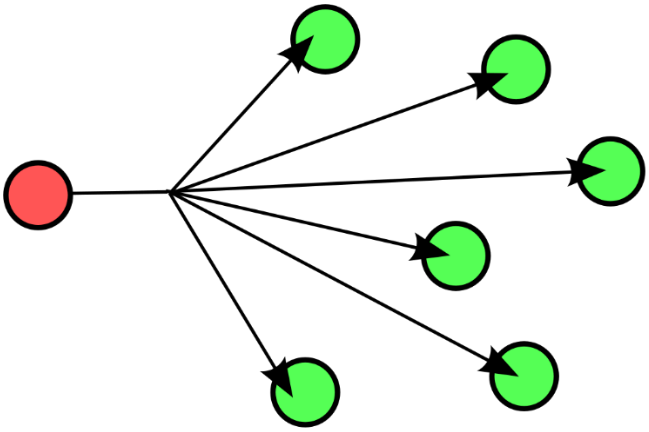


Figure 8-2 Broadcasting

C. Multicast is group communication where data transmission is addressed to a group of destination computers simultaneously. Multicast can be one-to-many or many-to-many distribution. Multicast should not be confused with physical layer point-to-multipoint communication. Multicast differs from broadcast in that the destination address designates a subset, not necessarily all, of the accessible nodes.

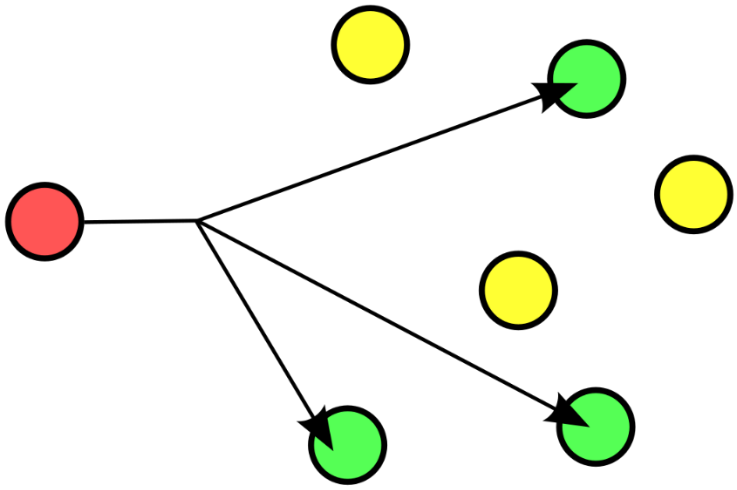


Figure 8-3 Multicast

D. Anycast delivers a message to anyone out of a group of nodes, typically the one nearest to the source using a one-to-one-of-many association where datagrams are routed to any single member of a group of potential receivers that are all identified by the same destination address. The routing algorithm selects the single receiver from the group based on which is the nearest according to some distance measure.

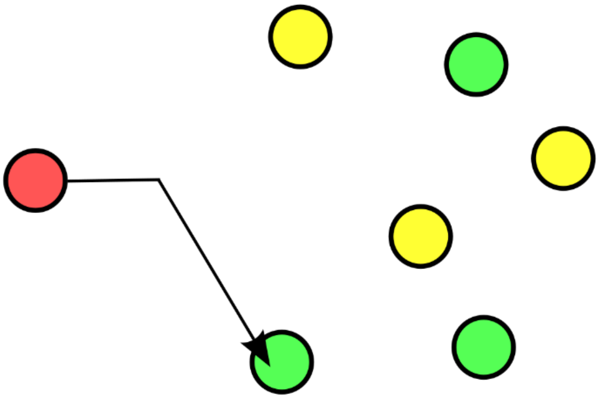


Figure 8-4 Anycast

E. Geocast delivers a message to a group of nodes in a network based on their geographic location. It is a specialized form of multicast addressing used by some routing protocols for mobile ad hoc networks.

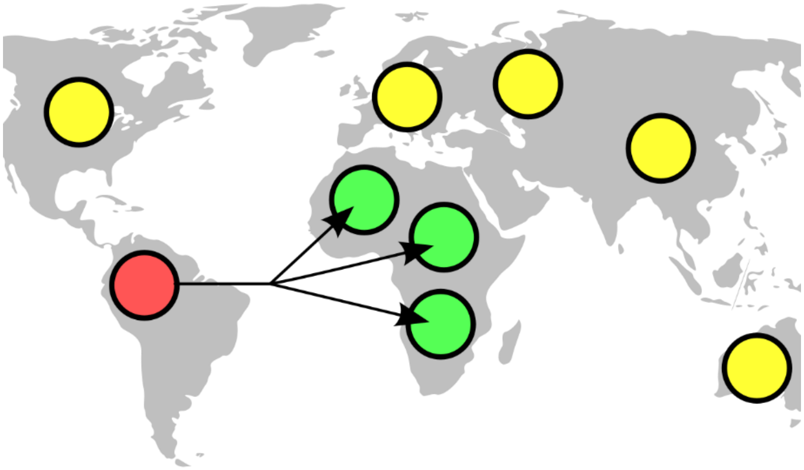


Figure 8-5 Geocast

Unicast is the dominant form of message delivery on the Internet. This article focuses on unicast routing algorithms.

8.3 Path selection

Path selection involves applying a routing metric to multiple routes to select (or predict) the best route. Most routing algorithms use only one network path at a time. Multipath routing and specifically equal-cost multi-path routing techniques enable the use of multiple alternative paths.

In computer networking, the metric is computed by a routing algorithm and can cover information such as bandwidth, network delay, hop count, path cost, load, maximum transmission unit, reliability, and communication cost.[3] The routing table stores only the best possible routes, while link-state or topological databases may store all other information as well.

In case of overlapping or equal routes, algorithms consider the following elements in priority order to decide which routes to install into the routing table:

Prefix length: A matching route table entry with a longer subnet mask is always preferred as it specifies the destination more exactly.

Metric: When comparing routes learned via the same routing protocol, a lower metric is preferred. Metrics cannot be compared between routes learned from different routing protocols.

Administrative distance: When comparing route table entries from different sources such as different routing protocols and static configuration, a lower administrative distance indicates a more reliable source and thus a preferred route.

Because a routing metric is specific to a given routing protocol, multi-protocol routers must use some external heuristic to select between routes learned from different routing protocols. Cisco routers, for example, attribute a value known as the administrative distance to each route, where smaller administrative distances indicate routes learned from a protocol assumed to be more reliable.

A local administrator can set up host-specific routes that provide more control over network usage, permits testing, and better overall security. This is useful for debugging network connections or routing tables.

In some small systems, a single central device decides ahead of time the complete path of every packet. In some other small systems, whichever edge device injects a packet into the network decides ahead of time the complete path of that particular packet. In both of these systems, that route-planning device needs to know a lot of information about what devices are connected to the network and how they are connected to each other. Once it has this information, it can use an algorithm such as A* search algorithm to find the best path.

8.4 Graphs and networks

Every day we are surrounded by countless connections and networks: roads and rail tracks, phone lines, the internet, electronic circuits, and even molecular bonds. There are even social networks between friends and families. In mathematics, all these examples can be represented as graphs A graph is a collection of vertices connected by edges. A graph consists of certain points called vertices, some of which are connected by edges.

In mathematics, graph theory is the study of graphs, which are mathematical structures used to model pairwise relations between objects. A graph in this context is made up of vertices (also called nodes or points) which are connected by edges (also called links or lines). A distinction is made between undirected graphs, where edges link two vertices symmetrically and directed graphs, where edges link two vertices asymmetrically; see Graph (discrete mathematics) for more detailed definitions and for other variations in the types of graph that are commonly considered. Graphs are one of the prime objects of study in discrete mathematics. Graphs model how various entities are connected

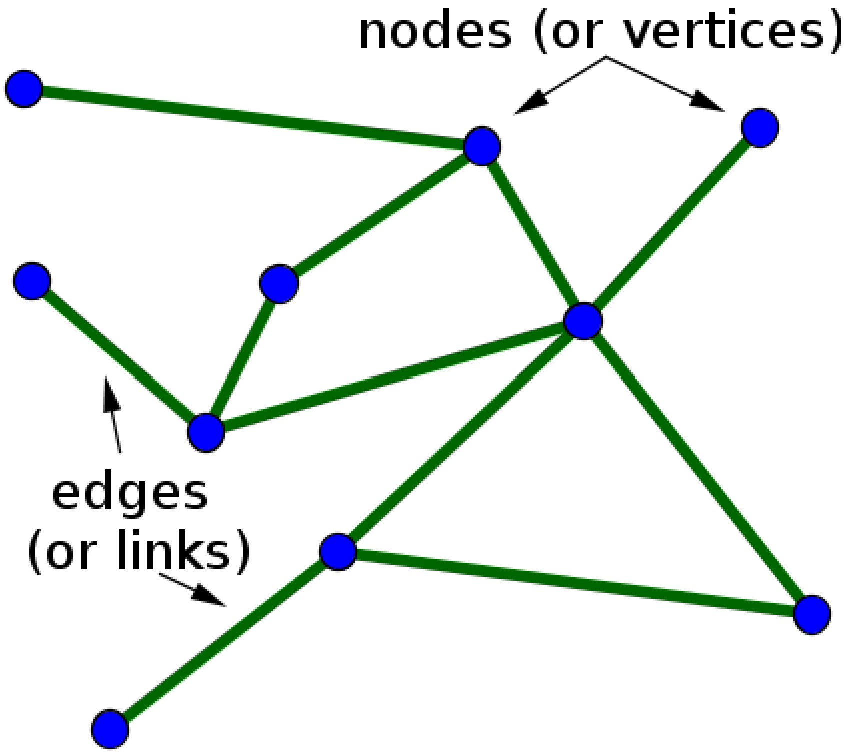


Figure 8-6 Graph or Network

A network is simply a collection of connected objects. We refer to the objects as nodes or vertices and usually draw them as points. We refer to the connections between the nodes as edges and usually draw them as lines between points.

8.4.1 Directed and Undirected Networks

A directed graph or digraph is a graph in which edges have orientations. A directed graph (also known as a digraph) (N, E) consists of

- set of **nodes** N (also known as vertices)
- set of **edges** E (also known as arcs)
    - edges are directed from one node to another
    - edge from node i to node j is denoted by (i, j)

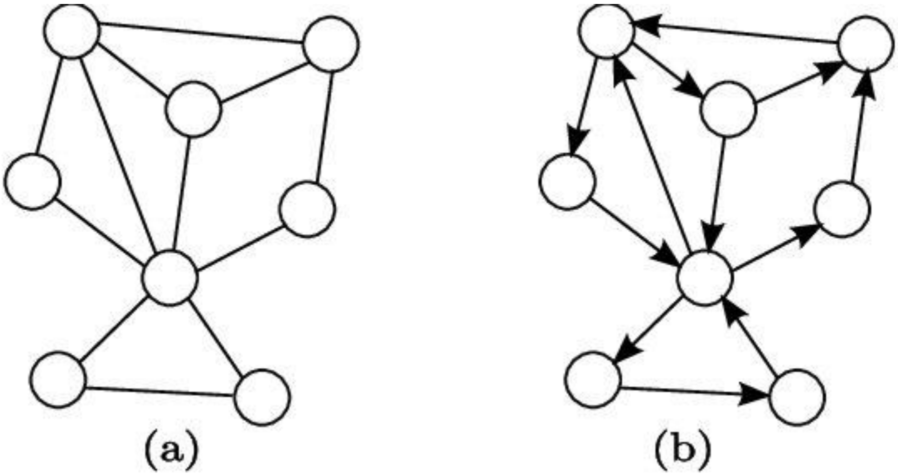


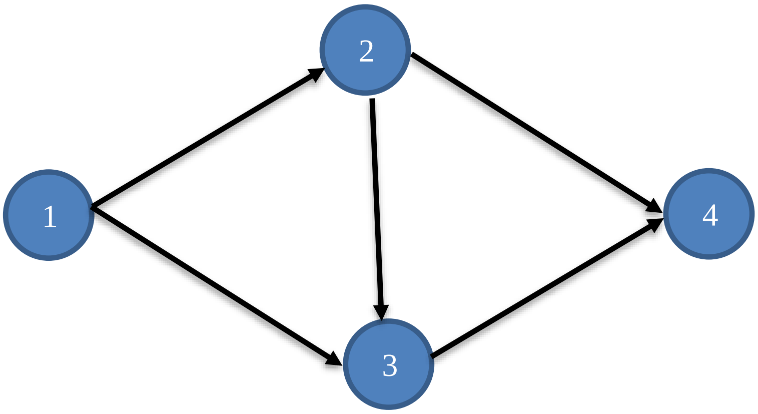
Figure 8-7 (a) Undirected and (b) Direct Graph

An undirected graph is a graph, i.e., a set of objects (called vertices or nodes) that are connected together, where all the edges are bidirectional. An undirected graph is sometimes called an undirected network. In contrast, a graph where the edges point in a direction is called a directed graph.

A path is a sequence of edges connecting two specified nodes in a graph:

- Each edge must have exactly one node in common with its predecessor in the sequence
- Edges must be passed in the forward direction
- No node may be visited more than once

Example1: Give some examples of graph



Answer the following question

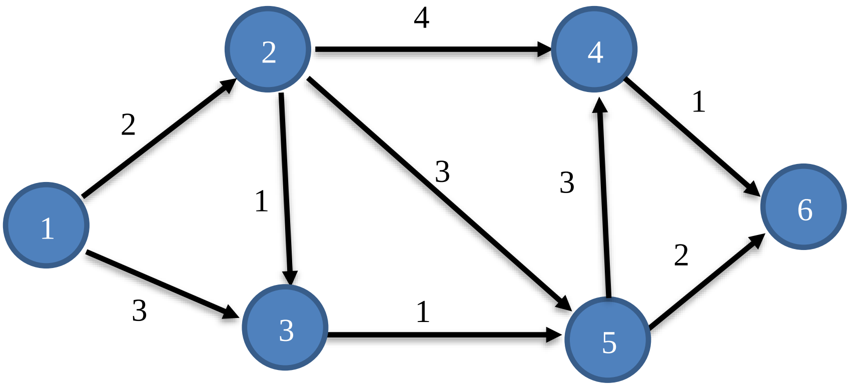
1- List node
2- List edge
3- Find paths from node 1 to node 4 in the network

Solution:

1- $N = \{1,2,3,4\}$
2- $E = \{(1,2),(1,3),(2,3),(2,4),(3,4)\}$
3- The path from 1 to 4
   - $(1,2),(2,4)$
   - $(1,2),(2,3),(3,4)$

- (1,3), (3,4)

Example 2: Consider the digraph below. The labels next to each edge represent that edge's length. What is the shortest path from node 1 to node 6



Solution :

Shortest path :

- (1,3), (3,5), (5,6)
- Also: (1,2), (2,3), (3,5), (5,6)

Shortest path =6

8.4.2 Dijkstra's algorithm

Dijkstra's algorithm or (Dijkstra's shortest path first algorithm) or SPF algorithm.

Is an algorithm for finding the shortest paths among nodes in a graph. It was found by Edsger W. Dijkstra in 1956. The idea beyond the algorithm is picking the unvisited vertex with the lowest distance, calculating the distance through each unvisited neighbor, then updating the neighbor’s distance if smaller, marking the visited node to be red when done with neighbors.

Although the original algorithm found the shortest path between two given nodes, but also there is a common variant that fires a single node by considering it as a (Source node) and finds the shortest path from the source node to all other nodes in the graph, and that will produce what is called the shortest-path tree. One uses the algorithm to find the shortest path from a single source node to a single destination one. For example, determining the shortest way between two cites.

8.4.2.1 Methodology

First, Dijkstra’s algorithm uses integer or real numbers as labels. The starting node is called the initial node. The algorithm will assign some initial distance values from initial nodes to others than trying to improve them step by step as described below:

1- Assign to every node a tentative distance value: set it to zero for our initial node and to infinity for all other nodes.

2- Set the initial node as current. Mark all other nodes unvisited. Create a set of all the unvisited nodes called the unvisited set.

3- For the current node, consider all of its unvisited neighbors and calculate their tentative distances. Compare the newly calculated tentative distance to the current assigned value and assign the smaller one. For example, if the current node A is marked with a distance of 6, and the edge connecting it with a neighbor B has length 2, then the distance to B (through A) will be 6 + 2 = 8. If

B was previously marked with a distance greater than 8 then change it to 8. Otherwise, keep the current value.

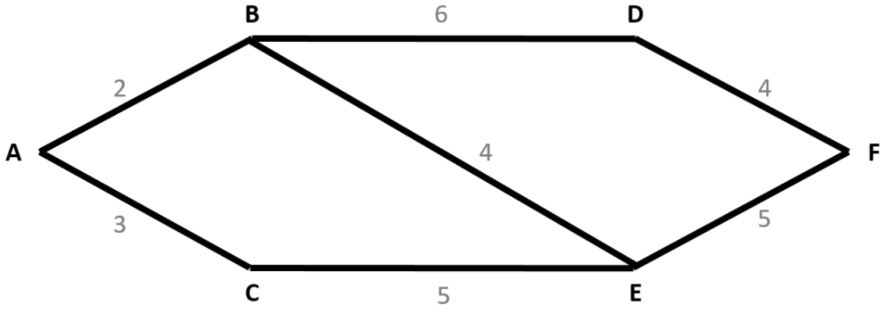
4- When we are done considering all of the neighbors of the current node, mark the current node as visited and remove it from the unvisited set. A visited node will never be checked again.

5- If the destination node has been marked visited (when planning a route between two specific nodes) or if the smallest tentative distance among the nodes in the unvisited set is infinity (when planning a complete traversal; occurs when there is no connection between the initial node and remaining unvisited nodes), then stop. The algorithm has finished.

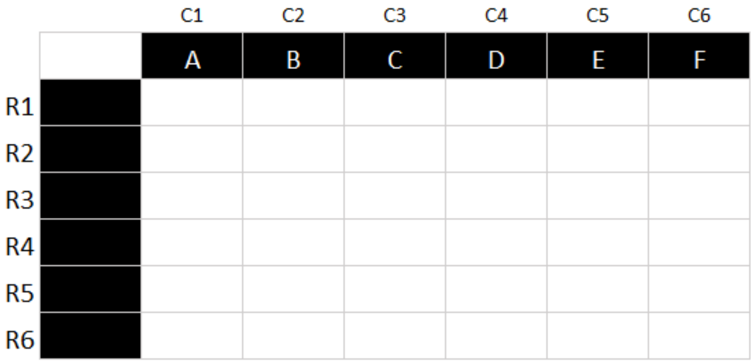
6- Otherwise, select the unvisited node that is marked with the smallest tentative distance, set it as the new “current node“, and go back to step 3

8.4.3 Example:

We are going to find the shortest path from A to F, using the following graph.

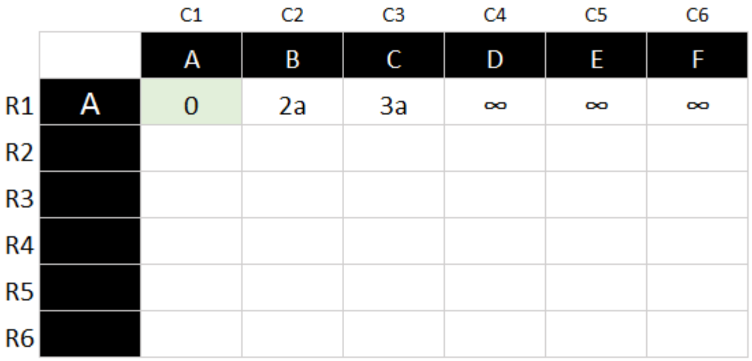


First, create a table like Table (a) below with a column for each node in the network excluding the starting node(A).



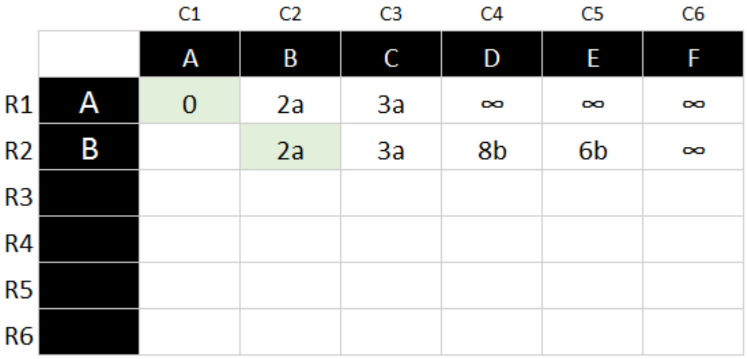
		C1	C2	C3	C4	C5	C6
		A	B	C	D	E	F
R1							
R2							
R3							
R4							
R5							
R6							

Since we are going to start from point A, we assign value for the first row as A and the value of A to A is 0, and then calculate the value for all the connected nodes, assign infinity(∞) for the rest. We also put a lower cap of the letter to indicate this value is calculated based on coming from which note. Just like the chart below.



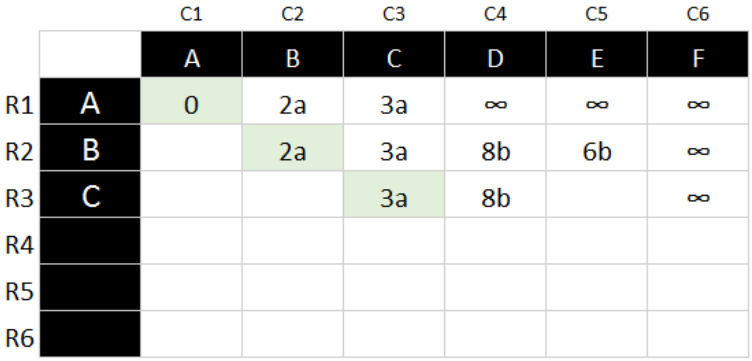
		C1	C2	C3	C4	C5	C6
		A	B	C	D	E	F
R1	A	0	2a	3a	∞	∞	∞
R2							
R3							
R4							
R5							
R6							

Copy the smallest value to the next row, and assign repeat the calculation of the new node to the rest of the connected node. Node B is not connected to C, so we have just copied the calculated value over.



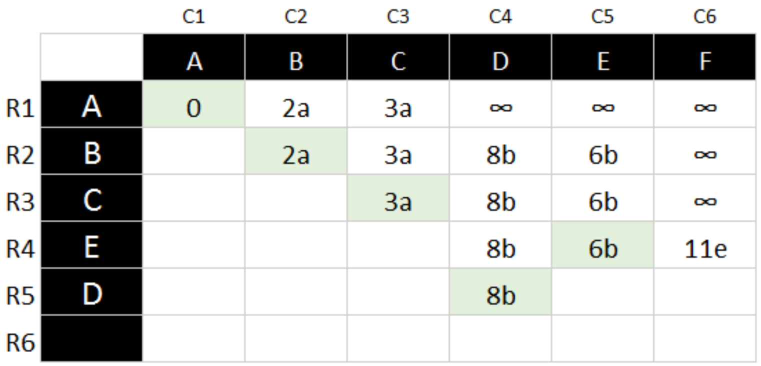
		C1	C2	C3	C4	C5	C6
		A	B	C	D	E	F
R1	A	0	2a	3a	∞	∞	∞
R2	B		2a	3a	8b	6b	∞
R3							
R4							
R5							
R6							

Repeat the above process until you find all the values for each node.



		C1	C2	C3	C4	C5	C6
		A	B	C	D	E	F
R1	A	0	2a	3a	∞	∞	∞
R2	B		2a	3a	8b	6b	∞
R3	C			3a	8b		∞
R4							
R5							
R6							

If we calculate the value for node C to node E, the value will be 8 which is bigger than 6 which we had calculated early. Hence, we will not accept the new value but kept the original value.



		C1	C2	C3	C4	C5	C6
		A	B	C	D	E	F
R1	A	0	2a	3a	∞	∞	∞
R2	B		2a	3a	8b	6b	∞
R3	C			3a	8b	6b	∞
R4	E				8b	6b	11e
R5	D				8b		
R6							

This is the result for all the nodes which start from node A. If you would like to find out the initial node to other nodes, you will have to repeat the above process.

How to read the chart?

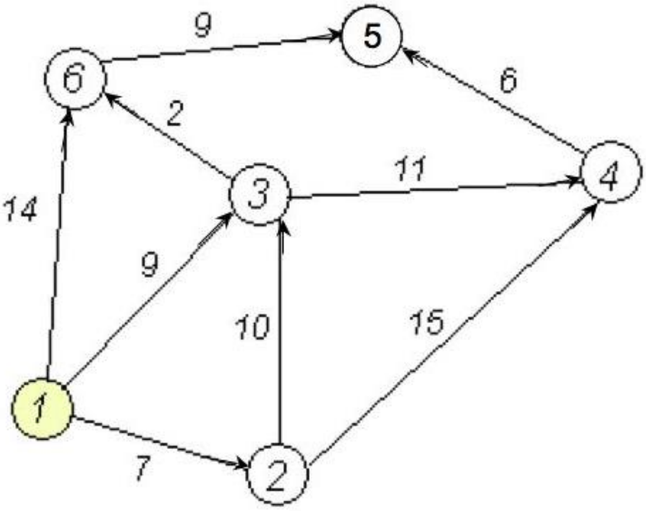
For example, if you want to find out the shortest path from, we start reading from F. At row R4, node F, it said 11e; this means to reach F is from node E, we follow the path to find E value, which is 6b, from 6b it brings us to 2a and finally it led us to 0a.

Now we can establish the path, F – E – B – A, by reversing the sequence, we knew the shortest path from node A to F is A – B – E – F.

In the next article, I will put this Dijkstra's algorithm into C# code, and demonstrate more complicated calculation.

8.5 Exercise

1- Find the shortest path from node 1 to all other nodes using Dijkstra’s algorithm



2- What's a vertex? What's an edge?