NEAR EAST UNIVERSITY

Faculty of Engineering

Department of Computer Engineering

IP Routing

Graduation Project
COM-400

Student: Dawood Ahmed Ghani/992177

Supervisor: Mr. Izzet Agorn

Lefkosa-2004

ACKNOWLEDGEMENT

I want to thanks Mr. Izzet Agoren to be my advisor, under his guidance, I successfully overcome many difficulties and learn a lot about IP Routing in Computer networks. In each discussion he explained my questions patiently, and I felt my quick progress from his advice. He always helps me a lot either in my study or in my life. I asked him many question in Computer Networks and he always anwered my questions quickly and in details.

I also want o thanks my NEU friends :Irfan Javed, Taimoor Hussain, Javed Afzal, Dawood Saleem, Ayoub Saleem, Atif Muneer and Rizwan Aslam. Being with make my time full of fun and systematic.

Finally, I want to thank my family, especially my parents. Without their endless support and love for me. I would never achieve my current position.

ABSTRACT

IP Routing defines the LAN, WAN, Protocols technically.

This project focuses on the basic concepts and techniques used in LAN and WAN technologies. It defines the basic concepts of networking including OSI model and TCP/IP protocols in detail.

This project also presents the LAN and WAN configuration by using different techniques. You can also understand the how packet transmission occur in computer networks.

This project shows you how IP address are classified into different classes and their use in computer networks.

INTRODUCTION

A Network is a group of computers and other devices that connected to each other. The most common types of Networks are LAN, WAM and MAN and on which software and hardware components added.

Open Systems Interconnection (OSI) developed a model whose functionality geared toward the needs of communicating between multiple manufacturers. In this model, the individual services that are required for communication between computers arranged in seven layers that build on one facilitate communication and sharing of information.

An IP address is a set of four numbers, or octets, which can range in value between 0 and 255. Each octet is separated by a period. Some examples are shown here:

- 34.120.66.79
- 200.200.20.2
- 2.5.67.123
- 107.219.2.34

These addresses are actually broken down into three distinct classes. These are known as class A, class B, and class C addresses

If definitions are helpful to you, here's some wire head vocabulary to get you started

- Address -- the unique number id assigned to one host or interface in a network
- Subnet -- a portion of a network sharing a particular subnet address
- Subnet mask -- a 32-bit combination used to describe which portion of an address refers to the subnet and which part refers to the host
- Interface -- a network connection

TABLE OF CONTENTS

Chapter 2 Local Area Network

Chapter 3 IP Addressing and Subnetting

Chapter 4 WAN Technologies

CHAPTER 1

Networking Overview

1.1 Introduction

This chapter defines the networking .It also presents the basic points, software components and hardware components used in networking.

This chapter also helps you to understand the different models of networking. It focuses on the OSI model, TCP/IP Protocols, routing Protocols and their functionality.

1.2 What is Network?

A network is a collection of machines that have been linked together physically and on which software components have been added to facilitate communication and sharing of information. By this definition, a network might be as simple as the computers shown in Figure 1.1. In fact, Figure 1.1 shows the simplest kind of network that can be created: two machines connected by a piece of coaxial cable. This example is deceptively simple and hides a fairly complex arrangement of pieces that must work together to enable these two machines to communicate.

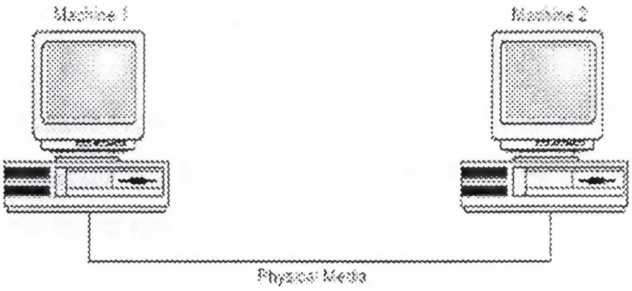


Fig1.1:-An example of a simple network.

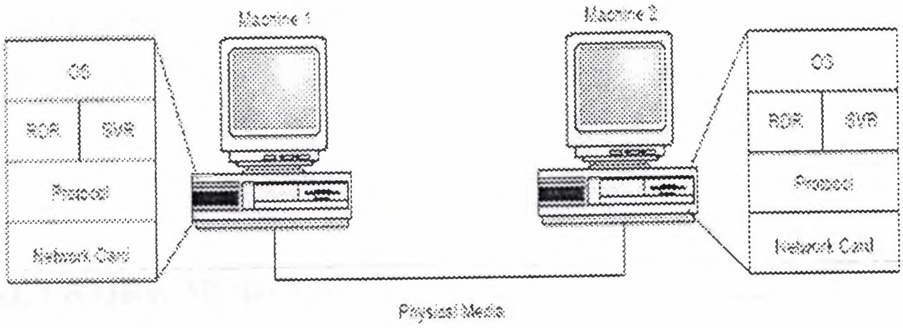


Fig 1.2 :-shows the main hardware and software components required to enable communication between these two machines.

1.2.1 Operating System (OS)

This is the operating system; more specifically, this is the user interface that you use to connect to other computers on the network.

1.2.2 Redirector (RDR)

The RDR, or redirector, intercepts requests for resource access and, if required, passes the request to the network. The redirector (or client, if you will) can talk only to a server that understands what it is talking about, or that has a common frame of reference.

1.2.3 Server

The server component receives and services the requests from a redirector.

1.2.4 Protocol

The requests from the redirector and the responses from the server are encapsulated in a transport protocol. The protocol (such as TCP/IP) then finds the other computer and moves the data to the target machine.

1.2.5 Network Card.

The protocol works with the Network Card to physically move the data to the other computer.

1.3 NETWORK MODELS

Networks generally fall into one of two broad network categories:

- Client/server networks
- Peer-to-peer networks

1.3.1 Client/Server-Based Networking

A client/server network consists of a group of user-oriented PCs (called *clients*) that issue requests to a server. The client PC is responsible for issuing requests for services to be rendered. The server's function on the network is to service these requests. Servers generally are higher-performance systems that are optimized to provide network services to other PCs. The server machine often has a faster CPU, more memory, and more disk space than a typical client machine. Some examples of client/server-based networks are Novell NetWare, Windows NT Server, and Banyan Vines. Some common server types include file servers, mail servers, print servers, fax servers, and application servers.

1.3.2 Peer-to-Peer Networking

A peer-to-peer network consists of a group of PCs that operate as equals. Each PC is called a *peer*. The peers share resources (such as files and printers) just like in a server-based network, although no specialized or dedicated server machines exist. In short, each PC can act as a client or a server. No one machine is set up with a higher-powered set of devices, nor is any one PC set up simply to provide one service (such as storing files). Small networks—usually with fewer than 10 machines—can work well in this configuration.

1.4 LOCAL AND WIDE AREA NETWORKS

Networks come in all shapes and sizes. Network administrators often classify networks according to geographical size. Networks of similar size have many similar characteristics, as you will learn in later chapters. The following are the most common size classifications:

- Local area networks (LANs)
- Wide area networks (WANs)

1.4.1 Local Area Networks (LANs)

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 a campus. LANs are characterized by the following:

- They transfer data at high speeds (higher bandwidth).
- They exist in a limited geographical area.
- Connectivity and resources, especially the transmission media,usually are managed by the company running the LAN.

1.4.2 Wide Area Networks (WANs)

A wide area network (WAN) interconnects LANs. A WAN can be located entirely within a state or a country, or it can be interconnected around the world. WANs are characterized by the following:

- They exist in an unlimited geographical area.
- They usually interconnect multiple LANs.
- They often transfer data at lower speeds (lower bandwidth).
- Connectivity and resources, especially the transmission media,usually are managed by a third-party carrier such as a telephoneor cable company.

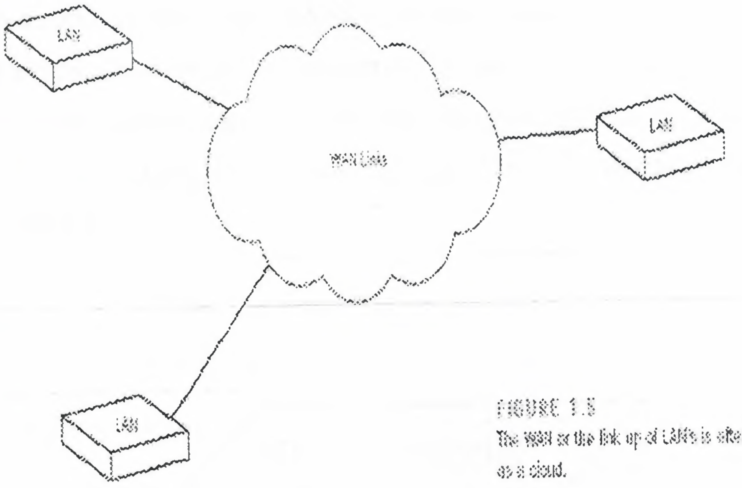


FIGURE 1.5
The WAN or the link up of LANs is often shown as a cloud.

1.5 ISO/OSI 7 Layer Model

At the beginning of the 1980s, the *International Organization for Standardization* (ISO) together with *Open Systems Interconnection* (OSI) developed a model whose functionality was geared toward the needs of communicating between multiple manufacturers. In this model, the individual services that are required for communication between computers are arranged in seven layers that build on one another. Each layer provides specific services and makes the results available to the next layer. ISO standardized this model when existing networks were already being operated. As a result, the ISO/OSI 7 Layer Model represents an ideal case to a certain extent. Figure 1-1 illustrates OSI model layering.

1.5.1 Physical Layer

The Physical layer regulates the transmission of unstructured bit streams over a transmission medium with regard to transmission speed, representation of the signals, and connection technique. Depending on the transmission medium, the Physical layer is recognized by the corresponding board, the connection elements to the network, and the transmission cable. Ethernet (IEEE 802.3) or Token Ring (IEEE 802.5) is frequently used as a transmission media for LANs. Fiber Distributed Data Interface (FDDI) ANSI standard is a typical transmission medium in the realm of Metropolitan Area Networks. For the most part, public networks are used for wide area network data transmission (Datex-P (X.25)), Integrated Services Digital Network (ISDN), analog telephone network (modem).

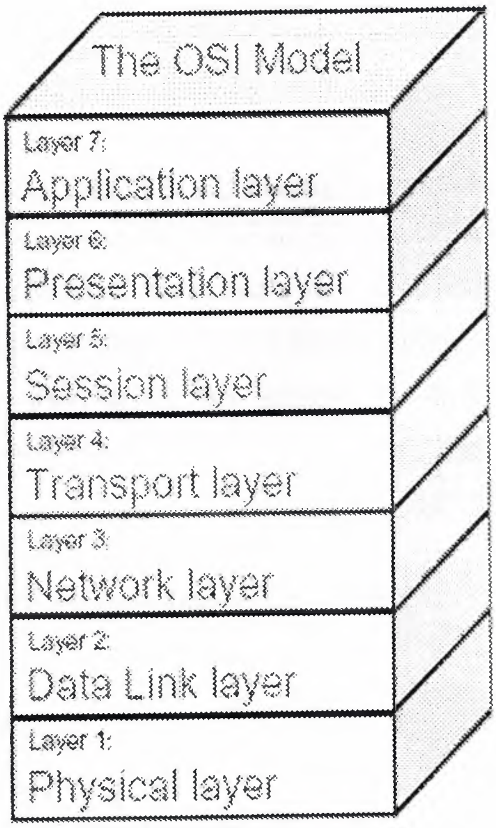


Fig 1.3:-OSI 7 Layer Model

1.5.2 Data Link Layer

The Data Link layer addresses the stations attached to the transmission medium and the next higher protocol that used the transmission service. This information is required for demultiplexing on the receiver side. For the most part, the transmission of information units is assured by a checksum which permits error detection and elimination.

If necessary, flow control is also conducted. Packets can now be recognized from the previously unstructured bit stream. Examples of protocols for the Data Link layer are

- LAPB (Link Access Procedure) (X.25)
- Ethernet V.2, Ethernet IEEE 802.3, Token Ring IEEE 802.5, and
- Token Bus IEEE 802.4

1.5.3 Network Layer

The Network layer protocol ensures that messages reach their destination system via an optimal route. To do this, a system uses a routing table to determine the next, directly accessible computer on the route to the packet's destination and then transmits to it with the aid of a service which is made available by the Data Link layer. This next computer is either the destination itself or the next gateway to the destination. Examples of protocols for the Network layer are

- Internet Protocol (IP)
- Connectionless-Mode/Connection-Mode (CLNS/CONS)

1.5.4 Transport Layer

The Transport layer handles the transport of messages between communication partners, controls the flow of data, and defines the transport quality (directional, non-directional) of the data transmission. Examples of protocols for the Transport layer are

- Transfer Control Protocol, User Datagram Protocol (TCP, UDP)
- TP-0 to TP-4 (OSI)

1.5.5 Session Layer

The Session layer allows users on different machines to establish sessions between them. A session allows ordinary data transport, as does the Transport layer, but can also provide enhanced services, such as authentication, which are useful in some applications. A session might allow a user to log into a remote time-sharing system or to transfer a file between two machines. An example of the services provided by the Session layer is management of dialogues. Sessions can allow traffic to go in both directions at the same time, or in only one direction at a time. If traffic can only go one way at a time, the Session layer keeps track of whose turn it is. Another example of the services provided by the Session layer is reestablishment of interrupted connections.

1.5.6 Presentation Layer

The Presentation layer stipulates a transfer syntax. The *transfer syntax* represents a coding agreement for the data to be transferred. Data is represented in different ways in various computer architectures (for example, representation of floating point numbers; character codes; ASCII [American Standard Code for Information Interchange] or EBCDIC [Extended Binary-coded Decimal Interchange Code], and different byte sequences: high-byte or low-byte). In the case of completely different computer architectures, successful data transmission would be of no benefit because the data is interpreted completely different on some systems. This layer is implemented using XDR (External Data Representation), which balances the interpretation differences. It transforms C basic structures into XDR data structure and vice versa. Any system can communicate via the network by using XDR.

1.5.7 Application Layer

The Application layer represents the interface to the application process. Basic functions such as file transfer, virtual terminal, and job transfer (remote execution) are realized.

Examples of the Application layer are

- SMTP (Simple Mail Transfer Protocol)
- FTP (File Transfer Protocol)
- TELNET (Remote Terminal Protocol)
- SNMP (Simple Network Management Protocol)

1.5.8 Hardware Layers

The Physical layer regulates the transmission of unstructured bit streams over a transmission medium with regard to transmission speed, representation of the signals, and connection technique. Depending on the transmission medium, the Physical layer is recognized by the corresponding board, the connection elements to the network, and the transmission cable. Ethernet (IEEE 802.3) or Token Ring (IEEE 802.5) are frequently used

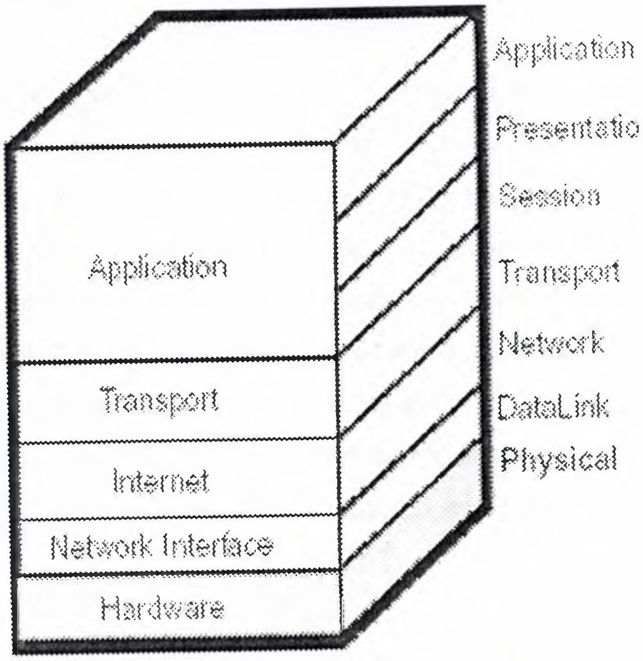


Fig 1.4 TCP/IP Model Hardware Layer

as transmission media for LANs. FDDI (ANSI standard) is a typical transmission medium in the realm of Metropolitan Area Networks. For the most part, public

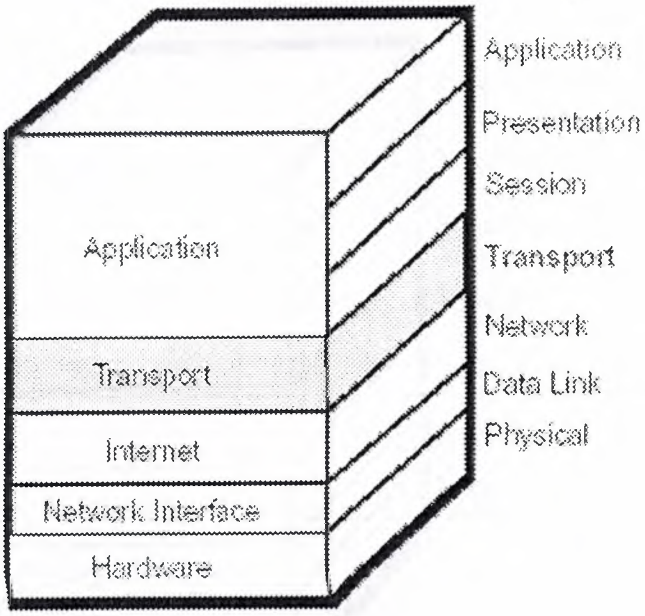
networks are used for WAN data transmission (Datex-P (X.25)), ISDN, analog telephone network
(modem). Figure 1-3 compares the Hardware layer of the TCP/IP mode to the Physical layer of the ISO/OSI reference model.

1.5.9 Internet Layer

The function of this layer is the same as the ISO/OSI network layer. The Internet layer uses IP and ICMP. IP is responsible for fragmenting and routing data while ICMP assists routing, and performs error detection and other network management tasks. Figure 1-5 compares the Internet layer of the TCP/IP model to the Network layer of the ISO/OSI reference mode.

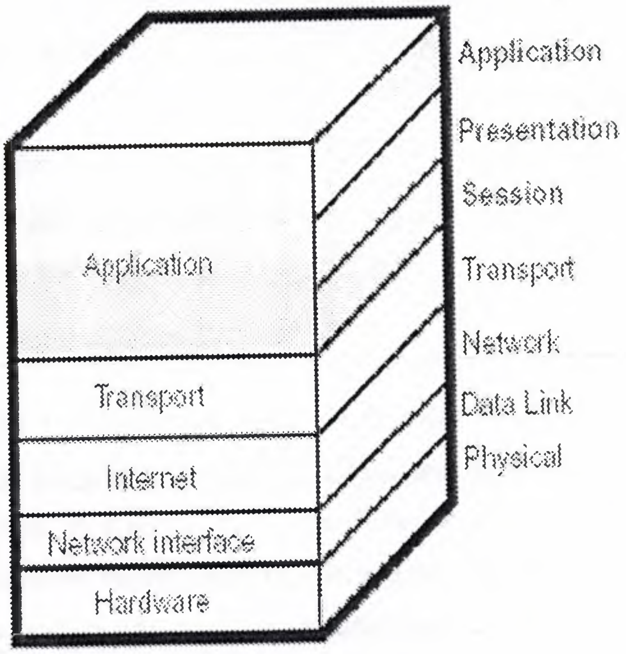
1.5.10 Transport Layer

The Transport layer uses TCP and UDP. TCP provides a reliable virtual circuit (connection-oriented) for application processes. *Connection-oriented* means that a connection must be established between systems before they can exchange data.
Furthermore, TCP uses acknowledgments between systems to ensure data delivery. UDP is a connectionless protocol for application processes. It is faster than TCP for certain applications since it does not require setting up a connection and handling acknowledgments. It is also known as a *stateless* protocol because systems using UDP to exchange data have no indication of the operational status of one another. Figure 1-6 compares the Transport layer of the TCP/IP model to the Transport layer of the ISO/OSI reference model.



1.5.11 Application Layer

The top layer of TCP/IP is the Application layer. This includes all processes that use Transport layer protocols to deliver data to the Internet layer. There are many application protocols and new protocols are frequently added. Figure 1-7 compares the Application layer of the TCP/IP model to the Application, Presentation, and Session layers of the ISO/OSI reference model.



1.6 What Is a Protocol?

A protocol is a set of rules governing the exchange of data between two entities. These rules cover

- Syntax – Data format and coding_
- Semantics – Control information and error handling
- Timing – Speed matching and sequencing

1.6.1 TCP/IP

TCP/IP is a set of protocols developed to allow cooperating computers to share resources across a network. TCP/IP provides services to many different types of computers, operating systems, and networks. Types of networks supporting TCP/IP range from local area networks, such as Ethernet, FDDI, and Token Ring, to wide-area networks such as T1 (telephone lines), X.25, and ATM. TCP/IP supports important network services such as

- File transfer
- Remote login
- Electronic mail

The Transmission Control Protocol/Internet Protocol (TCP/IP) is an industry-standard suite of protocols designed to be routable, robust, and functionally efficient. TCP/IP was originally designed as a set of *Wide Area Network (WAN)* protocols for the express purpose of maintaining communication links and data transfer between sites in the event of an atomic or nuclear war. Since those early days, development of the protocols has passed from the hands of the military and has been the responsibility of the Internet community. The evolution of these protocols from a small, four-site project into the foundation of the worldwide Internet has been extraordinary. And, despite more than 25 years of work and numerous modifications to the protocol suite, the ideas inherent to the original specifications are still intact. Following are some of the advantages of TCP/IP:

1.7 Peer-to-Peer Communication

When systems exchange data using the TCP/IP model, they are performing *peer-to-peer* communication. Peer-to-peer communication is the ability of a specific layer to communicate with the corresponding layer on another host At each layer, the data or message is encapsulated and header information about the corresponding protocol layer added. This information is key in the peer-to-peer communication and is used to de-encapsulate and direct the message to the appropriate application.

The TCP/IP model includes a number of protocols to insure proper communication between corresponding layers of networked machines.

(See Table 1.1.)

TCP/IP Protocol	TCP/IP Layer
NFS, NIS+, DNS, telnet, ftp, rlogin, SMTP, DHCP, and SNMP	Application
TCP and UDP	Transport
IP, ARP, RARP, ICMP, and RIP	Internet
SLIP (Serial Line IP), PPP (Point-to-Point Protocol), and Ethernet	Network Interface

Table1.1:-TCP/IP Protocol Stack

Protocol	Description
ARP	Address Resolution Protocol defines the method used to map a 32-bit IP address to a 48-bit Ethernet address.
RARP	Reverse Address Resolution Protocol is the reverse of ARP. It maps a 48-bit Ethernet address to a 32-bit IP address.
SLIP	Serial line IP encapsulates IP datagram on serial lines.
PPP	PPP Point-to-Point Protocol transmits datagram over serial point-to-point links.

Table 1.2 TCP/IP Network Interface Layer Protocol Descriptions

Protocol	Description
IP	Internet Protocol determines the path a packet must take, based on the receiving host's IP address.
ICMP	Internet Control Message Protocol communicates error messages and other controls within IP datagrams.

Table 1-3 TCP/IP Internet Layer Protocol Descriptions

Protocol	Description
TCP	Transmission Control Protocol is a connection oriented protocol that provides the full duplex, stream service on which many application protocols depend.
UDP	User Datagram Protocol provides datagram delivery service.

Table 1-4 TCP/IP Transport Layer Protocol Descriptions

Protocol	Description
NFS	Network File System is an Application layer protocol which provides file services for the Solaris operating system.
DNS	Domain Name System is a database used by the Internet to provide electronic mail routing information and to map between host names and IP addresses.
FTP	File Transfer Protocol transfers a file by copying a complete file from one system to another system.
Telnet	A service which enables terminals and terminal-oriented processes to communicate on a network running TCP/IP.
rlogin	A service offered by UNIX® systems that allows users of one machine to connect to other UNIX systems across an Internet and interact as if their terminals connected to the machines directly.
DHCP	Dynamic Host Configuration Protocol automates the assignment of IP addresses in an organization's network.
SMTP	Simple Mail Transfer Protocol transfers electronic mail messages from one machine to another.
SNMP	Simple Network Management Protocol is the language that allows for the monitoring and control of network

	devices.
POP-3	Post Office Protocol, Version 3, allows users to pick up email across the network from a central server.
HTTP	HTTP Hypertext Transfer Protocol is used by the World Wide Web to exchange text, pictures, sounds, and other multimedia information via a graphical user interface (GUI)
RIP	RIP Routing Information Protocol is used by network devices to exchange routing information.

Table 1-5 TCP/IP Application Layer Protocol Descriptions

Chapter 2

Local Area Network

2.1 Introduction

This chapter provides you important benefits of LAN, LAN topologies and hardware components. The architecture of LAN also described. It also helps you to understand the Ethernet operations in full and half duplex modes, LAN segmentation by using routers and switches.

2.2 Benefits of a LAN

There are numerous benefits to using LAN. These benefits are important and sometimes critical to an organization's success. These benefits include

- Resource sharing
- Workgroup synergy
- Management
- Centralized
- Decentralized
- Data access and integration
- Economic resources

2.3 Network Topologies

A topology defines the arrangement of nodes, cables, and connectivity devices that make up the network. The most common and the most important for understanding the Ethernet
and token-ring topologies

- Bus topologies
- Ring topologies
- Star topologies

- Mesh topology

2.3.1 Bus Topologies

A bus physical topology is one in which all devices connect to a common, shared cable.

2.3.2 Ring Topologies

Ring topologies are wired in a circle. Each node is connected to its neighbors on either side, and data passes around the ring in one direction only

2.3.3 Star Topologies

Star topologies require that all devices connect to a central hub

2.3.4 Mesh Topology

A popular test subject is the mesh topology. In *mesh* topology every device is directly connected to every other device on the network.

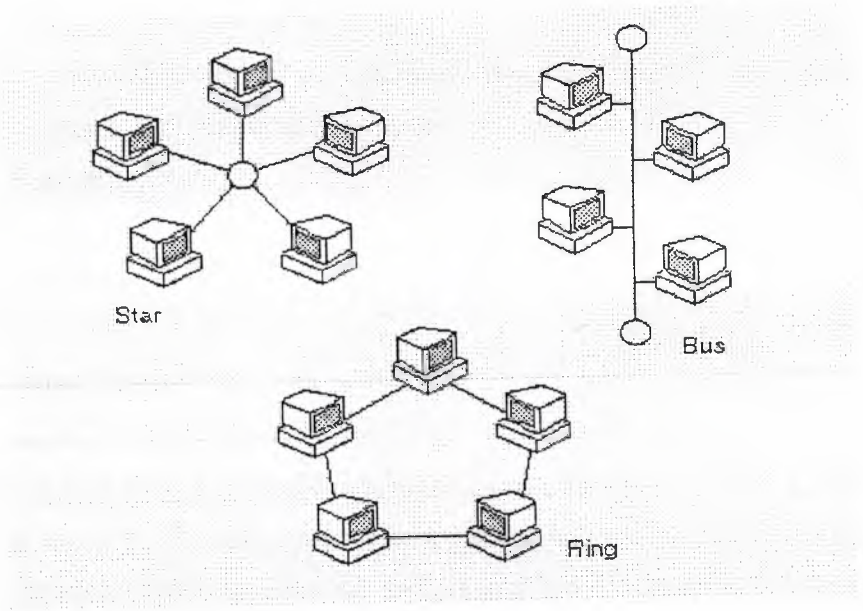


figure 2.1

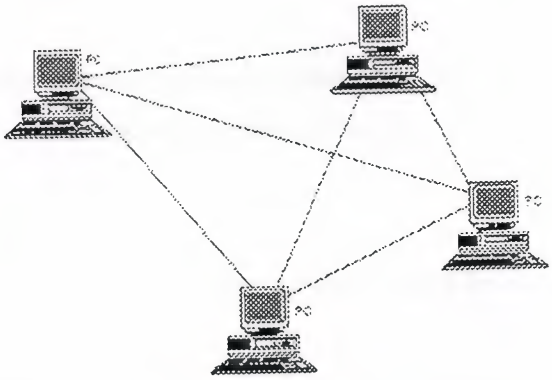


figure 2.2 A mesh topology.

2.4 LAN devices

2.4.1 REPEATERS

A repeater is a network device that repeats a signal from one port onto the other ports to which it is connected. Repeaters operate at the OSI Physical layer. A repeater does not filter or interpret—it merely repeats (regenerates) a signal, passing all network traffic in all directions.

2.4.2 HUBS

Hubs, also called wiring concentrators, provide a central attachment point for network cabling. Hubs come in three types:

- Passive
- Active
- Switching

2.4.2.1 Passive Hubs

Passive hubs do not contain any electronic components and do not process the data signal in any way. The only purpose of a passive hub is to combine the signals from several network cable segments. All devices attached to a passive hub receive all the packets that pass through the hub.

2.4.2.2 Active Hubs

Active hubs incorporate electronic components that can amplify and clean up the electronic signals that flow between devices on the network.

2.4.2.3 Intelligent Hubs

- Intelligent hubs are enhanced active hubs. Several functions can add intelligence to a hub:
- *Hub management.* Hubs now support network management protocols that enable the hub to send packets to a central network console. These protocols also enable the console to control the hub; for example, a network administrator can order the hub to shut down a connection that is generating network errors.
- *Switching.* The latest development in hubs is the switching hub, which includes circuitry that very quickly routes signals between ports on the hub. Instead of repeating a packet to all ports on the hub, a switching hub repeats a packet only to the port that connects to the destination computer for the packet. Many switching hubs have the capability of switching packets to the fastest of several alternative paths. Switching hubs are replacing bridges and routers on many networks.

2.4.3 Bridges

Functions the same as a repeater, but can also divide a network in order to reduce traffic problem. A bridge can also connect unlike network segments (i.e. token ring and Ethernet). Bridges create routing tables bases on the source address. If the bridge can't find the source address it will forward the packets to all segments.

2.4.4 Routers

Bridges are suitable for relatively simple networks, but bridges have certain limitations that become more significant in complex network situations. One limitation of bridges is that packets intended for all people on a subnet, also known as a broadcast, are received by every single device on the network. By being able to section off a LAN segment into different network segments, routers allow you to control and group devices that work together to be on the same network segment.

Routers organize the large network in terms of logical network segments. Each network segment is assigned an address so that every packet has both a destination network address and a destination device address.

Routers come in two general types:

- *Static Routers*. These routers do not determine paths. Instead, you must configure the routing table,, specifying potential routes for packets.
- *Dynamic Routers*. These routers have the capability to determine routes (and to find the optimum path among redundant routes) based on packet information and information obtained from other routers.

2.4.5 Brouters

A brouter is a router that also can act as a bridge. A brouter attempts to deliver packets based on network protocol information, but if a particular Network layer protocol isn't supported, the brouter bridges the packet using device addresses.

2.4.6 Gateways

Often used as a connected to a mainframe or the internet. Gateways enable communications between different protocols, data types and environments. This is achieved via protocol conversion, whereby the gateway the gateway strips the protocol stack off of the packet and adds the appropriate stack for the other side.

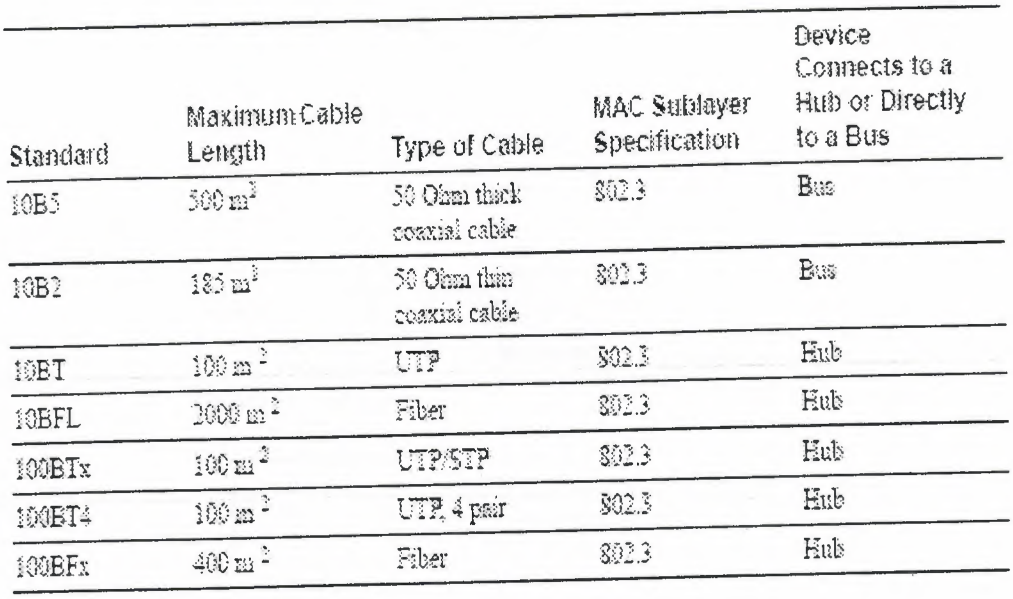
2.5 LAN Architecture

LAN architecture can be divided into two categories; software and hardware.

- Software An end-user application may use a software protocol suite such as the Transfer Control Protocol/Internet Protocol (TCP/IP) or ISO/OSI
- Hardware The physical network medium is designed to carry signals encoded with information, such as coaxial, twisted-pair cable, or fiber-optical materials carrying multi band modulated laser light.

2.6 Ethernet

Ethernet is a very popular local area network architecture based on the CSMA/CD access method. The original Ethernet specification was the basis for the IEEE 802.3 specifications. In present usage, the term "Ethernet" refers to original Ethernet (or Ethernet II, the latest version) as well as the IEEE 802.3 standards. The different varieties of Ethernet networks are commonly referred to as *Ethernet topologies*. Typically, Ethernet networks can use a bus physical topology, although, as mentioned earlier, many varieties of Ethernet such as 10BASE-T use a star physical topology and a bus logical topology. Ethernet networks, depending on the specification, operate at 10- or 100Mbps using base band transmission. Each IEEE 802.3 specification prescribes its own cable types.



Standard	Maximum Cable Length	Type of Cable	MAC Sublayer Specification	Device Connects to a Hub or Directly to a Bus
10B5	500 m[3]	50 Ohm thick coaxial cable	802.3	Bus
10B2	185 m[3]	50 Ohm thin coaxial cable	802.3	Bus
10BT	100 m [2]	UTP	802.3	Hub
10BFL	2000 m [2]	Fiber	802.3	Hub
100BTx	100 m [2]	UTP/STP	802.3	Hub
100BT4	100 m [2]	UTP, 4 pair	802.3	Hub
100BFx	400 m [2]	Fiber	802.3	Hub

table 2.1 Ethernet Standards

2.7 Full- and Half-Duplex Ethernet Operation

The use of full-duplex Ethernet can relieve some of the congestion. Half- and full-duplex Ethernet imply the use of 10BT or some other hub-based topology. Ethernet hubs were created with the advent of 10BT. These hubs are essentially multi port repeaters; repeaters extend the bus concept of 10B2 and 10B5 by regenerating the same electrical signal sent by the original sender of the frame. Therefore, collisions can still occur, so CSMA/CD access rules continue to be used. Knowledge of the operation of Ethernet cards and the attached hub is important to a complete understanding of the congestion problems and a need for full-duplex Ethernet. Figure 4-4 outlines the operation of half-duplex 10BT with hubs.

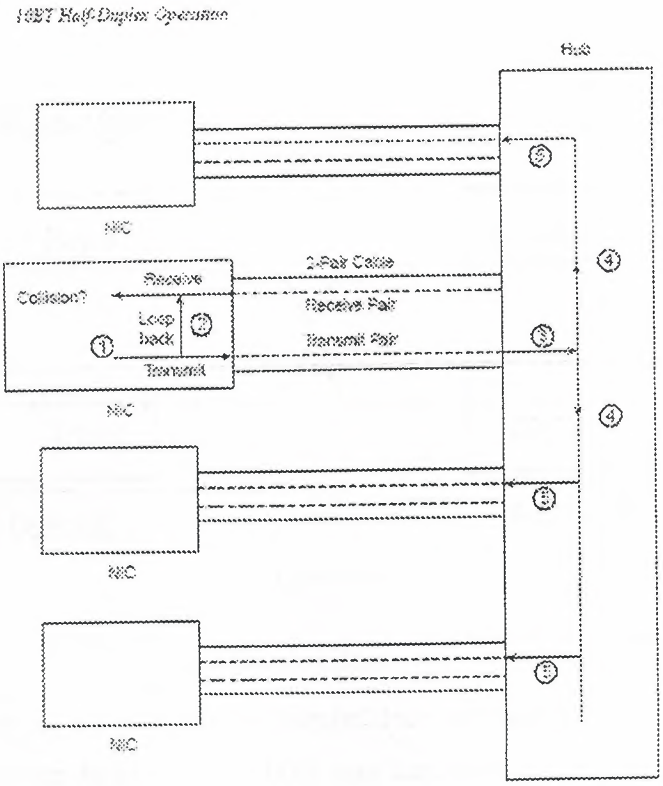


figure 2.3

The chronological steps illustrated in Figure2.2 are as follows:

1. The network interface card (NIC) sends a frame.
2. The NIC loops the sent frame onto its receive pair.
3. The hub receives the frame.
4. The hub sends the frame across an internal bus so all *other* NICs can receive the electrical signal.
5. The hub repeats the signal out of each receive pair to all other devices.

Because CSMA/CD rules are used when collisions could occur, full-duplex operation would not be useful. If a card is receiving a frame, it would not choose to also start sending another frame. Half-duplex operation is a side effect of the original design choice of retaining the CSMA/CD media access for 10BT networks. Full-duplex operation creates a situation whereby frames that are sent cannot collide with frames being received. Imagine the use of Ethernet between a pair of NICs instead of cabling the NIC to a hub. Figure 4-5 shows the full-duplex circuitry.

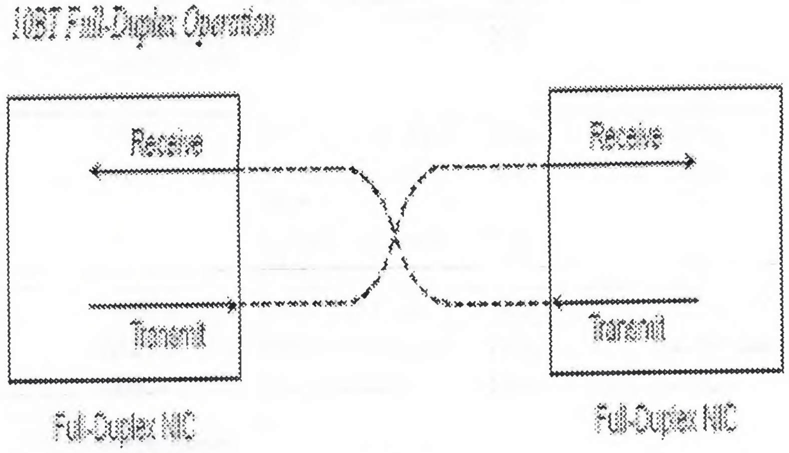


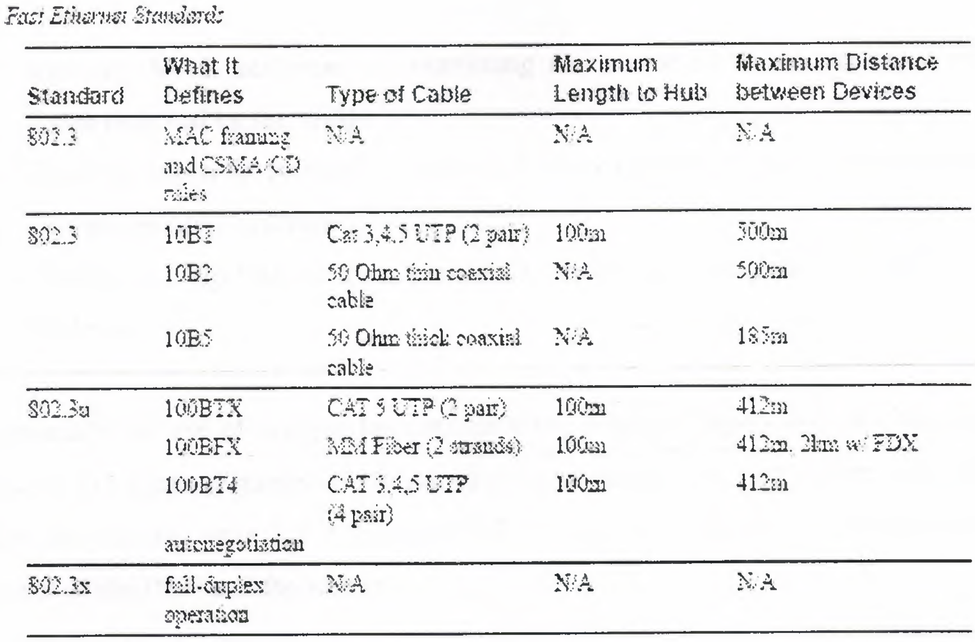
figure 2.4

Because no collisions are possible, the sender does not need to loop frames onto the receive pair, as shown in Figure 4-5. Both ends can send and receive simultaneously. This reduces Ethernet congestion related to all three points previously listed:

- Collisions do not occur; therefore, time is not wasted retransmitting frames.
- Waiting for others to send their frames is not necessary because there is only one sender for each twisted pair.
- There are 10 Mbps in each direction, increasing the available capacity (bandwidth).

2.8 Fast Ethernet

Fast Ethernet relieves congestion in some fairly obvious ways. Collisions and wait time are decreased when compared to 10 Mbps Ethernet, simply because it takes 90 percent less time to transmit the same frames. Capacity is greatly increased as well—with 1250 byte frames, one million frames per second theoretical maximum can be reached.



Fast Ethernet Standards

Standard	What It Defines	Type of Cable	Maximum Length to Hub	Maximum Distance between Devices
802.3	MAC framing and CSMA/CD rules	N/A	N/A	N/A
802.3	10BT	Cat 3,4,5 UTP (2 pair)	100m	300m
	10B2	50 Ohm thin coaxial cable	N/A	500m
	10B5	50 Ohm thick coaxial cable	N/A	185m
802.3u	100BTX	CAT 5 UTP (2 pair)	100m	412m
	100BFX	MM Fiber (2 strands)	100m	412m, 2km w/ FDX
	100BT4	CAT 3,4,5 UTP (4 pair)	100m	412m
	autonegotiation			
802.3x	full-duplex operation	N/A	N/A	N/A

table 2.2

2.9 ETHERNET LAN Segmentation

Advantages

Ethernet LAN segmentation has the following attributes:

- Overcomes distance limitations.
- Decreases or eliminates collisions, which should decrease latency and improve throughput.
- *Reduces the impact of broadcasts and multicasts, which should decrease latency* and improve throughput.
- Increases the amount of total bandwidth per user.
- Confines user traffic to different LAN segments

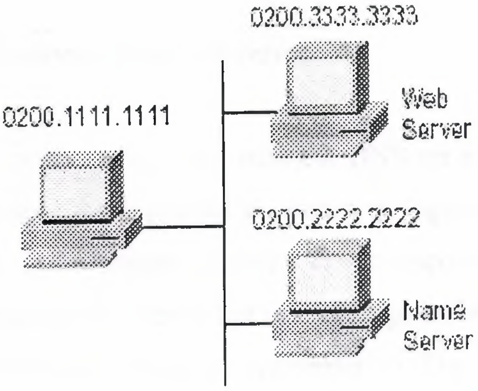
2.9.1 Transparent Bridging

Transparent bridging is the first of the three segmentation methods. The discussion on transparent bridging concludes with a list of other considerations unique to segmentation using bridges. Transparent bridges perform three key functions:

- Learning MAC addresses by examining the source MAC addresses of each frame received by the bridge
- Deciding when to forward a frame and when to filter a frame, based on the destination MAC address
- Creating a loop-free environment with other bridges using the Spanning-Tree Protocol

To appreciate the use of bridges for segmentation, consider Figure 4-6. A client first asks for a DNS name resolution, followed by connecting to a web server. All three devices are on the same LAN segment. ARP requests are used to find the MAC addresses of the DNS and the web server

.Example Protocol Flows—Single Ethernet Segment



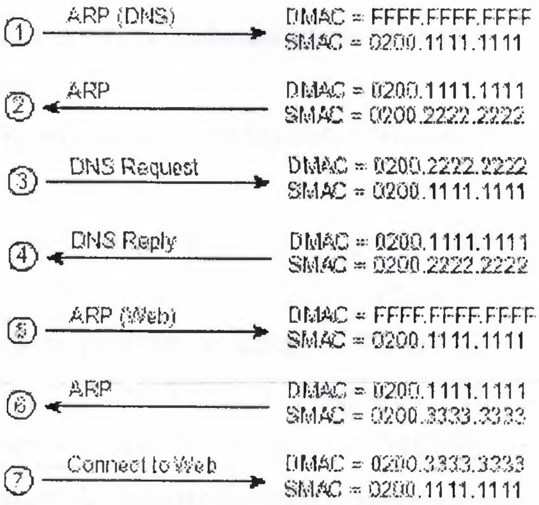


figure 2.5

The following list provides some additional text relating the steps shown in Figure 4-6:

1. The PC is preconfigured with the IP address of the DNS; it must ARP to find the DNS's MAC address.
2. The DNS replies to the ARP request with its MAC address, 0200.2222.2222.
3. The PC requests name resolution for the web server.
4. The DNS returns the IP address of the web server to the PC.
5. The PC does not know the web server's MAC address, so it sends an ARP broadcast to learn the MAC address.
6. The web server replies to the ARP, stating that its MAC address is 0200.3333.3333.
7. The PC can now connect to the web server.

Now consider the same protocol flow, but with the DNS on a separate segment and a transparent bridge separating the segments as shown in Figure. The computers act no differently, sending the same frames/packets. The transparent bridge forwards all broadcasts, all unicast destination frames not in its bridge table, and multicasts. Figure illustrates several important ideas related to segmentation. The ARP requests in Steps 1 *and 5 are forwarded by the bridge because they are broadcasts. However, the rest of the* frames from the client to the web server and back will not be forwarded by the bridge because the bridge knows that both MAC addresses are on the same Ethernet as its E0 interface. Also, because there is no redundant path through other bridges, there is no need to use the Spanning-

Tree Protocol to block interfaces and limit the flow of frames.

The following list provides the key features of transparent bridging,

- Broadcasts and multicast frames are forwarded by a bridge.
- Transparent bridges perform switching of frames using Layer 2 headers and Layer 2 logic and are Layer 3 protocol independent. This means that installation is simple because no Layer 3 address group planning or address changes are necessary. For example, because the bridge retains a single broadcast domain, all devices on all segments attached to the bridge look like a single subnet. Cisco might consider this *plug-and-play.*
- Store-and-forward operation is typical in transparent bridging devices. Because an entire frame is received before being forwarded, additional latency is introduced (as compared to a single LAN segment).
- The transparent bridge must perform processing on the frame, which also can increase latency (as compared to a single LAN segment).
- The following list addresses the concepts raised by objective 53 of the CCNA exam and provides the benefits of Ethernet LAN segmentation in light of transparent bridging. The comments in this list compare a single LAN segment versus multiple LAN segments separated by a transparent bridge:

Distance limitations are overcome because each segment can be built with the maximum distance for that type of Ethernet.

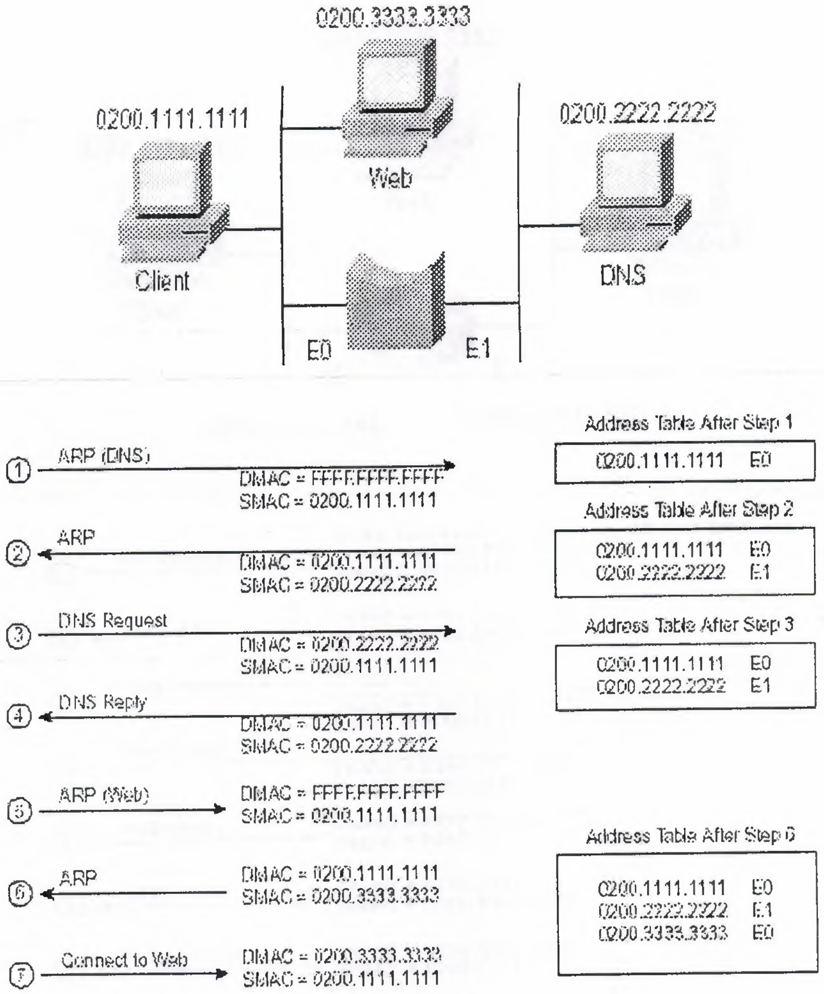
Collisions are decreased because some frames are filtered by the bridge.

Bridges do not reduce the impact of broadcasts/multicasts.

Total bandwidth is increased because each segment runs at 10 or 100 Mbps instead of a single 10 or 100 Mbps segment.

User traffic is confined to individual LAN segments for frames whose source and destination are on the same LAN segment. Bridges often allow administrative filters to limit the flow of frames as well.

Example Protocol Flows—Using a Transparent Bridge



figue 2.6

2.9.2 LAN Segmentation Using Routers

Segmenting LANs using routers is the second segmentation method, Figure illustrates a couple of key features.

Example Protocol Flows—Using a Router

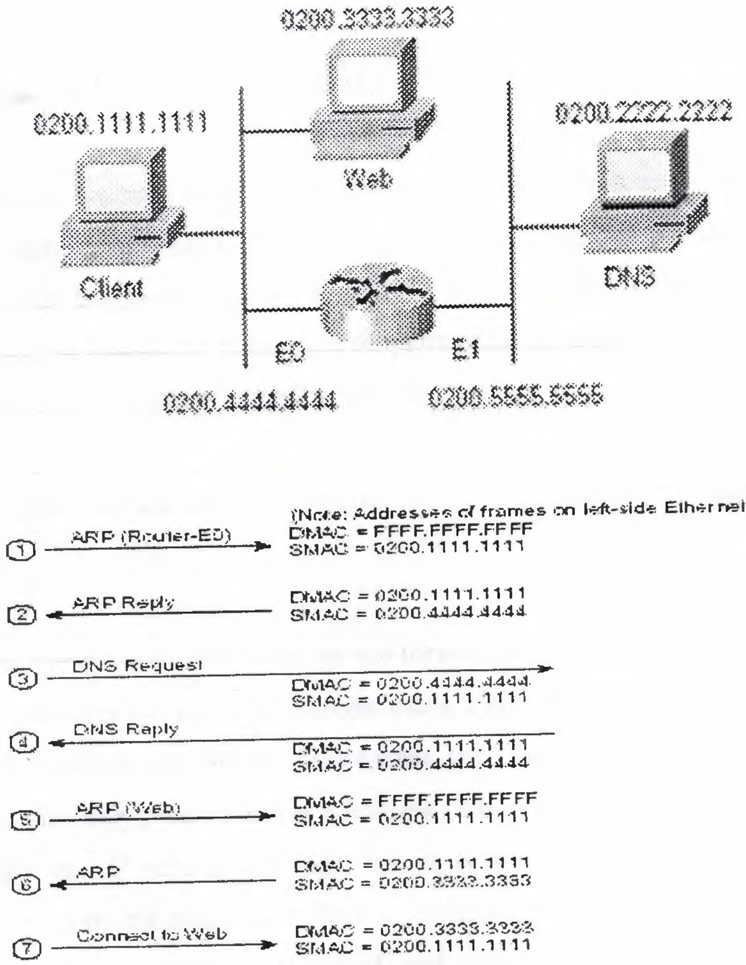


figure 2.7

The following list provides some additional text relating the steps shown in Figure

1. The PC is preconfigured with the IP address of the DNS. It first notices that the IP address is on a different subnet, so the PC will want to forward the packet to its default router first. However, the PC does not know its default router's MAC address yet, so it must ARP to find that router's MAC address.
2. The router replies to the ARP request with its MAC address, 0200.4444.4444.
3. The PC requests name resolution for the web server by sending a packet with the destination IP address of the DNS but the destination MAC address of the router.
4. The DNS returns the IP address of the web server to the PC in the DNS reply.
5. The PC does not know the web server's MAC address, so it sends an ARP broadcast to learn the MAC address. The router has no need to forward the ARP broadcast.

6. The web server replies to the ARP, stating that its MAC address is 0200.3333.3333.
7. The PC can now connect to the web server.

The ARP broadcasts are not forwarded by the router. In fact, the logic in Step 1 begins with an ARP looking for the MAC of the client's default router, namely the router's E0 MAC address. This broadcast was not forwarded by the router, a fact that causes a router to be called a *broadcast firewall*. Comparing this to a transparent bridge, this difference in broadcast treatment is the biggest advantage of routers.

The following list summarizes the features of routing relating to Ethernet LAN segmentation .

- Broadcasts and multicast frames are not forwarded by a router (by default).
- Routers perform switching of packets using Layer 3 headers and logic and are Layer 3 protocol dependent. This means that migration from a single LAN requires planning because Layer 3 address changes are necessary. For example, in Figure two IP subnets are used, one on each LAN attached to the router. If migrating from the network in Figure , where one subnet was in use, a new subnet would need to be allocated and new addresses assigned to some interfaces.
- Routers use the store-and-forward process like a transparent bridge, although it is unusual to see the term used to describe a router. Because an entire packet is received before being forwarded, additional latency is introduced, as compared to a single LAN segment.
- The router must process more portions of the received frames and possibly apply many additional logic steps before a packet is routed, which can add latency.

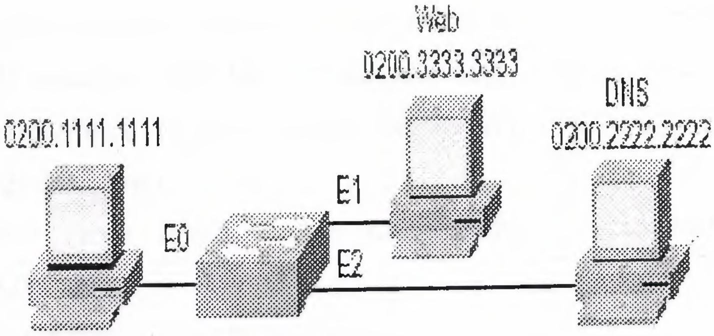
The following list summarizes the benefits of Ethernet LAN segmentation with routers

- Distance limitations are overcome because each segment can be built with the maximum distance for that type of Ethernet.
- Collisions are decreased because frames between devices on the same segment are not forwarded by the router.

- Routers reduce the impact of broadcasts/multicasts because routers do not forward broadcasts/multicasts.
- Total bandwidth is increased because each segment runs at 10 or 100 Mbps instead of a single 10 or 100 Mbps segment.
- Routers provide better manageability, particularly because the routing process has knowledge of more details of the packet flows than does a transparent bridge.
- Routers provide more functionality compared to transparent bridge devices, for example, packet fragmentation and reassembly, plus packet lifetime control.
- Multiple active paths (routes) are possible with routers (unlike transparent bridges).
- The extra workload of routing can introduce more latency than bridges. However, faster internal processing can make up the difference. Faster internal processing methods, like fast switching, autonomous switching, Silicon switching, optimum switching, and NetFlow switching can speed the internal processes and greatly decrease latency of each packet.

2.9.3 LAN Segmentation Using Switches

Example Protocol Flows—Using a Switch



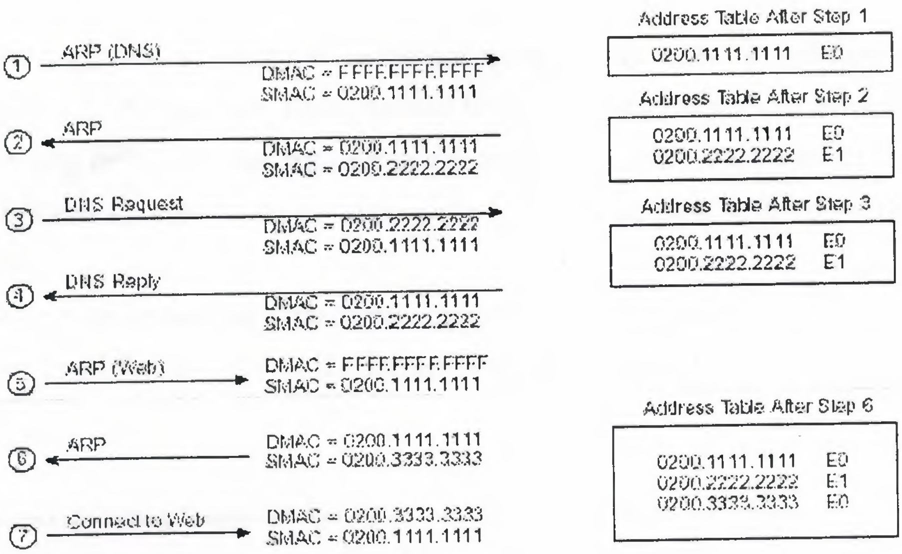


figure 2.8

The following list provides some additional text relating the steps shown in Figure :

1. The PC is preconfigured with the IP address of the DNS. The PC notices that the DNS IP address is in the same subnet as its own IP address; therefore, the PC sends an ARP broadcast hoping to learn the DNS's MAC address.
2. The DNS replies to the ARP request with its MAC address, 0200.2222.2222.
3. The PC requests name resolution for the web server by sending a packet with the destination IP address of the DNS.
4. The DNS returns the IP address of the web server to the PC in the DNS reply.
5. The PC does not know the web server's MAC address, so it sends an ARP broadcast to learn the MAC address. Because it is a MAC broadcast, the switch forwards the frame on all ports.
6. The web server replies to the ARP, stating that its MAC address is 0200.3333.3333.
7. The PC can now connect to the web server.

The two ARP broadcasts (Steps 1 and 5) are sent out all switch ports because switches and bridges do not perform the *broadcast firewall* function that a router performs. After the switching table (often called the address table) is built, the switch forwards unicasts only out of the appropriate ports. The switch network has created three separate

Ethernet segments, as compared to the transparent bridge network in Figure 4 which creates two LAN segments. Each segment is called a *collision domain* because frames sent by any device on that segment could collide with other frames on the segment. Switches can be used to create many collision domains, each with 10 or 100 Mbps capacity.

Frames can be forwarded concurrently through a switch. Consider Figure 4-10, with Fred sending a frame to Wilma and Barney sending a frame to Betty.

Concurrently Switching Frames in a Switch

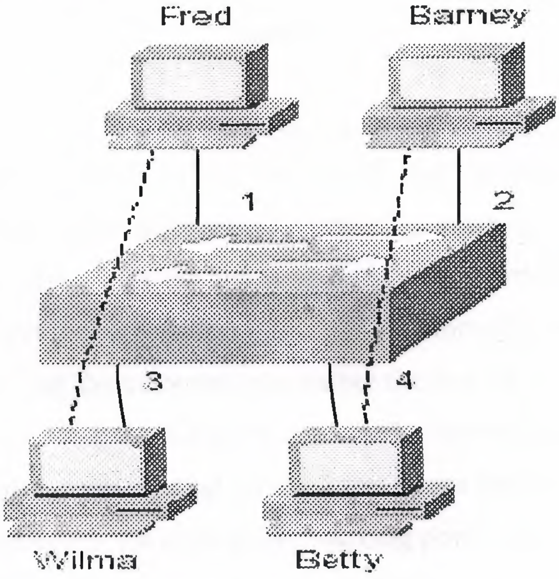


figure 2.9

Because the switch forwards the frame coming in port 1 out onto port 3, and likewise the frame coming in port 2 out port 4, and because these are all in four different collision domains, no collision occurs. A 4-port transparent bridge would behave the same way, but switches are optimized for concurrent frame forwarding, so latency is likely to be less with a switch. Full-duplex Ethernet, in conjunction with switches, can add other benefits. Figure shows a server (Pebbles) that is both sending and receiving a frame at the same time. Betty and Wilma are in different collision domains, and Pebbles cannot have a collision due to the nature of full duplex Ethernet.

Full-Duplex Ethernet and Switches

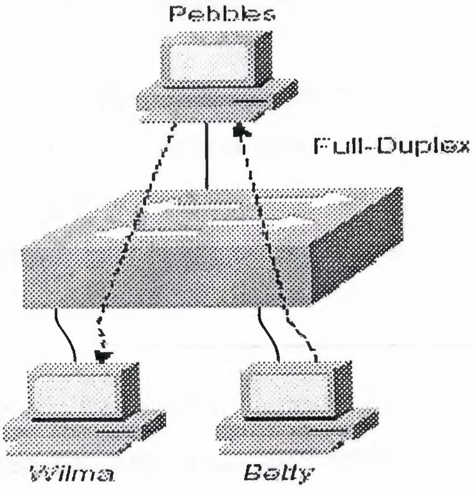


figure 2.10

Finally, the internal processing on the switch can decrease latency for frames. Transparent bridges use store-and-forward processing, meaning that the entire frame is received before the first bit of the frame is forwarded. Switches can use store-and-forward, as well as cut-through, processing logic. Cut-through means that the first bits of the frame are sent out the outbound port before the last bit of the incoming frame is received, instead of waiting for the entire frame to be received. In other words, as soon as the switching port receives enough of the frame to see the destination MAC address, the frame is transmitted out the appropriate outgoing port to the destination device. The unfortunate side effect is that, because the frame check sequence (FCS) is in the Ethernet trailer, the forwarded frame may have bit errors that the switch would have noticed with store-and-forward logic.

The following list summarizes the features of switching relating to Ethernet LAN segmentation

- Broadcasts and multicast frames are forwarded by a switch.
- Switches perform switching of frames using Layer 2 headers and logic and are Layer 3 protocol independent. This means that installation is simple because no Layer 3 address group planning or address changes are necessary. For example, because the switch retains a single broadcast domain, all devices on all segments

attached to the bridge look like a single subnet. Cisco might consider this *plug-and-play*.

- Store-and-forward and cut-through operations are typical in switches. Both types introduce latency; cut-through reduces latency compared to store-and-forward, at the risk of forwarding error frames.
- Switches must perform processing on the frame, which also can increase latency.

The following list summarizes the benefits of Ethernet LAN segmentation with switches

- Distance limitations are overcome because each segment can be built with the maximum distance for that type of Ethernet.
- Collisions are decreased because unicast frames are forwarded only out of the correct port.
- Switches do not reduce the impact of broadcasts. However, Cisco uses the Cisco Group Message Protocol (CGMP) to allow switches to help reduce the impact of multicasts.
- Total bandwidth is increased because each segment runs at 10 or 100 Mbps instead of a single 10 or 100 Mbps segment.
- User traffic is confined to individual LAN segments for frames whose source and destination is on the same LAN segment. Switches often allow administrative filters, such as Cisco access lists, to limit the flow of frames as well.
- Concurrent frame forwarding is allowed, with switches using specialized processors to optimize the process.
- Switches are typically hardware-optimized for speedy switching, which reduces latency as compared to a transparent bridge, which typically uses a single processor.

Chapter 3

IP Addressing and Subnetting

3.1 Introduction

This document will give you basic information you'll need to configure your router for routing IP, such as how addresses are broken down and how subnetting works. You'll learn how to assign each interface on the router an IP address with a unique subnet. And don't worry, we'll show you lots of examples to help tie everything together.

3.2 IP Addressing Basics: Terminology and Concepts

RFC 791, which defines IP addressing, does not claim to predict the future or anticipate private networks with thousands and tens-of-thousands of hosts, and a global Internet with hundreds of millions of hosts. With some literary license, one might imagine the original IP address structure was designed with the following criteria in mind:

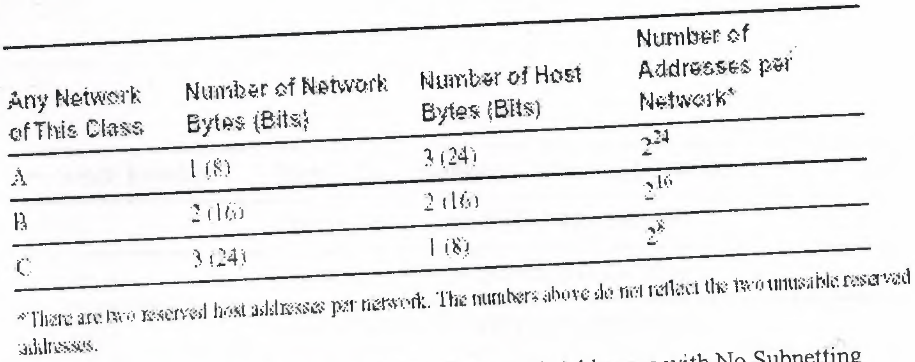
- Each host should have a unique IP address.
- The IP address structure should be logical, not physical, to allow for future growth into new technologies.
- The address is assigned to the interface of the computer, not the computer itself.
- Addresses are grouped (both numerically) and based on where the interfaces are physically attached.
- The numeric grouping is the set of all addresses that have the same numeric value in the first part of the address, called the *network part* of the address.
- The interfaces in the same group must be attached to the same medium and must not be separated by an IP router.
- One address in each grouping is reserved as the number representing the entire group; this is called the *network number* or *network address*.

- By assigning each organization a unique network number, globally unique addresses can be accomplished. This allows for creation of a global Internet without confusing routers with duplicate groups or duplicate individual addresses.
- Some networks need to be large, others need to be small, so create networks of different sizes.
- Use a 32-bit address so that we will never run out.

3.3 IP Networks

Class A, B, and C networks provide three network sizes. By definition, all addresses in the same network have the same numeric value network portion of the addresses. The rest of the address is called the *host* portion of the address. Individual addresses in the same network all have a different value in the host parts of the addresses.

For example, Class A networks have a 1–byte–long network part. That leaves 24 bits for the "rest" of the address, or the host part. That means that 224 addresses are numerically possible in a Class A network. Similarly, Class B networks have a 2–byte–long network part, leaving 16 bits for the host portion of the address. So, 216 possible addresses exist in a single Class B network. Finally, Class C networks have a 3–byte–long network part, leaving only 8 bits for the host part, which implies only 28 addresses in a Class C network. Table summarizes the characteristics of Class A, B, and C networks.



Any Network of This Class	Number of Network Bytes (Bits)	Number of Host Bytes (Bits)	Number of Addresses per Network*
A	1 (8)	3 (24)	2^{24}
B	2 (16)	2 (16)	2^{16}
C	3 (24)	1 (8)	2^{8}

*There are two reserved host addresses per network. The numbers above do not reflect the two unusable reserved addresses.

Table 3.1 Sizes of Network and Host Parts of IP Addresses with No Subnetting

For example, Figure is a small network with addresses filled in. Network 8.0.0.0 is a Class A network; Network 130.4.0.0 is a Class B network; 199.1.1.0 is a Class C network.

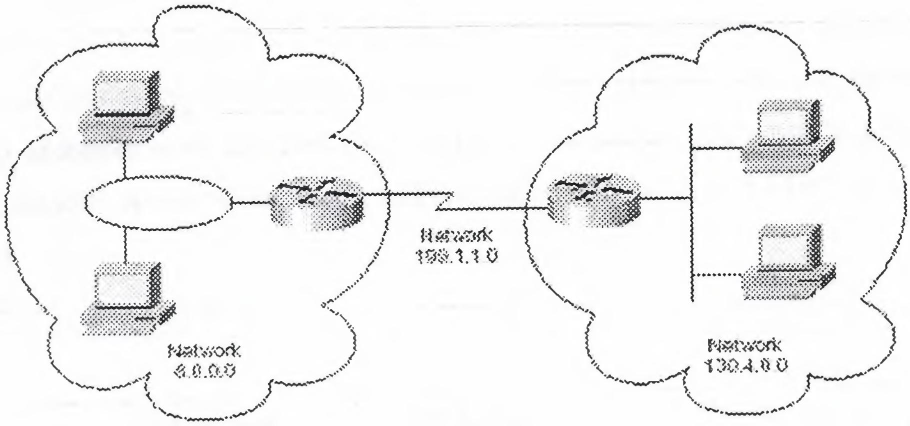
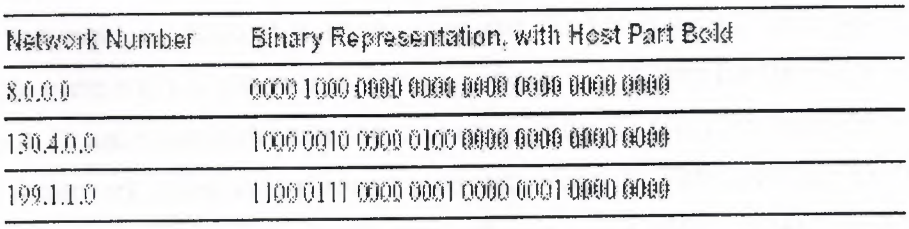


Figure 3.1 Sample Network Using Class A, B, and C Network Numbers

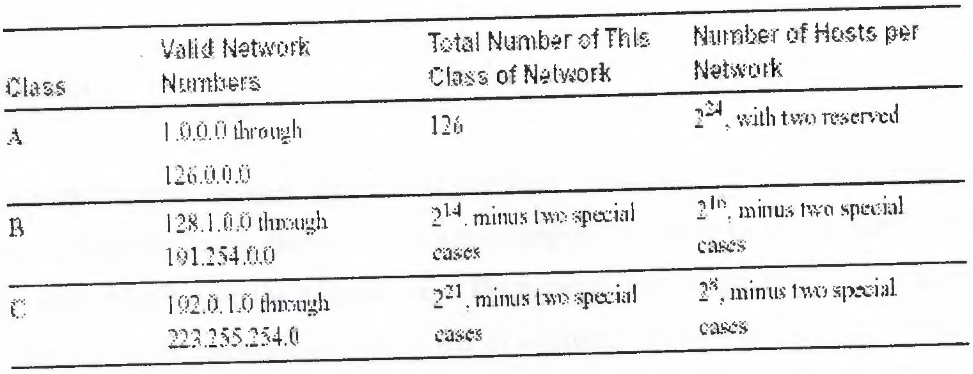
Network numbers look like addresses (canonical decimal format), but they are not assignable to any interface as an IP address. Conceptually, network numbers represent the group of all IP addresses in the network. Numerically, the network number is built with the actual value of the network number in the network part, but all binary 0s in the host part of the address. Given the three examples from Figure 5-11, Table 5-6 provides a closer look at the numerical version of the three network numbers: 8.0.0.0, 199.1.1.0, and 130.4.0.0.



Network Number	Binary Representation, with Host Part Bold
8.0.0.0	0000 1000 **0000 0000 0000 0000 0000 0000**
130.4.0.0	1000 0010 0000 0100 **0000 0000 0000 0000**
199.1.1.0	1100 0111 0000 0001 0000 0001 **0000 0000**

Table 3.2 Example Network Numbers, Decimal and Binary

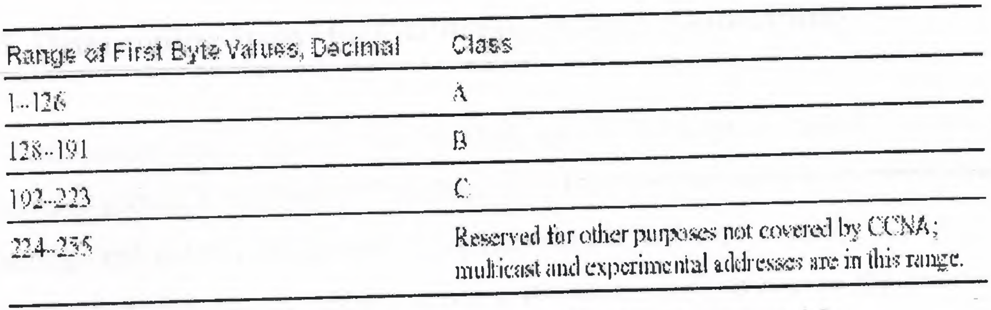
There are many different Class A, B, and C networks. One goal of the writers of RFC 791 was to ensure that an individual IP address would be, by definition, in only one IP network. (In other words, the IP networks defined did not overlap.) So a strategy was used to take half of the address "space" and assign those numbers to the large (Class A) networks. Then, half of the remaining address space (25 percent of the total) was used to create medium sized (Class B) networks. Finally, 50 percent of the remaining space (12.5 percent of the total) was used to define small (Class C) networks. For other address types, for example, Class D multicast addresses, half of the then-remaining addresses were allocated for use. Table summarizes the possible network numbers, the total number of each type, and the number of hosts in each Class A, B, and C network.



Class	Valid Network Numbers	Total Number of This Class of Network	Number of Hosts per Network
A	1.0.0.0 through 126.0.0.0	126	2^{24}, with two reserved
B	128.1.0.0 through 191.254.0.0	2^{14}, minus two special cases	2^{16}, minus two special cases
C	192.0.1.0 through 223.255.254.0	2^{21}, minus two special cases	2^{8}, minus two special cases

Table 3.3 List of All Possible Valid Network Numbers*

The third column in Table 5-7 is sometimes confusing, but it is accurate. The number of networks of a particular class is equal to 2 to the power of the number of bits in the network part of the address. Normally, we think of the network part of a Class A address as 8 bits long, Class B as 16 bits long, and Class C as 24 bits long, and in most cases, that perspective is reasonable. However, when considering the true total number of Class A, B, and C networks, it is useful to consider the nit-picky but accurate fact that a Class A network's first byte always begins with binary 0. Therefore only seven bits are actually considered to comprise the network part of the address. Likewise, Class B networks always begin with binary 10; therefore only 14 bits of the 16 in the first two bytes are considered part of the network number. Similarly, Class C networks always begin with binary 110, and so only 21 bits of the 24 in the first three bytes are considered part of the network number. Table summarizes the valid values in the first byte of IP addresses and the class of network that is implied by each:

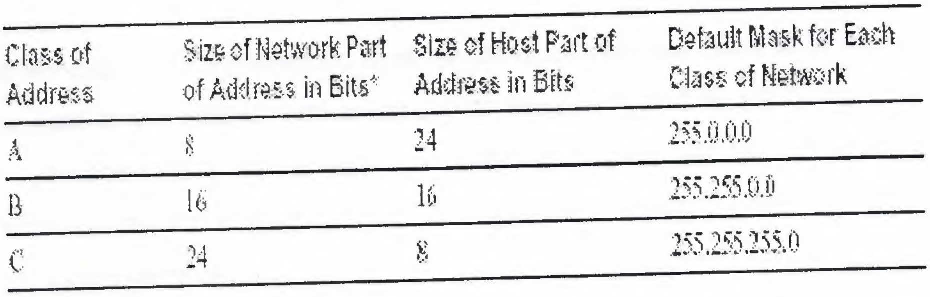


Range of First Byte Values, Decimal	Class
1–126	A
128–191	B
192–223	C
224–255	Reserved for other purposes not covered by CCNA; multicast and experimental addresses are in this range.

Table 3.4 Range of First Bytes of Addresses, Class A, B, and C

3.4 Masks

The address mask is used for several purposes. One key purpose is to define the number of host bits in an address; when subnetting is not being used, this then implies that the rest of the bits in the address are in the network part of the address. We already know the size of the network and host parts of addresses in each of the three classes of networks. Table summarizes those details and adds a reference to the default network masks for each type of network.



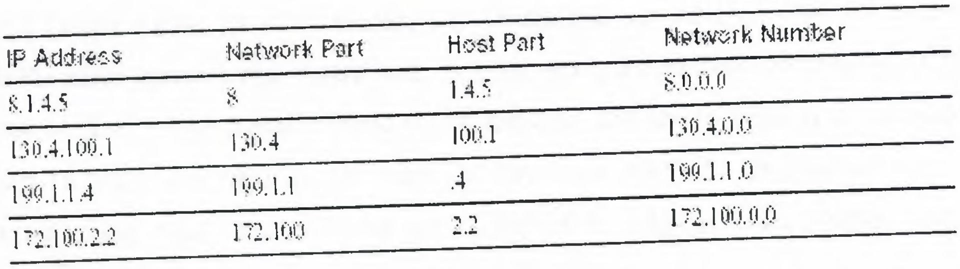
Class of Address	Size of Network Part of Address in Bits*	Size of Host Part of Address in Bits	Default Mask for Each Class of Network
A	8	24	255.0.0.0
B	16	16	255.255.0.0
C	24	8	255.255.255.0

Table 3.5 Class A, B, and C Networks—Network and Host Parts and Default Masks

The mask implies the number of host bits in an address. If a bit position in the binary version of the mask has a value of 0, that corresponding bit position in the address is in the host portion of the address. For example, a mask of 255.255.0.0, which has 16 bits of value 1, followed by 16 bits of value 0, implies that there are 16 host bits in the address, which is true of Class B addresses.

3.5 Determining Individual Address/Network Associations

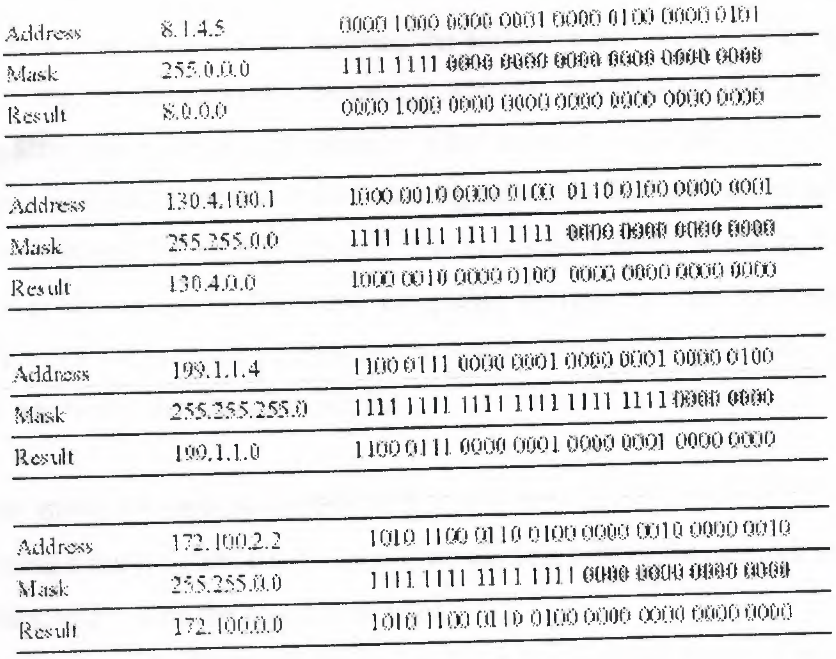
Both people and computers need to think about the question, "which network is a particular address a member of?" Humans care because it is useful in troubleshooting, planning, and address assignment; computers need to know because the answer to this question is a vital part of routing. When a computer needs to answer the question, it performs a Boolean math operation called AND between the address in question and the mask. The result of the AND is that the host bits are *masked* out, that is, changed to binary 0s. Look at Table for example.



IP Address	Network Part	Host Part	Network Number
8.1.4.5	8	1.4.5	8.0.0.0
130.4.100.1	130.4	100.1	130.4.0.0
199.1.1.4	199.1.1	4	199.1.1.0
172.100.2.2	172.100	2.2	172.100.0.0

Table 3.6 Example Dissections of IP Addresses, No Subnetting

The Boolean AND is performed between the IP address and mask, in binary. Each bit is examined in the address and compared to the corresponding bit in the mask. The AND operation results in a binary 1 if both the address and mask bits are also 0; otherwise, the result is 0. The Boolean AND for the addresses in Table 5-10 is shown in the following examples.



Address	8.1.4.5	0000 1000 0000 0001 0000 0100 0000 0101
Mask	255.0.0.0	1111 1111 0000 0000 0000 0000 0000 0000
Result	8.0.0.0	0000 1000 0000 0000 0000 0000 0000 0000
Address	130.4.100.1	1000 0010 0000 0100 0110 0100 0000 0001
Mask	255.255.0.0	1111 1111 1111 1111 0000 0000 0000 0000
Result	130.4.0.0	1000 0010 0000 0100 0000 0000 0000 0000
Address	199.1.1.4	1100 0111 0000 0001 0000 0001 0000 0100
Mask	255.255.255.0	1111 1111 1111 1111 1111 1111 0000 0000
Result	199.1.1.0	1100 0111 0000 0001 0000 0001 0000 0000
Address	172.100.2.2	1010 1100 0110 0100 0000 0010 0000 0010
Mask	255.255.0.0	1111 1111 1111 1111 0000 0000 0000 0000
Result	172.100.0.0	1010 1100 0110 0100 0000 0000 0000 0000

Table 3.7

Consider the second example using address 130.4.100.1, mask 255.255.0.0. The binary mask shows 16 binary 1s; any other binary value ANDed with binary 1 yields the original binary value. In other words, any 16-bit number ANDed with 16 binary 1s yields the same number you started with. So, the result shows **1000 0010 0000 0100** for the first 16 bits, which literally could be copied from the binary version of the address. The last 16 bits of the mask are all binary 0s; any value ANDed with a binary 0 yields a 0. So, no matter what value is in the last 16 bits of the address, once ANDed with the mask, the result will be all binary 0s, as shown in the example result. The result is called the *network number* when no subnetting is used; the result is the *subnet number* when subnetting is used.

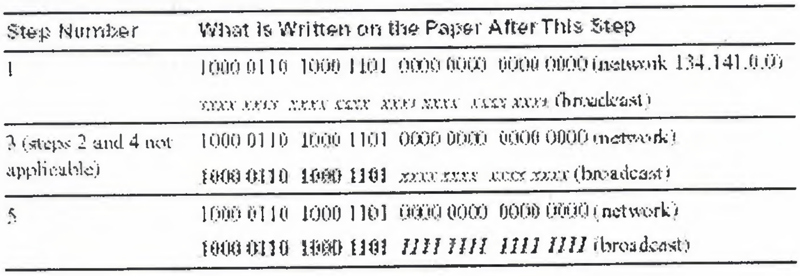
3.6 Broadcast Addresses

As mentioned earlier, there are two reserved numbers in each network. One number is the

network number, which is used to represent the entire network. The other reserved number is called the *broadcast address*. This number is used to represent all IP addresses in the network. The broadcast address is used when a packet needs to be sent to all hosts in a network. All hosts receiving the packet should notice that the packet is destined for their own network's broadcast address, and process the packet. The broadcast address for a network is important when planning an IP addressing structure for a network. The reason for that is the following definition: The network number is the lowest value numerically in that network. The broadcast address is the *largest* value numerically in that network. The valid, assignable addresses in that network are the numbers between the network number and broadcast address. To derive the broadcast address for a network, use the following list:

1. Write down the network number, in binary.
2. If using a mask of 255.0.0.0, write down the first byte of the network number in binary, underneath the network number.
3. If using a mask of 255.255.0.0, write down the first two bytes of the network number in binary, underneath the network number.
4. If using a mask of 255.255.255.0, write down the first three bytes of the network number in binary, underneath the network number.
5. Complete the broadcast address by writing down all binary 1s in the remaining bits in the number created in Steps 2, 3, or 4.

Any number between the first number (network number) and second number (broadcast address) is an assignable IP address in this network. Each binary number will need to be converted to a decimal eight bits at a time, to show the addresses in decimal form.



Step Number	What Is Written on the Paper After This Step
1	1000 0110 1000 1101 0000 0000 0000 0000 (network 134.141.0.0) xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx (broadcast)
3 (steps 2 and 4 not applicable)	1000 0110 1000 1101 0000 0000 0000 0000 (network) **1000 0110 1000 1101** xxxx xxxx xxxx xxxx (broadcast)
5	1000 0110 1000 1101 0000 0000 0000 0000 (network) **1000 0110 1000 1101** ***1111 1111 1111 1111*** (broadcast)

Table 3.8 Process for Deriving the Network Broadcast Address, in Binary.

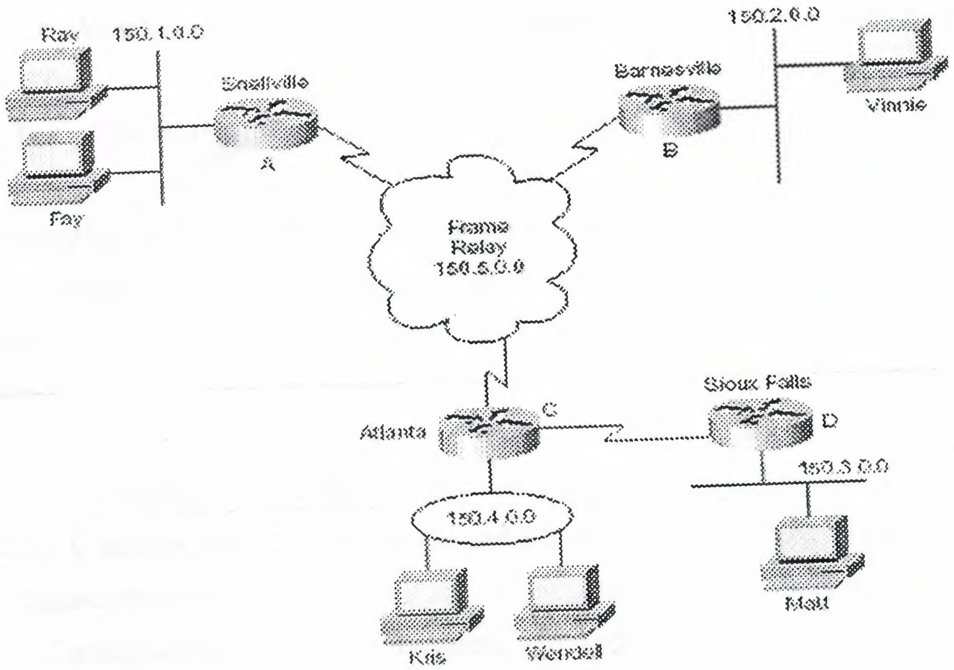
3.7 IP Subnetting

Almost every organization with a network uses IP, and almost every one of these organizations uses subnetting. Subnetting is simply the process of treating subdivisions of a single Class A, B, or C network as if it were a network itself. By doing so, a single Class A, B, or C network can be subdivided into many nonoverlapping subnets. There are two main reasons why organizations choose to use subnets, rather than just using lots of Class A, B, and C networks:

- The grouping concept in IP required that hosts in the same group not be separated by a router.
- Conversely, IP routing requires that hosts separated by a router must be in a different group (subnet). Without subnetting, that means each group would need to be a different Class A, B, or C network, which would be impractical if the organization is directly connected to the Internet, considering the lack of currently unassigned networks the NIC has available.

Consider all network interfaces in Figure 5-12 and note which ones are not separated by a router.

Figure 3.2 Backdrop for Discussing Numbers of Different Networks/Subnets



In Figure , six groupings exist. Four groups are more obvious, those being the set of all interfaces attached to each of the four LANs. In other words, the LANs attached to Routers A, B, C, and D are each a separate subnet. Additionally, the two serial interfaces composing the point-to-point serial link between Routers C and D are both in the same group because they are not separated by a router. Finally, the three router interfaces composing the Frame relay network between Routers A, B, and C would not be separated by an IP router and would compose the sixth group. if building this network today, the NIC would not assign six separate network numbers. Instead, you might get a couple of Class C networks assigned by the NIC, with the expectation that you would use subnetting.

3.7.1 Definition of Subnetting

Subnets are subdivisions of a Class A, B, or C network. These subdivisions take on the properties of a network in many ways:

- Members of one subnet have the same numeric value in the subnet parts of the addresses.
- Members of one subnet cannot be separated by a router.

- Members of a second subnet must be separated from the first subnet by a router.

Two of the more popular views of subnetting follow.

Pretending the Network Part of the Address is Longer Than When Not Subnetting

One method that is typically easier to understand for those less inclined to enjoy binary math is *to pretend that the network field is longer than the Class A, B, and C rules imply.*

For example, network 8.0.0.0 might be assigned. The organization treats it like a Class C address, with 24 network bits, and 8 host bits. The real NIC could care less; it is assigned you network 8.0.0.0, and it is happy! But inside your organization, someone must assign the different subnet numbers, like the NIC would have done. For example, imagine your organization has Class B network 150.150.0.0, and you want to treat it as a Class C network for the purposes of subnetting.Fig. Shows one way to implement that idea. Continuing with the "pretending" view of subnetting, the subnet numbers shown behave like Class C networks. These subnets are actually subnets of a Class B network; do not fall into the trap of thinking they have magically become Class C networks! All hosts beginning with 150.150.1 must be on the Router A Ethernet; all Frame Relay interface addresses must begin 150.150.5, and so on.

The two examples shown here use *basic* subnetting.

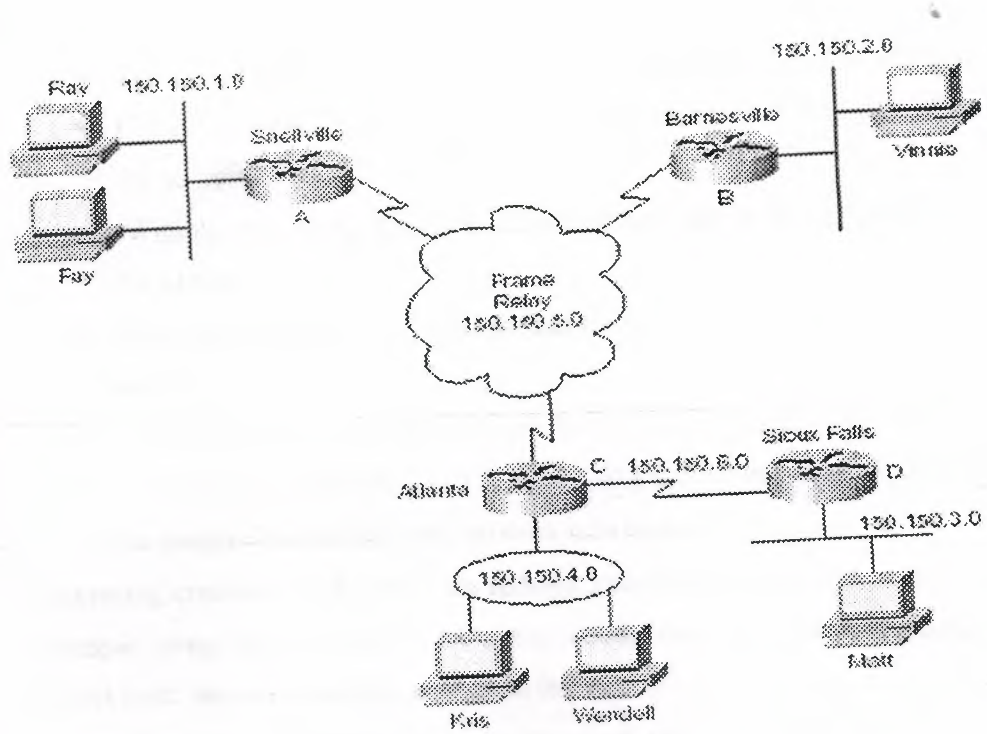


Figure 3.3 Using Subnets

3.7.2 Binary View of Subnetting

The benefit of a binary definition of subnetting is that it is exact. For a full understanding of subnetting, particularly more advanced subnetting topics, as well as other IP addressing and routing topics beyond the scope of this book, an exact definition is required. If your job will include planning subnet number assignment, or troubleshooting, this binary understanding will be useful. A review of some basic concepts used when not using subnetting can be used as a comparison to subnetting. When not subnetting, the default mask defined the number of host bits. The mask accomplished this by simply using binary 0 for each bit position in the mask that corresponded to the host part of the address in question. For example, the mask 255.255.0.0 (Class B) has a value of all binary 0s in the last 16 bits. This implies 16 network bits at the beginning of the address.

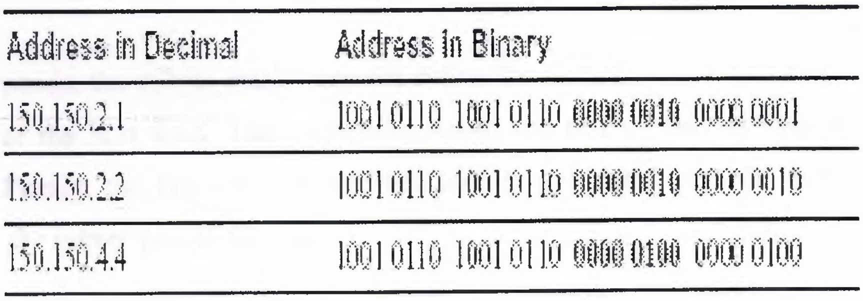
The following list summarizes basic concepts when not using subnetting:

- The mask defines the number of host bits in the host part of an address.
- Class A, B, and C rules define the number of network bits in the network part of the address.
- Without subnetting, these two field (network and host) compose the entire 32-bit address.
- Each host address in the network has the same value in the network part of the address.
- Each host address in the network has a unique value in the host part of the address. (For example, 130.1.1.1 and 130.1.1.2 are in the same network, but can be assigned to two different network interfaces.)

Subnetting creates a third part of the address, called the *subnet field* or *subnet part.* For example, using network 150.150.0.0 again, assume that you want a third field called the subnet field. several assertions are true in this case:

- The Class A, B, and C network field sizes cannot be changed; they remain as 8, 16, and 24 bits, respectively.
- The IP address must still be 32 bits in length.
- Therefore, to create a third field called the subnet part of the address, *some of the bits previously in the host part of the address are used.*

The subnet part of an address identifies the different subdivisions of this network. An address with a different value in the subnet field, as compared with a second address, is considered to be in a different subnet. For example, examine the following three IP addresses that would be part of Table



Address in Decimal	Address in Binary
150.150.2.1	1001 0110 1001 0110 0000 0010 0000 0001
150.150.2.2	1001 0110 1001 0110 0000 0010 0000 0010
150.150.4.4	1001 0110 1001 0110 0000 0100 0000 0100

Table 3.9 Subnet Part of Sample Addresses

The example defines that the subnet field consists of bits 17–24 (the entire third byte).

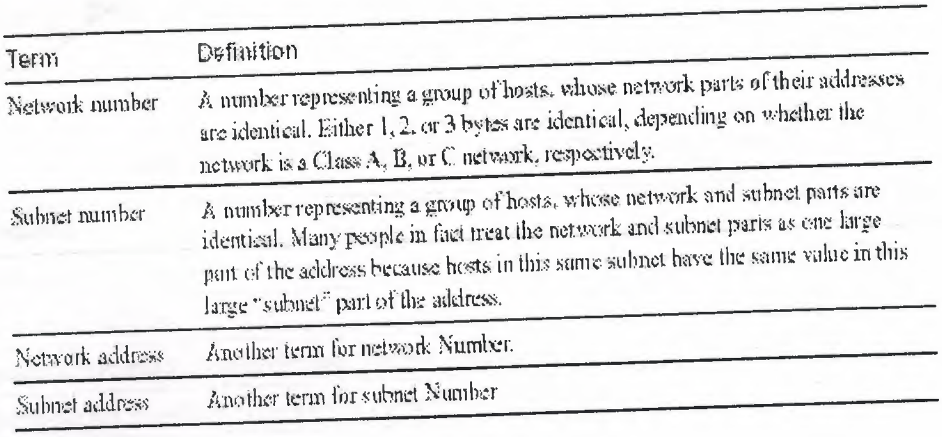
150.150.2.1 and 150.150.2.2 are in the same subnet because they are in the same Class B network, and *their subnet fields have the same value* (0000 0010). 150.150.4.4 is in a different subnet of the same Class B network because the subnet field has a different value than the first two addresses (0000 0100). 150.150.4.4 must be physically located with at least one IP router between itself and 150.150.2.1 and 150.150.2.2. The three different parts of an address need to be defined. Class A, B, or C rules are applied to define the size of the network part of the addresses. The subnet mask will be used for several purposes, including defining the number of host bits in the host part of an address. The remaining part of the address is the subnet part of the address. The following list summarizes these rules, along with a few other useful corollaries.

- The mask defines the number of host bits in the host part of an address, located at the end of the address.
- Class A, B, and C rules define the number of network bits in the network part of the address, located at the beginning of the address.
- With subnetting, the number of network and host fields total less than 32 bits. The remaining bit positions compose the subnet field and are located between the other two fields.
- Each host address in the network has the same value in the network part of the address.
- Each host address in the same subnet has a unique value in the host part of the address, but the same value in the network and subnet parts of the addresses.

In other words, the subnet mask does not define the size of the subnet field; it defines the size of the host field. The class rules define the size of the network part of the address. Finally, the bits left over between the network and host parts of the address compose the subnet part of the address.

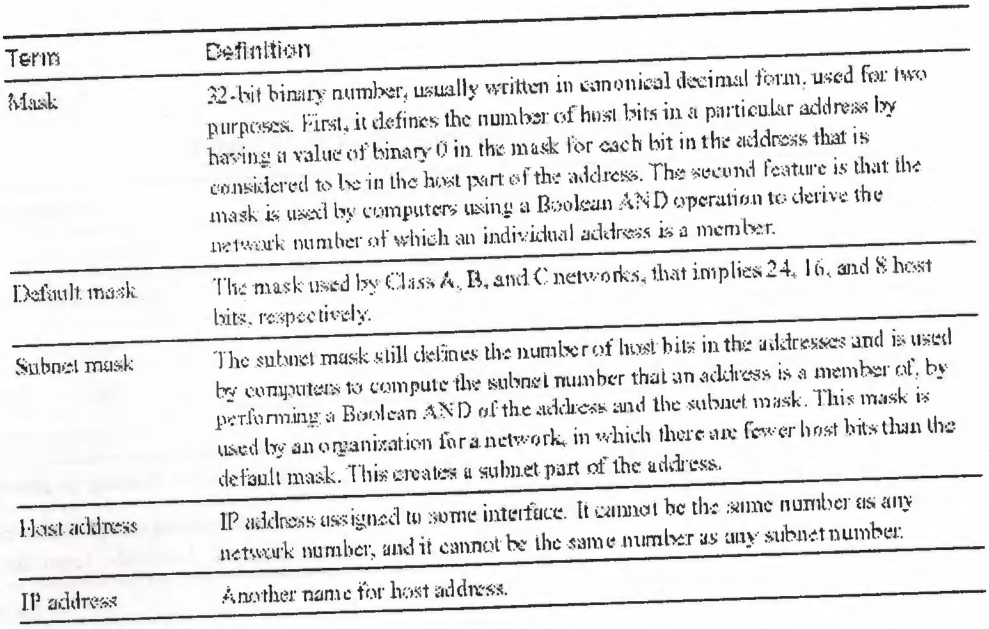
3.7.3 Subnetting Terminology

The terminology used when subnetting is very similar to the terminology used when not subnetting. To ensure a full understanding of subnetting, review the terms defined in Table



Term	Definition
Network number	A number representing a group of hosts, whose network parts of their addresses are identical. Either 1, 2, or 3 bytes are identical, depending on whether the network is a Class A, B, or C network, respectively.
Subnet number	A number representing a group of hosts, whose network and subnet parts are identical. Many people in fact treat the network and subnet parts as one large part of the address because hosts in this same subnet have the same value in this large "subnet" part of the address.
Network address	Another term for network Number.
Subnet address	Another term for subnet Number

Table 3.10 Subnetting Terminology



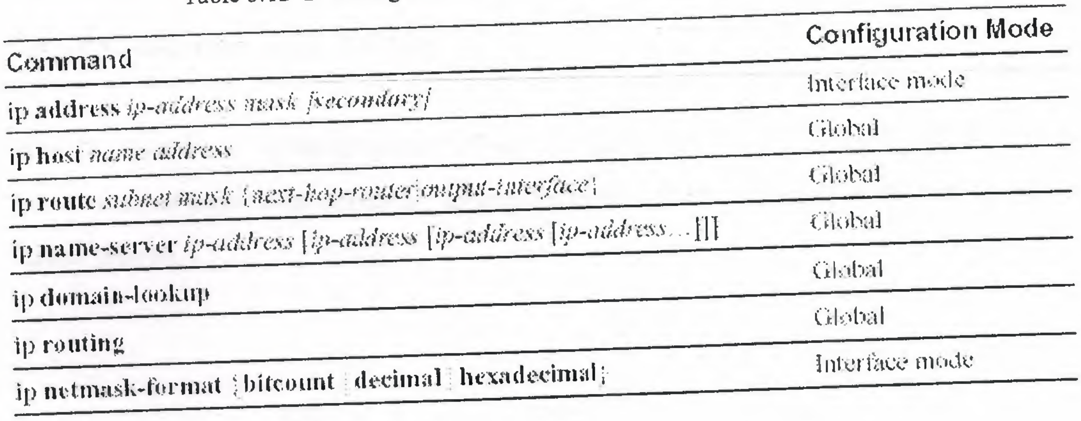
Term	Definition
Mask	32-bit binary number, usually written in canonical decimal form, used for two purposes. First, it defines the number of host bits in a particular address by having a value of binary 0 in the mask for each bit in the address that is considered to be in the host part of the address. The second feature is that the mask is used by computers using a Boolean AND operation to derive the network number of which an individual address is a member.
Default mask	The mask used by Class A, B, and C networks, that implies 24, 16, and 8 host bits, respectively.
Subnet mask	The subnet mask still defines the number of host bits in the addresses and is used by computers to compute the subnet number that an address is a member of, by performing a Boolean AND of the address and the subnet mask. This mask is used by an organization for a network, in which there are fewer host bits than the default mask. This creates a subnet part of the address.
Host address	IP address assigned to some interface. It cannot be the same number as any network number, and it cannot be the same number as any subnet number.
IP address	Another name for host address.

Table 3.11

3.8 Configuration of IP

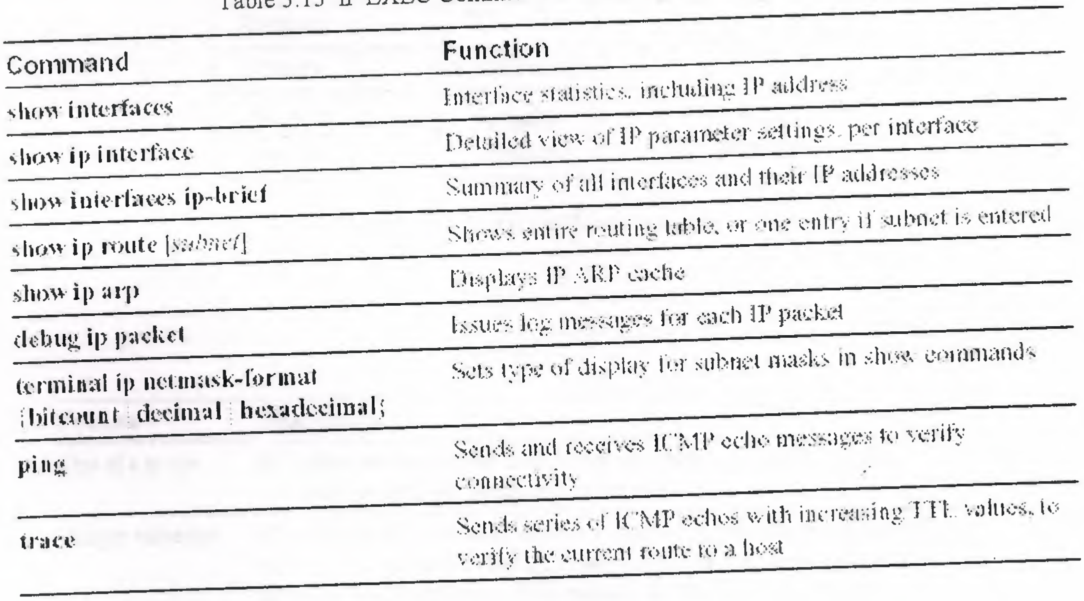
Configuration of TCP/IP in a Cisco router is straightforward. Table 5-18 and Table 5-19 summarize the commands used in Training Paths 1 and 2 for IP configuration and verification. Two samples, with both configuration and **EXEC** command output, follow..

Table 3.12 IP Configuration Commands in Training Paths 1 and 2



Command	Configuration Mode
ip address *ip-address mask [secondary]*	Interface mode
ip host *name address*	Global
ip route *subnet mask {next-hop-router|output-interface}*	Global
ip name-server *ip-address [ip-address [ip-address...]]*	Global
ip domain-lookup	Global
ip routing	Global
ip netmask-format {bitcount | decimal | hexadecimal}	Interface mode

Table 3.13 IP EXEC Commands in Training Paths 1 and 2

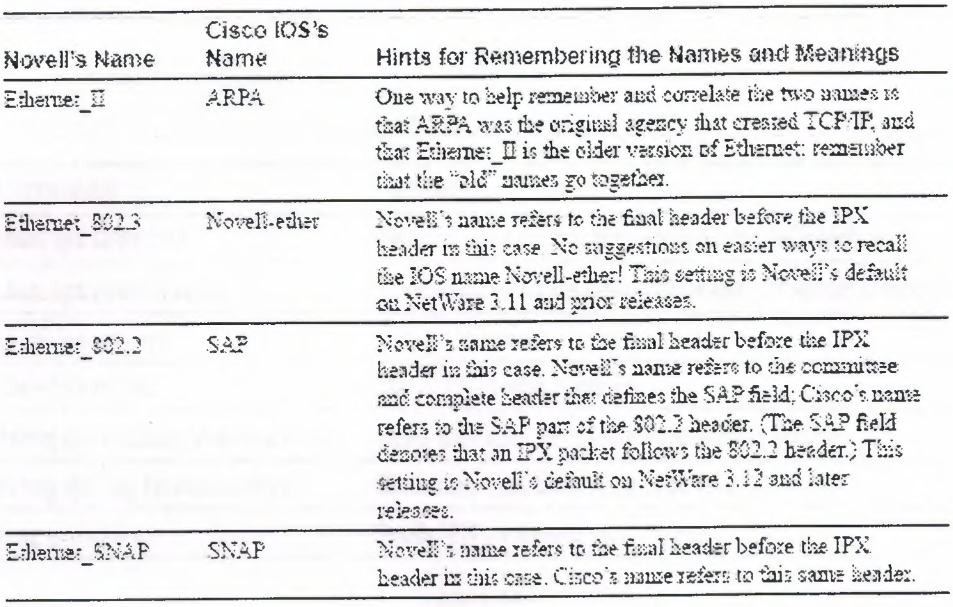


Command	Function
show interfaces	Interface statistics, including IP address
show ip interface	Detailed view of IP parameter settings, per interface
show interfaces ip-brief	Summary of all interfaces and their IP addresses
show ip route *[subnet]*	Shows entire routing table, or one entry if subnet is entered
show ip arp	Displays IP ARP cache
debug ip packet	Issues log messages for each IP packet
terminal ip netmask-format {bitcount | decimal | hexadecimal}	Sets type of display for subnet masks in show commands
ping	Sends and receives ICMP echo messages to verify connectivity
trace	Sends series of ICMP echos with increasing TTL values, to verify the current route to a host

Collectively, Figure 5-15, along with Example 5-2, Example 5-3, and Example 5-4, show three sites, each with two serial links and one Ethernet. The following site guidelines were used when choosing configuration details:

Table 3.13 IPX Addressing Details

3.9.1 IPX Ethernet Encapsulations

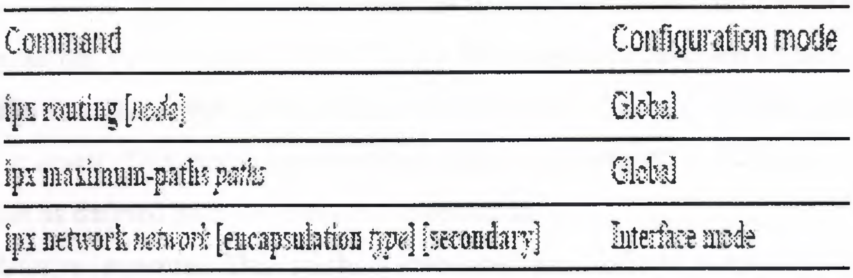


Novell's Name	Cisco IOS's Name	Hints for Remembering the Names and Meanings
Ethernet_II	ARPA	One way to help remember and correlate the two names is that ARPA was the original agency that created TCP/IP, and that Ethernet_II is the older version of Ethernet: remember that the "old" names go together.
Ethernet_802.3	Novell-ether	Novell's name refers to the final header before the IPX header in this case. No suggestions on easier ways to recall the IOS name Novell-ether! This setting is Novell's default on NetWare 3.11 and prior releases.
Ethernet_802.2	SAP	Novell's name refers to the final header before the IPX header in this case. Novell's name refers to the committee and complete header that defines the SAP field; Cisco's name refers to the SAP part of the 802.2 header. (The SAP field denotes that an IPX packet follows the 802.2 header.) This setting is Novell's default on NetWare 3.12 and later releases.
Ethernet_SNAP	SNAP	Novell's name refers to the final header before the IPX header in this case. Cisco's name refers to this same header.

Table 3.14

3.9.2 Configuration of IPX

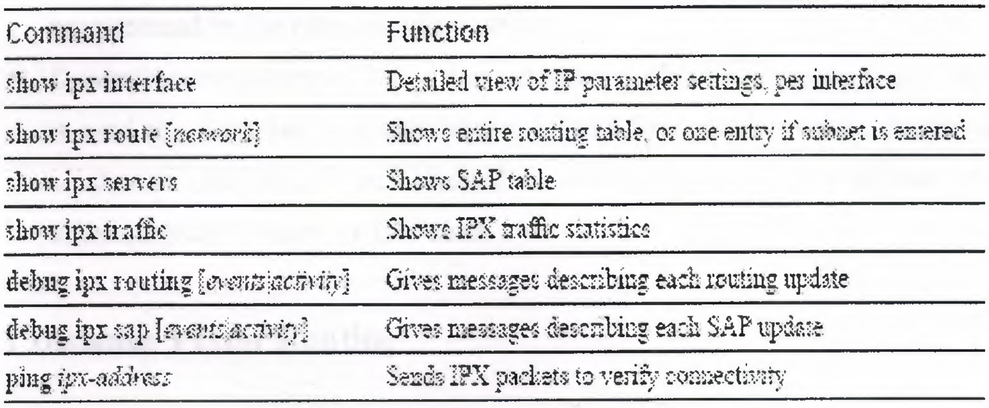
IPX and IPX RIP Configuration Commands



Command	Configuration mode
ipx routing [*node*]	Global
ipx maximum-paths *paths*	Global
ipx network *network* [encapsulation *type*] [secondary]	Interface mode

Table 3.15

IPX EXEC Command



Command	Function
show ipx interface	Detailed view of IP parameter settings, per interface
show ipx route [*network*]	Shows entire routing table, or one entry if subnet is entered
show ipx servers	Shows SAP table
show ipx traffic	Shows IPX traffic statistics
debug ipx routing [*events*|*activity*]	Gives messages describing each routing update
debug ipx sap [*events*|*activity*]	Gives messages describing each SAP update
ping *ipx-address*	Sends IPX packets to verify connectivity

table 3.16

3.10 DYNAMIC ROUTING APPLIED—ROUTING ALGORITHMS

Routing refers to the process of forwarding messages through internetworks of LANs. In some cases, routing information is programmed into the routing devices. However, preprogrammed, or static, routers cannot adjust to changing network conditions. Most routing devices, therefore, are dynamic, which means that they have the capability of discovering routes through the internetwork and then storing the route information in route tables. Route tables do not store only path information. They also store estimates of the time, cost or calculated distance taken to send a message through a given route. This time estimate is known as the cost of a particular path. Some of the methods of estimating routing costs are as follows:

- *Hop count.* This method describes the number of routers that a message might cross before it reaches its destination. If all hops are assumed to take the same amount of time, the optimum path is the path with the smallest hop count.
- *Tic count.* This method provides an actual time estimate, where a tic is a time unit as defined by the routing implementation.
- *Relative expense.* This method calculates any defined measure of the cost (including the monetary cost) to use a given link.

After costs are established, routers can select routes, either statically or dynamically, as follows:

- *Static route selection.* This selection method uses routes that have been programmed by the network administrator.
- *Dynamic route selection.* Under this selection method, routing cost information is used to select the most cost effective route for a given packet. As network conditions change and are reflected in routing tables, the router can select different paths to maintain low costs.

3.11 Distance Vector Routing

Distance vector routers advertise their presence to other routers on the network. Periodically, each router on the network broadcasts the information in its routing table. Other routers can use this information to update their own router tables. Figure illustrates how the process works. In the figure, Server S3 learns that Server S2 can reach Server S1 in one hop. Because S3 knows that S2 is one hop away, S3 knows that its cost to reach S1 through S2 is two hops. Distance vector routing is an effective algorithm, but it can be fairly inefficient. Because changes must ripple through the network from

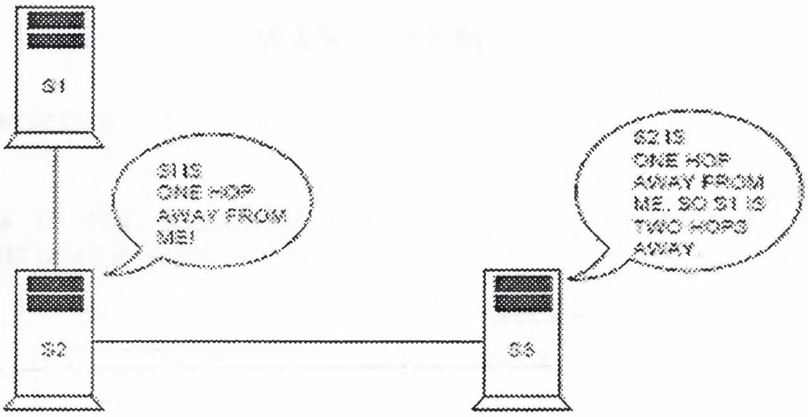

S1
S1 IS ONE HOP AWAY FROM ME!
S2 IS ONE HOP AWAY FROM ME, SO S1 IS TWO HOPS AWAY.
S2
S3

Figure 3.5 Distance vector routing

Router to router, it might take a while for a change to become known to all routers on the network. In addition, the frequent broadcasts of routing information produce high levels of network traffic that can hurt performance on larger networks.

3.12 Link-State Routing

Link-state routing reduces the network traffic required to update routing tables. Routers that are newly attached to the network can request routing information from a nearby router. After routers have exchanged routing information about the network, routers broadcast messages only when something changes. These messages contain information about the state of each link the router maintains with other routers on the network. Because routers keep each other updated, complete network routing updates are not needed often.

WAN Technologies

4.1 Introduction

The focus of this chapter is WAN technology. It describes hardware, components used in WAN technology.

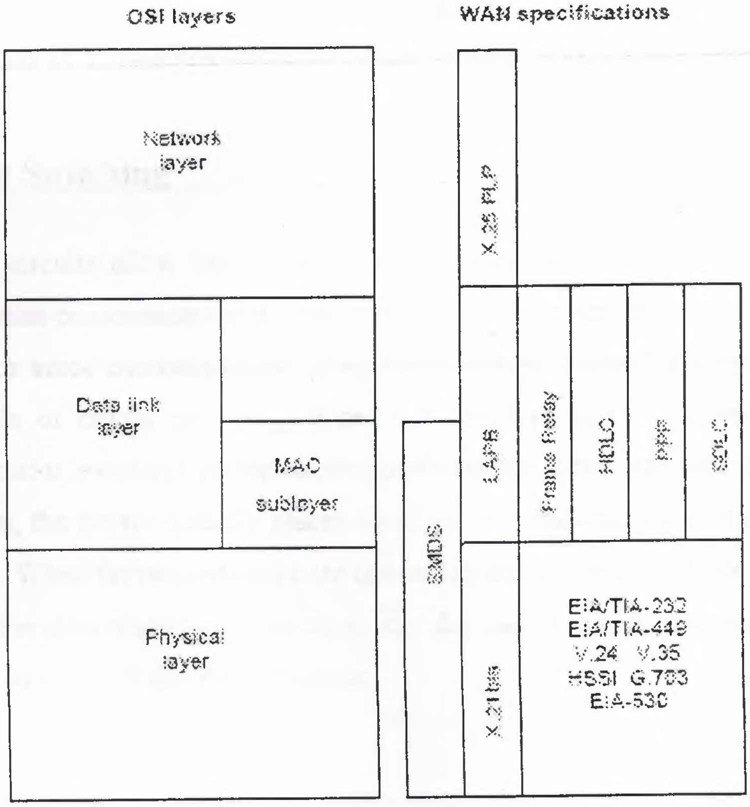


Figure 4.1 WAN Technologies Operate at the Lowest Levels of the OSI Model

4.2 Point-to-Point Links

A point-to-point link provides a single, pre-established WAN communications path from the customer premises through a carrier network, such as a telephone company, to a remote network. Point-to-point lines are usually leased from a carrier and thus are often called leased lines. For a point-to-point line, the carrier allocates pairs of wire and facility hardware to your line only. These circuits are generally priced based on bandwidth required and distance between the two connected points. Point-to-point links are generally more expensive than shared services such as Frame Relay. Figure 3-2 illustrates a typical point-to-point link through a WAN.

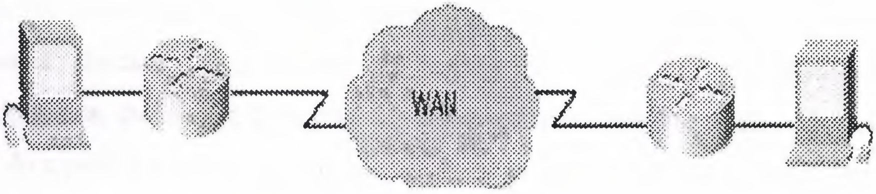


Figure 4.2 A Typical Point-to-Point Link Operates Through a WAN to a Remote Network

4.3 Circuit Switching

Switched circuits allow data connections that can be initiated when needed and terminated when communication is complete. This works much like a normal telephone line works for voice communication. Integrated Services Digital Network (ISDN) is a good example of circuit switching. When a router has data for a remote site, the switched circuit is initiated with the circuit number of the remote network. In the case of ISDN circuits, the device actually places a call to the telephone number of the remote ISDN circuit. When the two networks are connected and authenticated, they can transfer data. When the data transmission is complete, the call can be terminated. Figure 3-3 illustrates an example of this type of circuit.

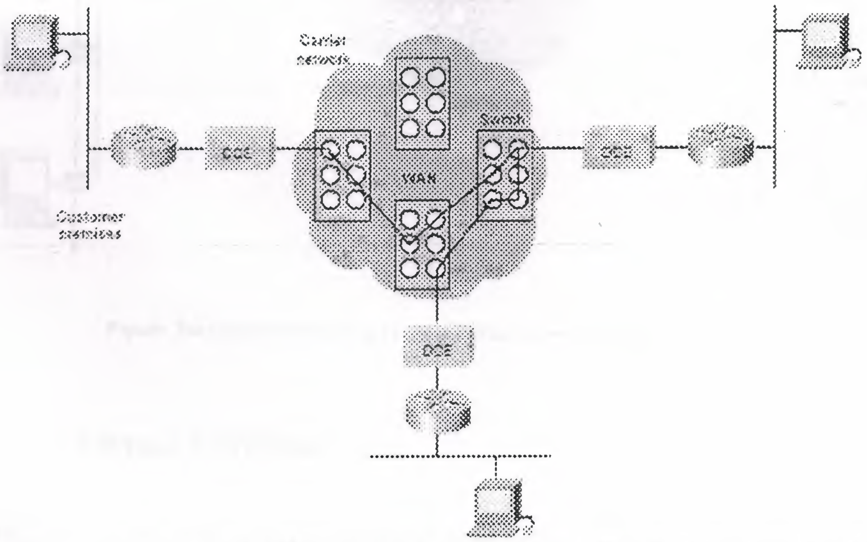


Figure 4.3 A Circuit-Switched WAN Undergoes a Process Similar to That Used for a Telephone Cal

4.4 Packet Switching

Packet switching is a WAN technology in which users share common carrier resources. Because this allows the carrier to make more efficient use of its infrastructure, the cost to the customer is generally much better than with point-to-point lines. In a packet switching setup, networks have connections into the carrier's network, and many customers share the carrier's network. The carrier can then create virtual circuits between customers' sites by which packets of data are delivered from one to the other through the network. The section of the carrier's network that is shared is often referred to as a cloud. Some examples of packet-switching networks include Asynchronous Transfer Mode (ATM), Frame Relay, Switched Multimegabit Data Services (SMDS), and X.25. Figure 3-4 shows an example packet-switched circuit. The virtual connections between customer sites are often referred to as a virtual circuit.

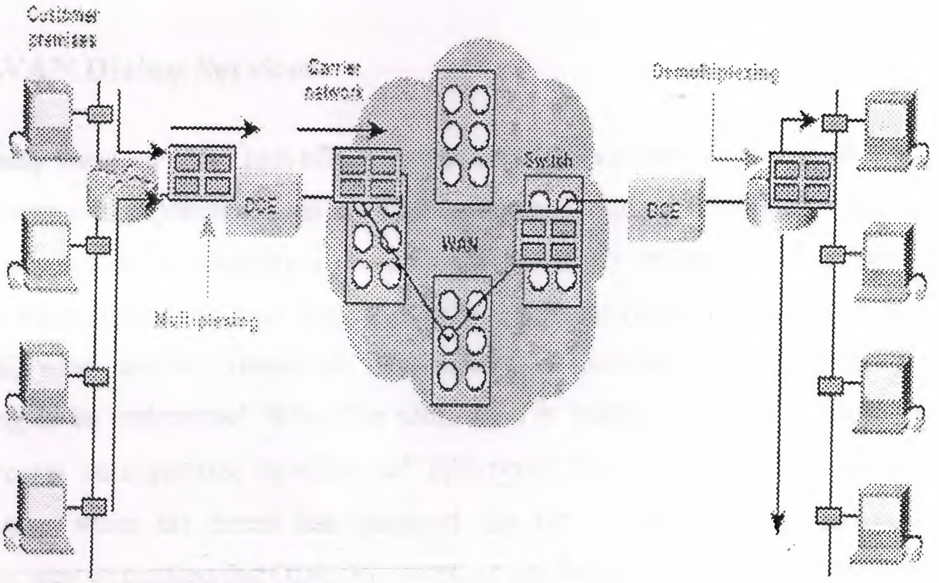


Figure 3-4 Packet Switching Transfers Packets Across a Carrier Network

4.5 WAN Virtual Circuits

A virtual circuit is a logical circuit created within a shared network between two network devices. Two types of virtual circuits exist: switched virtual circuits (SVCs) and permanent virtual circuits (PVCs). *SVCs* are virtual circuits that are dynamically established on demand and terminated when transmission is complete. Communication over an SVC consists of three phases: circuit establishment, data transfer, and circuit termination. The establishment phase involves creating the virtual circuit between the source and destination devices. Data transfer involves transmitting data between the devices over the virtual circuit, and the circuit termination phase involves tearing down the virtual circuit between the source and destination devices. SVCs are used in situations in which data transmission between devices is sporadic, largely because SVCs increase bandwidth used due to the circuit establishment and termination phases, but they decrease the cost associated with constant virtual circuit availability. *PVC* is a permanently established virtual circuit that consists of one mode: data transfer. PVCs are used in situations in which data transfer between devices is constant. PVCs decrease the bandwidth use associated with the establishment and termination of virtual circuits, but they increase costs due to constant virtual circuit availability. PVCs are generally configured by the service provider when an order is placed for service.

4.6 WAN Dialup Services

Dialup services offer cost-effective methods for connectivity across WANs. Two popular dialup implementations are dial-on-demand routing (DDR) and dial backup. *DDR* is a technique whereby a router can dynamically initiate a call on a switched circuit when it needs to send data. In a DDR setup, the router is configured to initiate the call when certain criteria are met, such as a particular type of network traffic needing to be transmitted. When the connection is made, traffic passes over the line. The router configuration specifies an idle timer that tells the router to drop the connection when the circuit has remained idle for a certain period. *Dial backup* is another way of configuring DDR. However, in dial backup, the switched circuit is used to provide backup service for another type of circuit, such as point-to-point or packet switching. The router is configured so that when a failure is detected on the primary circuit, the dial backup line is

initiated. The diai backup line then supports the WAN connection until the primary circuit is restored. When this occurs, the dial backup connection is terminated.

4.7 WAN Devices

WANs use numerous types of devices that are specific to WAN environments. WAN switches, access servers, modems, CSU/DSUs, and ISDN terminal adapters are discussed in the following sections. Other devices found in WAN environments that are used in WAN implementations include routers, ATM switches, and multiplexers.

4.8 WAN Switch

A WAN switch is a multiport internetworking device used in carrier networks. These devices typically switch such traffic as Frame Relay, X.25, and SMDS, and operate at the data link layer of the OSI reference model. Figure 3-5 illustrates two routers at remote ends of a WAN that are connected by WAN switches.

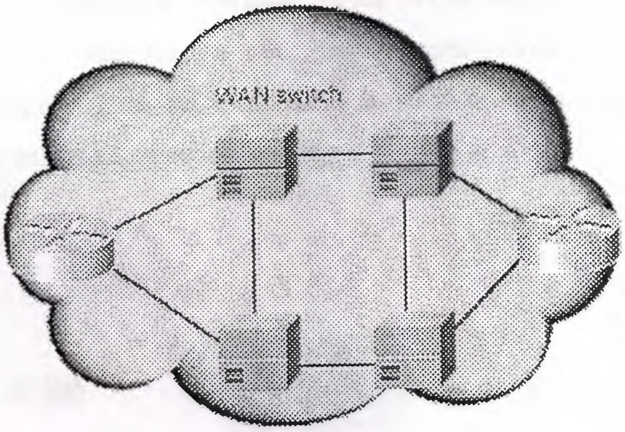


Figure 4.5 Two Routers at Remote Ends of a WAN Can Be Connected by WAN Switches

4.9 Access Server

An *access server* acts as a concentration point for dial-in and dial-out connections. Figure 3–6 illustrates an access server concentrating dial-out connections into a WAN

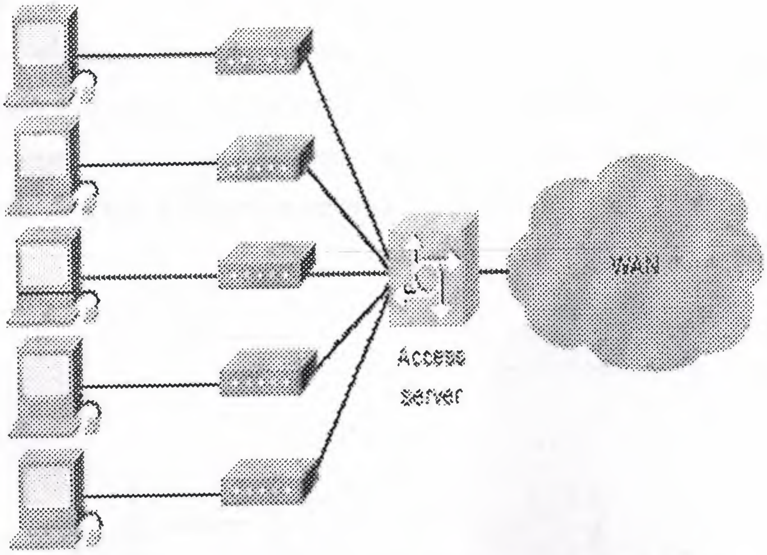


Figure 4.6 An Access Server Concentrates Dial-Out Connections into a WAN

4.10 Modem

A modem is a device that interprets digital and analog signals, enabling data to be transmitted over voice-grade telephone lines. At the source, digital signals are converted to a form suitable for transmission over analog communication facilities. At the destination, these analog signals are returned to their digital form. Figure 3-7 illustrates a simple modem-to-modem connection through a WAN.

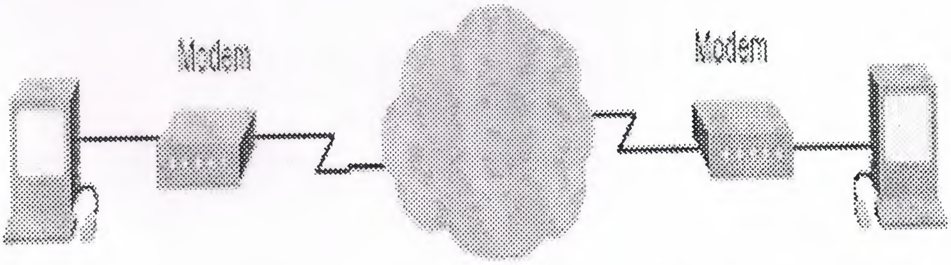


Figure 4.7 A Modem Connection Through a WAN Handles Analog and Digital Signals

4.11 CSU/DSU

A channel service unit/digital service unit (CSU/DSU) is a digital-interface device used to connect a router to a digital circuit like a T1. The CSU/DSU also provides signal timing for communication between these devices. Figure 3–8 illustrates the placement of the CSU/DSU in a WAN implementation.

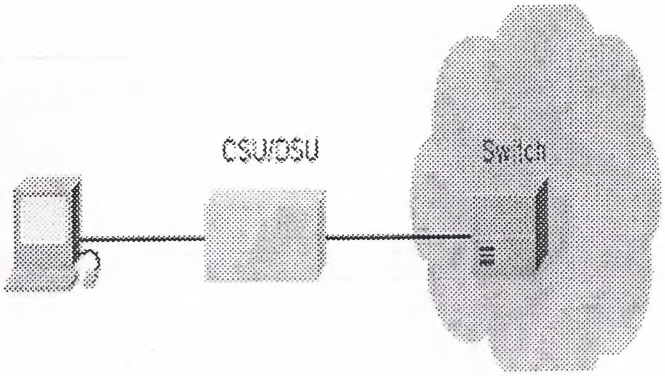


Figure 4.8 The CSU/DSU Stands Between the Switch and the Terminal

4.12 ISDN Terminal Adapter

An ISDN terminal adapter is a device used to connect ISDN Basic Rate Interface (BRI) connections to other interfaces, such as EIA/TIA-232 on a router. A terminal adapter is essentially an ISDN modem, although it is called a terminal adapter because it does not actually convert analog to digital signals. Figure 3-9 illustrates the placement of the terminal adapter in an ISDN environment.

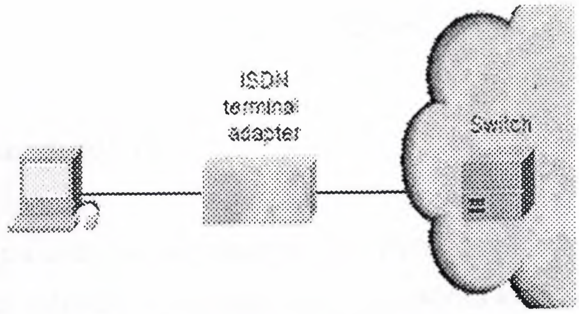


Figure 4.9 The Terminal Adapter Connects the ISDN Terminal Adapter to Other Interfaces

CONCLUSIONS

From this project I concluded that:

- A network is a collection of machines that have been linked together physically and on which software components have been added to facilitate communication and sharing of information..
- Client/Server-Based Networking, Peer-to-Peer Networking are models of networking.
- A local area network (LAN) is a group of computers and network communication devices interconnected within a geographically limited area.
- A wide area network (WAN) interconnects LANs.
- A protocol is a set of rules governing the exchange of data between two entities..
- TCP/IP is a set of protocols developed to allow cooperating computers to share resources across a network.
- Software An end-user application may use a software protocol suite such as the Transfer Control Protocol/Internet Protocol (TCP/IP) or ISO/OSI
- Hardware the physical network medium is designed to carry signals encoded with information, such as coaxial, twisted-pair cable, or fiber-optical materials carrying multi band modulated laser light
- Distance limitations are overcome because each segment can be built with the maximum distance for that type of Ethernet.
- The IP address structure should be logical, not physical, to allow for future growth into new technologies.
- The address is assigned to the interface of the computer, not the computer itself. As mentioned earlier, there are two reserved numbers in each network. One number is the, *network number*, which is used to represent the entire network. The other reserved number is called the *broadcast address*.
- A virtual circuit is a logical circuit created within a shared network between two network devices.

References

1. COTTON, I. [1979], Technologies for local area computer networks.

2. FRANTA, W. R and I. CHLAMTAC [1981], Local networks, Lexington books, Lexington Massachusetts.

3. GREEN, P.E (ED) [1982], Computer network Architectures and protocols, Plenum Press, New York.

4. Tanedaum Andrew S. Computer Network,1996

WORLD WIDE WEB

1. http://www.cisco.com

2. www.IEEE.net

3. www.mit.edu