COURSE TECHNOLOGY
CENGAGE Learning

EC-Council | Press

Network Defense
Fundamentals & Protocols

This title maps to

EC-Council | Network Security Administrator

COURSE TECHNOLOGY
CENGAGE Learning™

Fundamental and Protocols: EC-Council | Press

Course Technology/Cengage Learning Staff:

Vice President, Career and Professional Editorial: Dave Garza

Director of Learning Solutions: Matthew Kane

Executive Editor: Stephen Helba

Managing Editor: Marah Bellegarde

Editorial Assistant: Meghan Orvis

Vice President, Career and Professional Marketing: Jennifer Ann Baker

Marketing Director: Deborah Yarnell

Marketing Manager: Erin Coffin

Marketing Coordinator: Shanna Gibbs

Production Director: Carolyn Miller

Production Manager: Andrew Crouth

Content Project Manager: Brooke Greenhouse

Senior Art Director: Jack Pendleton

EC-Council:

President | EC-Council: Sanjay Bavisi

Sr. Director US | EC-Council: Steven Graham

Library of Congress Control Number: 2010923379

ISBN-13: 978-1-4354-8355-2

ISBN-10: 1-4354-8355-3

Cengage Learning
5 Maxwell Drive
Clifton Park, NY 12065-2919
USA

Cengage Learning is a leading provider of customized learning solutions with office locations around the globe, including Singapore, the United Kingdom, Australia, Mexico, Brazil, and Japan. Locate your local office at: **international.cengage.com/region**

Cengage Learning products are represented in Canada by Nelson Education, Ltd.

For more learning solutions, please visit our corporate website at **www.cengage.com**

NOTICE TO THE READER

Cengage Learning and EC-Council do not warrant or guarantee any of the products described herein or perform any independent analysis in connection with any of the product information contained herein. Cengage Learning and EC-Council do not assume, and expressly disclaim, any obligation to obtain and include information other than that provided to it by the manufacturer. The reader is expressly warned to consider and adopt all safety precautions that might be indicated by the activities described herein and to avoid all potential hazards. By following the instructions contained herein, the reader willingly assumes all risks in connection with such instructions. Cengage Learning and EC-Council make no representations or warranties of any kind, including but not limited to, the warranties of fitness for particular purpose or merchantability, nor are any such representations implied with respect to the material set forth herein, and Cengage Learning and EC-Council take no responsibility with respect to such material. Cengage Learning and EC-Council shall not be liable for any special, consequential, or exemplary damages resulting, in whole or part, from the readers' use of, or reliance upon, this material.

Printed in the United States of America
1 2 3 4 5 6 7 13 12 11 10

Chapter 1

Fundamentals of Computer Networks

Objectives

After completing this chapter, you should be able to:

- List the operations of various key elements in a network
- Understand IP address assignments
- Create a domain name space
- List the functional categories and operations of gateways
- List the media types used to connect networks
- Use various media access methods
- Understand the OSI reference model
- Understand various data transmission methods
- Explain logical network arrangements
- Classify networks

Key Terms

Backbone a network component that combines many networks and subnets into a single channel

Bus topology a multipoint topology that consists of a long cable that acts like a support structure for the entire network

Domain name system (DNS) an Internet service that translates domain names into IP addresses

Gateway a node that routes traffic from one workstation to an outside network

IP address a unique 32-bit number assigned to all devices communicating in a network using the Internet Protocol (IP)

Network a group of computers connected together so that information can be exchanged among the computers

Operations security (OPSEC) a identifies, controls, and protects classified or sensitive information

Peer-to-peer network a network in which every computer operates as a client and a server

Subnet a logical grouping of the devices in a network, created by subdividing a larger network address

Introduction to the Fundamentals of Computer Networks

This chapter discusses the operations of various key elements in a network, including: IP address assignments, domain name spaces, working and functional categories of gateways, media types used to connect networks, media access methods, the OSI reference model, data transmission methods, logical network arrangements, network classes, physical arrangements of the network (including topologies), and network equipment functions.

Networks

A ***network*** is a group of computers connected together so that information can be exchanged among the computers. A network can be divided into several subnets depending on usage and the requirements. Network speed is measured in megabits per second (Mbps). Networking allows the user to perform the following tasks:

- Share a single Internet connection among many systems
- Share network resources like printers, scanners, etc.
- Share files and folders

Setting Up a Network

Table 1-1 shows how to connect computers together using an Ethernet adapter, Home Phoneline Networking Alliance (HPNA) adapter, or wireless network adapter.

Connection Type	Required Hardware	Computer Configuration
Ethernet	A network adapter is installed into each computer and then connected to a network hub.	Configure an Ethernet network using a network hub
HPNA	A network adapter is installed into each computer, and then they are plugged into phone jacks using telephone cables.	Configure a phone-line network
Wireless network	A wireless network adapter is installed into each computer.	Configure a wireless network

Table 1-1 **This table shows the necessary elements of various connection types**

Steps to Set Up a Network

The checklist below lists the steps, in order of completion, for setting up a home or small office network using the Wireless Network and Network Setup Wizards for a Windows XP/NT system. If a step does not apply, go on to the next step. Print this checklist for reference:

1. Sketch the network. Draw a diagram of the home or office, showing the location of each computer and printer.
2. Next to each computer, note the hardware, such as modems and network adapters, installed on each computer.
3. Choose the computer on which the residential gateway will be set up (or the computer that will be the Internet Connection Sharing [ICS] host computer). It is recommended that this computer be running Windows XP Home Edition, Windows XP Professional, Windows Vista, or Microsoft Windows XP Service Pack 2 (SP2).
4. Determine the type of network adapters needed for the network: Ethernet, HPNA, wireless.
5. Make a list of necessary hardware. This includes modems, network adapters, hubs, and cables.
6. Buy the hardware.
7. Install the correct network adapters and modems on each computer.
8. If the network will be wireless, run the Wireless Network Setup Wizard.

9. Physically connect the computers together. Plug the cables into hubs, phone jacks, and the computer.
10. Turn on all computers and printers.
11. Make sure the computer attached to the residential gateway (or the ICS host computer) has an active Internet connection. To establish an Internet connection, run the New Connection Wizard.
12. Run the Network Setup Wizard on the computer attached to the residential gateway (or the ICS host computer).
13. Run the Network Setup Wizard on the other computers on the network.

Backbone

A ***backbone*** combines many networks and subnets into a single channel. The capacity of the backbone is greater than that of the network. A backbone network uses a mesh topology, which provides many-to-many connections on the network. There was once just a single backbone network called ARPANET, but now each Internet service provider (ISP) has its own backbone network.

There are two types of backbones:

1. *Distributed backbones*: A distributed backbone runs through the premises/building and connects to each local area network (LAN) and subnet. A router is used to connect the network to the backbone.
2. *Collapsed backbones*: A collapsed backbone is configured with the star-wired topology. A hub or switch is placed in the center of the premises, and each network is connected to the central hub or switch.

80/20 and 20/80 Rule

Old network backbones were used to pass nearly 20% of the network traffic, and the remaining 80% was limited to LANs and subnets. This rule (known as 80/20) failed due to inadequate utilization of the network backbone.

The current backbones are designed in such a way that only 20% of the traffic remains limited to LANs and subnets, whereas 80% is passed to backbones. This rule (known as the 20/80 rule) increases the efficiency of backbones because approximately 80% of LAN traffic is passed to them through the central hub or switch.

Reasons to adopt the 20/80 rule include:

- Users communicate more to an external network than within the same network.
- Organizations typically use a centralized server.
- Network traffic is routed through the hub or switch due to the use of the Internet.

Segments

Large networks are divided into segments to improve the performance of the network. Segments also reduce IP address collisions. Routers, switches, bridges, and multihomed gateways are used to connect the different segments. Segments enable organizations to provide different levels of security to individual departments.

Any data packet sent from a host goes to the default gateway. The packet's destination IP address and subnet mask are matched with the host IP address and subnet mask. If the IP addresses and subnet masks match, the packet is forwarded to the host's local segment; otherwise, it is forwarded to the default gateway of the destination host. If the IP addresses and subnet masks match, traffic broadcasting and multicasting is done in the local segment without disturbing the traffic of other subnets.

Segments help in containing virus and malware attacks in a network, by limiting an attack on a segment of the network to that particular segment. Before segmenting a network, an administrator has to look for the following factors:

- Types of service available to users
- Broadcasting domains

Segmentation makes it easier to implement different technologies or applications, in different departments, according to their specific needs.

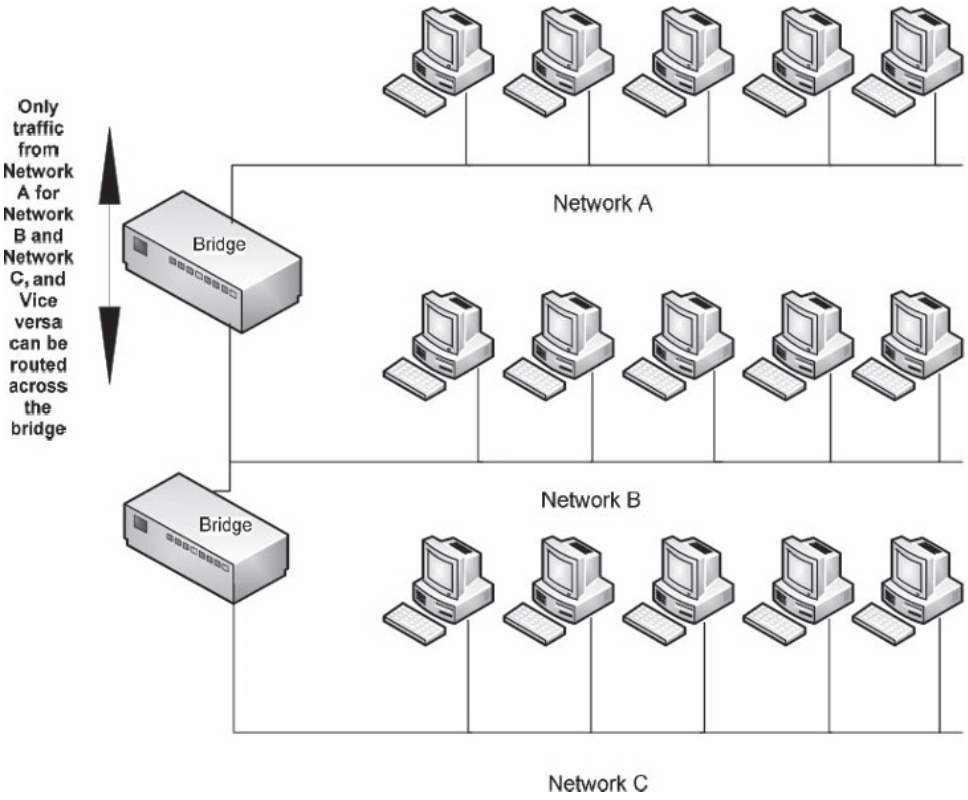


Figure 1-1 This figure represents segmentation with the use of a bridge.

Segmenting a Network with a Bridge

A bridge operates in the data-link layer and helps in collision detection. Bridges dynamically build a routing table containing MAC addresses and port addresses. Bridges are also used to connect different segments in a LAN. The forwarding of frames is done by the destination addresses in the frame. The primary issue with using a bridge is that it broadcasts to all network segments, as shown in Figure 1-1. This is called a *broadcast storm*.

Segmenting a Network with Switches

Many objectives are achieved in using a switch to segment a network. It offers the following advantages:

- Full-duplex communication
- Medium-rate adaptation
- Easy migration from one segment to another
- Switches can dynamically learn the network topology and filter the traffic

Segmenting a Network with Routers

Routers maintain a table of records for the devices connected to the network. Routers operate at the network layer of the OSI reference model and keep a record of the networks, irrespective of the hosts. Logical addresses perform packet filtering.

Subnet

A ***subnet*** is a logical grouping of the devices in a network, created by subdividing a larger network address. It is a logical partitioning of the network address into smaller, discrete sections. The addresses of the devices in the subnet have the same prefix. A subnet mask defines the boundary of the network. An IP address subnet can be identified by its subnet mask, as shown in Figure 1-2.

	Subnet mask	total -addresses
/20	255.255.240.0	4096
/21	255.255.248.0	2048
/22	255.255.252.0	1024
/23	255.255.254.0	512
/24	255.255.255.0	256
/25	255.255.255.128	128
/26	255.255.255.192	64
/27	255.255.255.224	32
/28	255.255.255.240	16
/29	255.255.255.248	8
/30	255.255.255.252	4

Figure 1-2 Subnet masks hide network architecture.

Subnets have the following advantages:

- Can hide the internal architecture or the network from the external router.
- Can be used to group hosts according to their actual logical structure in the organization's physical network; it gives each department an opportunity to implement specific security measures.

Tips to Find Subnets and Broadcast Addresses

Subnets and broadcast addresses can be identified by the subnet mask. The incremental number of the subnet mask can be calculated by subtracting the last octet of the subnet mask from 256.

For example, an IP address of 10.1.12.1 and subnet mask of 255.255.248.0 has an octet of 248. So 256 – 248, which equals 8, will be the incremental number for subnets 10.1.8.0, 10.1.16.0, and 10.1.24.0. In this example, each subnet network address will have an assignable range of 2,046 IP addresses from 10.1.8.1 to 10.1.15.254. This excludes the network address 10.1.8.0 and the broadcast address, which cannot be assigned to any device. Since 10.1.12.1 falls between 10.1.8.0 and 10.1.16.0, within the referred to range, the subnet address for IP 10.1.12.1 will be 10.1.8.0.

The broadcast address is one less than the next subnet address (10.1.16.0); thus, 10.1.15.255 will be the broadcast address of IP 10.1.12.1.

IP Address Assignments

IP Address

An ***IP address*** is a unique 32-bit number assigned to all devices communicating on a network using the Internet Protocol (IP). The IP address is also used to identify a network and its host. IPv4 addresses are represented in dotted-decimal notation, with four numbers, each ranging from 0 to 255, separated by dots. There are 2^{32} possible IP addresses.

IP address classifications include the following designations:

- *Class A*: Large networks with many devices
- *Class B*: Medium-sized networks
- *Class C*: Small businesses with fewer than 256 devices
- *Class D*: Multicast networks
- *Class E*: Not assigned; reserved for future purposes

The following IP address parameters apply to the various IP designations:

- *Default network*: The default IP address is 0.0.0.0.
- *Class A*: The first higher-order bit in the binary address starts with 0. The decimal number is between 0 and 127 and is mostly used by international companies. From the 32-bit address, the Class A address uses the leftmost 8 bits for identifying networks with a default subnet mask of 255.0.0.0. It should be noted that the 127 address range is used exclusively for testing, as in the loopback address 127.0.0.1.
- *Class B*: Medium-scale networks use the leftmost 16 bits of this class for the network part of the address, and the first two higher-order bits in the binary address are 10. The first octet has a decimal number from 128 to 191 and a default subnet mask of 255.255.0.0.
- *Class C*: The first three higher-order bits in the binary address of Class C are 110, so the decimal number can be anywhere between 192 and 223; it is mainly used for small businesses. It uses the first 24 bits, while the other 8 bits are used for the identification of the host on the network. Its default subnet mask is 255.255.255.0.
- *Class D*: The first four higher-order bits in the binary address are 1110, and the decimal address is between 224 and 239. This address range is used exclusively for multicasting.
- *Class E*: The first five higher-order bits in the binary addresses in this class are 11110 and are primarily reserved for future use.
- *Loopback address*: The address 127.0.0.1 is used as the loopback address, which is mainly used by the host computer to send messages to itself and for network testing.
- *Broadcast address*: Messages sent to all the computers on a network are broadcast using the address 255.255.255.255.

ICANN

The Internet Corporation for Assigned Names and Numbers (ICANN) is the authority that manages the assignment of IP addresses, IP address spaces, and protocol identifier assignments. ICANN is a nonprofit organization. The aim of ICANN is to ensure that all users are assigned valid addresses. ICANN is not related to Internet content control, data protection, or unsolicited mail.

ICANN is responsible for the management of the following gTLDs (generic top-level domains):

- *.com*: For businesses
- *.net*: For network providers
- *.org*: Miscellaneous
- *.edu*: For educational institutes
- *.gov*: For government agencies
- *.mil*: For military agencies
- *.int*: For international organizations

"Country Code" Top-Level Domains

Top-level domains also exist for every country in the world (for example, .ca for Canada and .au for Australia).

In 2000, the ICANN Board selected seven new TLDs to be included in the first addition of a global TLD to the Internet since the 1980s.

They are the following:

- *.aero*: For the air transport industry
- *.biz*: For business organizations
- *.coop*: For cooperative organizations
- *.info*: For information services
- *.museum*: For museums

- *.name*: For individuals, by name
- *.pro*: For professionals

In the years 2005–2006, the following four additional gTLDs were sponsored:

- .cat
- .jobs
- .mobi
- .travel

IP Address Space

IPv4 addresses are made up of 32 bits, which provides a limited address space of 2^{32}. With the growing technology and the exponential increase in the number of Internet users, an IPv4 address shortage was inevitable. This has served as a motivation for development of a more-robust addressing system, IPv6, which has addresses made up of 128 bits and provides an address space of 2^{128}. In the meantime, organizations as well as the Internet community are adopting subnetting and the use of private IP addresses to manage the IP address shortage.

Purpose of Dots

It can be difficult to remember a particular decimal number address. To make it easier to remember, the decimal is used to divide it into four parts. With the logical classification of the address, it is easier to identify a particular host on the network. The scheme is based on decimal number and the address space used is binary. Certain schemes use binary numbers, whereas others use decimal numbers directly. Therefore, the 32-bit address space is further divided into four equal components, called octets, of 8 bits each. An example is 202.53.13.138.

Subnetting a Classful Address Space

The IP address space is divided into Classes A, B, C, D, and E. Subnetting these address class spaces into smaller sections is called classful addressing. Classful addressing is adopted to overcome the problem of duplication of addresses, as shown in Figure 1-3. However, public networks do not use classful addressing.

Address Space Allocation Among Major Geographical Areas

Address Space	Area of Allocation	Date Allocated
64.0.0.0 to 64.255.255.255	ARIN	Jul-99
128.0.0.0 to 191.255.255.255	Various registries	May-93
192.0.0.0 to 192.255.255.255	Multiregional	May-93
193.0.0.0 to 195.255.255.255	RIPE NCC-Europe	5/1/1993
196.0.0.0 to 198.255.255.255	various registeries	5/1/1993
199.0.0.0 to 199.255.255.255	ARIN-North America	May-93
200.0.0.0 to 200.255.255.255	ARIN-Central and South America	5/1/1993
201.0.0.0 to 200.255.255.255	Reserved- Central and South America	May-93
202.0.0.0 to 203.255.255.255	APNIC-Pacific Rim	May-93
204.0.0.0 to 205.255.255.255	ARIN-North America	Mar-94
206.0.0.0 to 206.255.255.255	ARIN-North America	Apr-95
207.0.0.0 to 207.255.255.255	ARIN-North America	Nov-95
208.0.0.0 to 208.255.255.255	ARIN-North America	Apr-96
209.0.0.0 to 209.255.255.255	ARIN-North America	Jun-96
210.0.0.0 to 210.255.255.255	APNIC-Pacific Rim	Jun-96
211.0.0.0 to 211.255.255.255	APNIC-Pacific Rim	Jun-96
212.0.0.0 to 212.255.255.255	RIPE NCC-Europe	Oct-97
213.0.0.0 to 213.255.255.255	RIPE NCC-Europe	Mar-99
216.0.0.0 to 217.255.255.255	ARIN-North America	Apr-98

Figure 1-3 Address spaces are allocated to specific areas.

The following protocols are examples of those used to route information from one network or subnet to another:

- *RIP*: Routing Information Protocol
- *IGRP*: Internet Gateway Routing Protocol

IP Address Assignment

Every computer in a network can have a static IP address, as shown in Figure 1-4. In a network that has a shared connection, addresses can also be assigned dynamically. Generally, the ISP providing the connectivity assigns the IP addresses.

Addressing types include the following:

- Prefix-based addressing
- Per-interface based assignment
- Virtual addressing
- Static addressing
- Dynamic addressing

Prefixed-Based Addressing

The prefix can be used for general routing decisions. For example, the first 8 bits may identify the particular company, and then the next 8 bits may identify the particular department of the office. The next 8 bits may identify the particular network in that office. Finally, all 32 bits will identify the host on the network.

Per-Interface Assignment

A host can have an equal number of IP addresses and interfaces. An IP address can also represent an interface.

Virtual Addressing

Virtual addresses are used when a single server provides services through several addresses. There is no standard for virtual addressing.

Static Addressing

The following are the steps for assigning a static IP address in Windows:

1. From the Start menu, select **Control Panel**, and then open **Network Connections**.
2. Select **Network and Internet Connections**.
3. Double-click **Active LAN or Internet Connection**.
4. Select **Properties**.
5. As a result, the **Local Area Connection Properties** dialog box will be opened.
6. Double-click **Internet Protocol TCP/IP**.
7. Click the **Properties** button, as shown in Figure 1-5.
8. Select the **Use the following IP address** check box, as shown in Figure 1-4.
9. In the **IP address** field, type the IP address.
10. Insert the subnet mask used by your router.
11. The default gateway is the IP address of the router.
12. In the **Use the following DNS server address** field, enter the IP addresses of the DNS server the router is using.
13. Click **OK**.

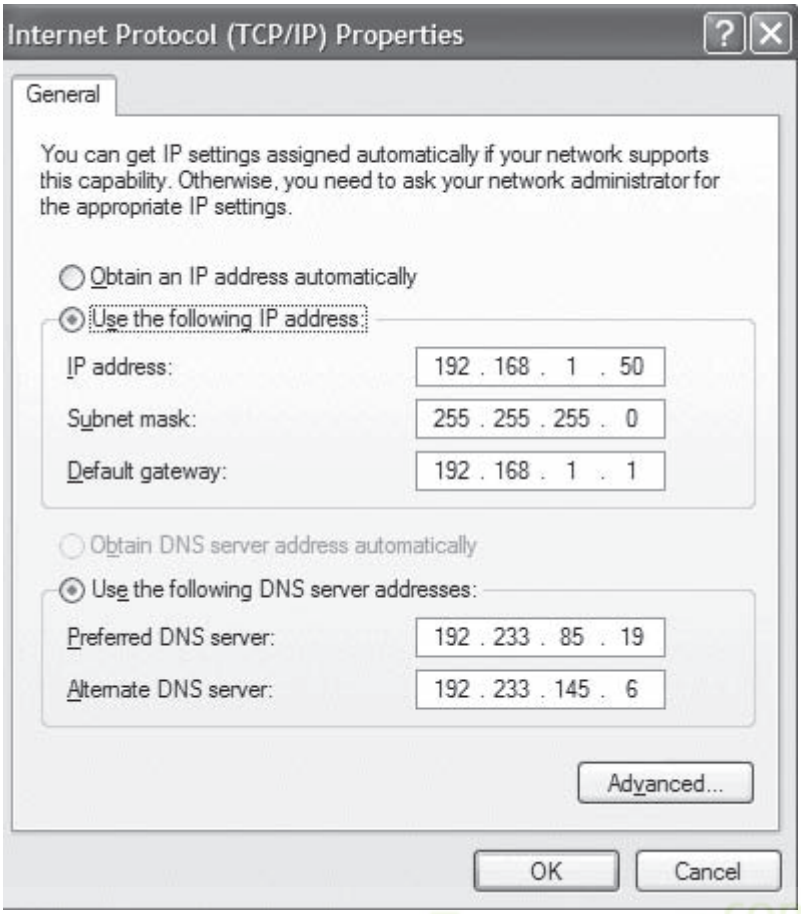


Figure 1-4 Static addressing can be performed through the Control Panel.

Dynamic Addressing

The following are the steps for assigning a dynamic address in Windows:

1. From the Start menu, select **Control Panel** and then double-click **Network Connections**.
2. Right-click **Desired Network Connection** to configure it, and then click **Properties**.
3. Select the **General** tab or **Networking** tab.
4. Click **Properties**.
5. Check the **Obtain the IP address automatically** check box, and then click **OK**, as shown in Figure 1-6.

To locate the current IP address, perform the following steps:

- Go to the Start menu
- Select **Run**
- Type **cmd**
- Run the **ipconfig /all** command

Check the **Dhcp Enabled** line to determine if the IP address is dynamically assigned or is static (Figure 1-7).

- *No* means the IP address is static.
- *Yes* means the IP address is dynamic.

The IP address shown is the current system IP address.

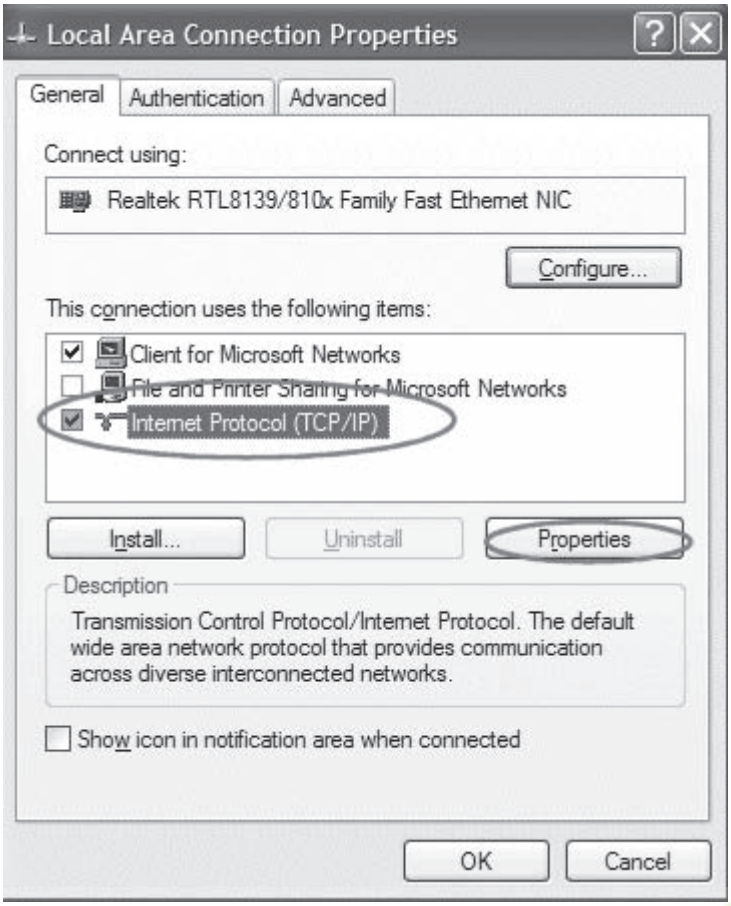


Figure 1-5 Click the **Properties** button.

Creating a Domain Name Space

Domain Name System

The ***domain name system (DNS)*** is an Internet service that translates domain names into IP addresses. It is a hierarchical and distributed database containing host and domain names. A fully qualified domain name (FQDN) can identify the particular host within the hierarchical tree architecture. DNS makes it possible to assign domain names independent of the physical routing hierarchy represented by the numerical IP address.

Domain Name System Organization

DNS is organized in the form of a hierarchy, as shown in Figure 1-8. The topmost level in the hierarchy is the root domain, which is represented as a dot (.) at the very end of the domain name, but is seldom shown in domain names. The next level in the hierarchy includes the top-level domains (TLDs).

The name of each node or domain could be up to 63 characters long. Traversal of DNS is done in reverse order from the leaf node to the root, meaning from the leftmost name to the rightmost. Whenever a particular message consists of multiple domains, the traversal will start from the first domain.

TLDs are divided into three categories:

1. *Country-code TLDs (ccTLDs)*: Domains associated with countries and territories. There are more than 240 ccTLDs. Examples include .uk, .in, and .jp.
2. *Sponsored generic TLDs (gTLDs)*: Specialized domains with a sponsor representing a community of interest. These TLDs include .edu, .gov, .int, .mil, .aero, .coop, and .museum.
3. *Unsponsored gTLDs*: Domains without a sponsoring organization. The list of unsponsored gTLDs includes .com, .net, .org, .biz, .info, .name, and .pro.

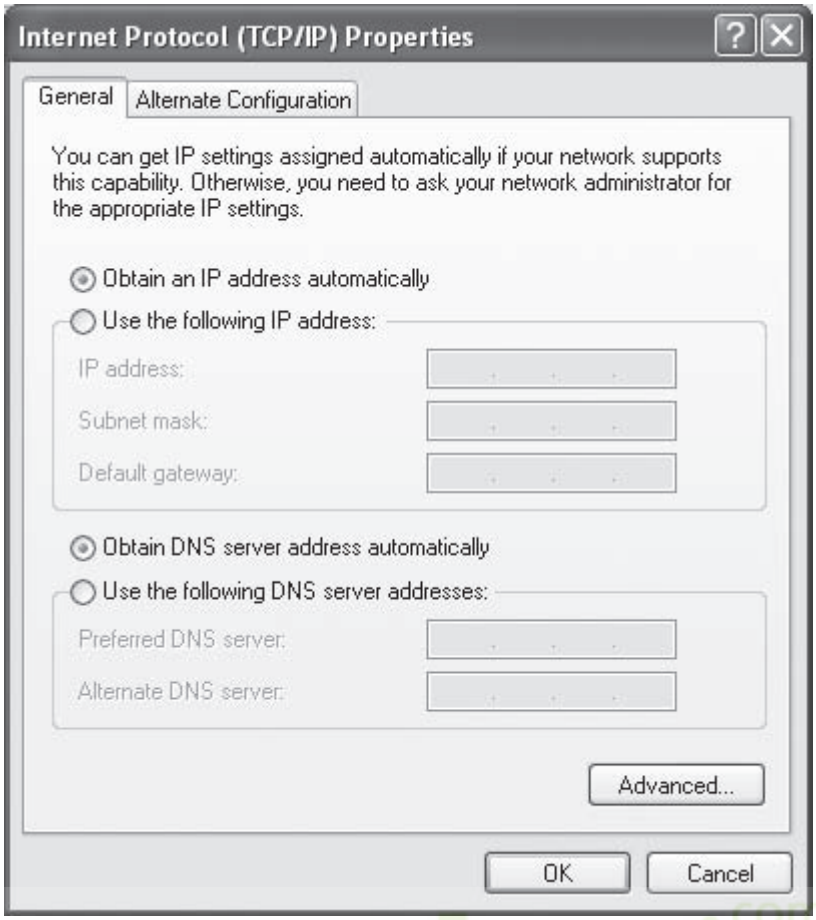


Figure 1-6 Users can also choose to assign an IP address automatically.

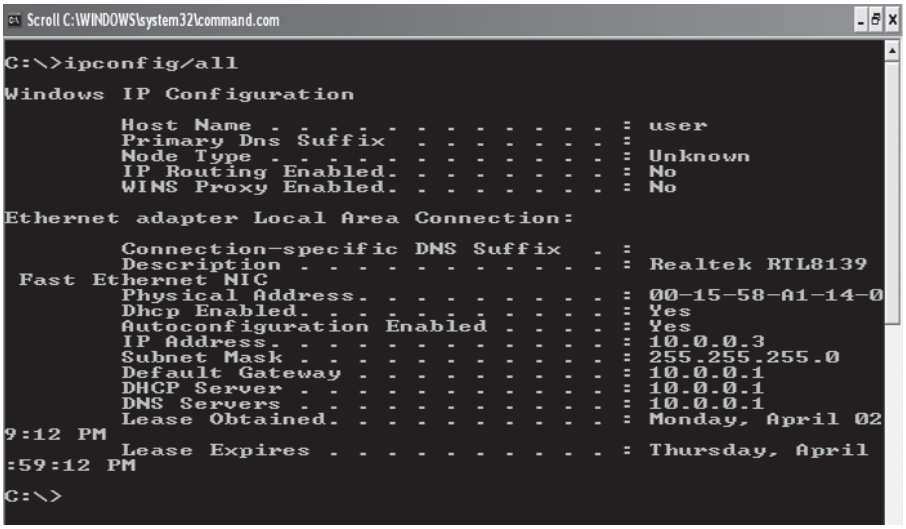


Figure 1-7 *Yes* or *no* on the Dhcp Enabled line indicates the state of the IP address.

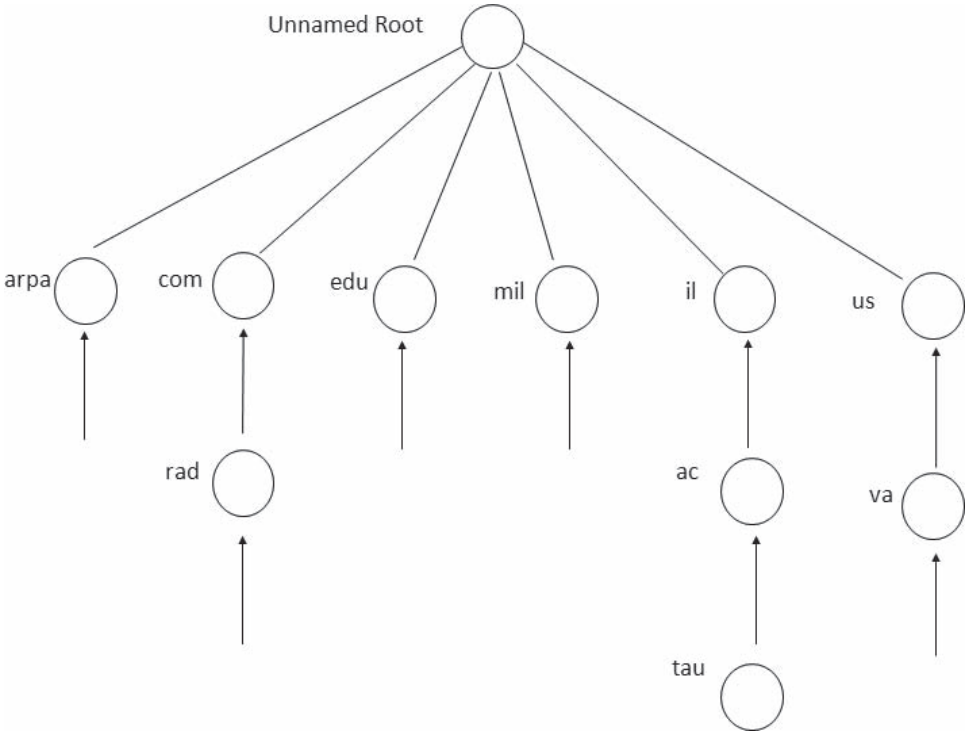


Figure 1-8 DNS is organized hierarchically.

Domain Names

Domain names give a unique identity to an organization or an entity on the Internet. Domain names should be catchy, short, and easy to remember. The domain name has to be registered before it can be used.

A domain name consists of a set of resource records (RR). An RR must have the host address and specifies the domain name. The RR consists of a resource type field, which specifies the type of resource the particular resource record has, and a class field, which specifies the format of the data.

Domains use the hierarchical format for the structured information. The different values used in the resource type field are the following:

- *A*: Host address that is associated with the domain
- *MF*: Identifies a mail forwarder for the domain
- *MX*: Mail Exchanger records
- *NS*: Identifies the name server that is authoritative for the domain
- *SOA*: Start of a zone for an authority
- *CNAME*: Lists the canonical name of an alias
- *PTR*: Pointer records that facilitate reverse lookup from an IP address to a domain name

Creating a New Domain Name The name should give an idea of what a particular organization does. Review the following naming conventions for domains:

- A dot
- Letters from A to Z in uppercase or lowercase
- Numbers from 0 to 9

- Combinations of alphabetic characters and numbers
- Maximum length should not exceed 64 bits
- Hyphens and underscores are also acceptable

Once the name is decided, the domain name should be registered. Domain names are registered by government agencies as well as nonprofit organizations. Every domain name has a set of registry policies that should be followed.

Components of a DNS

There are three main components of a DNS:

1. Domain name space and resource records
2. Name servers
3. Resolvers

Domain Name Space and Resource Records

These elements specify the structural hierarchy of the name space and the data associated with it. Each node has particular information associated with it. Queries are sent to get the specific information from the domains. The result is the domain name and the type of information required.

Name Servers

These contain information about the structure of the domain. Authoritative information is organized into units called zones, which can be automatically distributed to the name servers that provide redundant service for the data in a zone.

There are two types of name servers:

1. Authoritative
2. Caching

Resolvers Resolvers are programs that obtain information from name servers when they get the client request. Resolvers refer to at least one server, and answer a query directly or take the reference from the other servers. It is a system routine, which directly accesses the user programs.

Securing the Cache Against Pollution The DNS query response sometimes contains malicious data, but by default, DNS is secured against cache pollution. An attacker can successfully pollute the cache of a DNS server by sending resource records without the request of the server.

Disabling Recursion Recursion is not disabled in a DNS server. Because of this, a DNS server executes queries for the DNS clients repeatedly in response to a request. Attackers use recursion to reduce the performance of a DNS server.

Managing the DACL With a DACL (discretionary access control list), control of active directory users and groups is possible. The list for default groups, usernames, and permissions for the DNS server service is illustrated in Figure 1-9.

Threats to DNS

Rogue DNS Server Information on a rogue DNS server is not trustworthy. Host-name spoofing and DNS spoofing is done using rogue DNS servers. On the primary server, the PTR record in the ZONE data file is configured to point somewhere other than the correct record. Host-name spoofing can have a TTL of zero that results in caching of misleading information.

Denial of Service There is a chance of a negative response from a DNS server. Sending back a negative response for a DNS name that could not be resolved can result in a denial of service (DoS).

Another DoS attack involves cache poisoning, in which a CNAME record is inserted that refers to itself in its canonical form.

Client Flooding Client flooding results when the client sends a request and gets thousands of responses from a DNS server. This attack cannot be identified, as the client thinks that it is coming from an authorized DNS server. The flooding cannot be identified because the origin of the responses is unknown.

Group or User names	Permissions
Administrator	Allow: Read, Write, Create All Child Objects, Special Permissions
Authenticate Users	Allow: Read, Special Permissions
Create Owner	Special Permissions
DNS Admins	Allow: Full control, Read, Write, Create All Child Objects, Delete Child objects, Special Permissions
Domain Admins	Allow: Full control, Read, Write, Create All Child Objects, Delete Child objects
Enterprise Admins	Allow: Full control, Read, Write, Create All Child Objects, Delete Child objects
Enterprise Domain Controllers	Allow: Special Permissions
Pre-Windows 2000 Compatible Accecss	Allow: Special Permissions
System	Allow: Full control, Read, Write, Create All Child Objects, Delete Child objects, Special Permissions

Figure 1-9 Specific permissions are assigned for the DNS server service.

Functional Categories and Operations of Gateways

Gateways

A ***gateway*** is a node that routes traffic from workstations to an outside network. For example, when an e-mail is sent, there is a gateway that permits the connection to take place. Gateways are also used as proxy servers and firewalls. Gateways consist of a router and switch. The router determines where the packets are to be sent, and the switch provides the actual path in and out of the gateway.

Functional Categories of Gateways

Gateways are commonly divided into three categories:

1. Data gateways
2. Multimedia gateways
3. Home-control gateways

Data Gateways These simple routers are basically used for data throughput. They support both wired and wireless networking, and they provide pass-through support for network protocols and services. Data gateways can be used to pool multiple Internet connections and secure private networks using firewalls. Some of these also provide storage, such as e-mail and voice-mail storage.

Multimedia Gateways Multimedia gateways provide features for audio and video content delivery. They are often used in combination with digital entertainment devices (including TVs and stereo systems) and provide centralized storage. They can behave like a home server for digital media such as photos, videos, MP3 files, and Web site hosting. In multimedia gateways, audio and video streaming are important features. Video on demand (VOD) and VoIP (Voice over IP) are gateways that include encoding capabilities that translate analog audio and video signals.

Home-Control Gateways Home-control gateways provide home-control and security management services on a network. For example, users can access automated lighting, heating, and security systems with a home-control gateway. They also permit network service providers to provide new service packages and generate new revenue streams.

Media Types Used to Connect Networks

Types of Network Media

There are three primary types of network cables:

1. Twisted-pair cables
2. Coaxial cables
3. Fiber-optic cables

Historical Versus Current Communication Methodology

The method of exchanging information from one system to another is a communication method. Historically, the means to communicate were direct connections or telecommunication used as media. However, this method was unstable as well as time consuming.

Currently, communication has evolved into various networking and highly secured features. Organizations can rely on data obtained through this communication. Communication has extended its growth to such an extent that information can be exchanged or sent globally within a short amount of time (for example, over the Internet).

Asynchronous Versus Synchronous

Communication between two parties is performed by the communication circuit as described in the physical layer and data-link layer of the Open System Interconnection (OSI) model. In general, there are two strategies for communication over the physical link: asynchronous and synchronous.

Asynchronous Communication

An asynchronous communication unit includes a transmitter, a receiver, and a wire. Each device uses a clock to measure the length of the message in terms of bits. The transmitter only transmits the message, and the receiving device looks at the incoming signal and coordinates to match it.

In order to match the data, the sender and receiver should use the same encoding and decoding techniques. This is very important, as it will decide where to look for the data in the transmitted signal as it is encoded. Asynchronous systems do not send separate information to indicate the data or clocking information; it is the responsibility of the receiver to decide the clocking of the signal. This means the receiver has to decide where the bits are starting and where they stop. Thus, communication in asynchronous transmission works without consulting the transmitting device.

In asynchronous communication, the data is not retransmitted; it is said to be more efficient when there is low loss and low error rates over the transmission medium. Additionally, no time is wasted in asynchronous communication because none is spent in setting up the connection at the beginning of transmission. Asynchronous communication is a faster means of sending data, but is less reliable.

Synchronous Communication

In synchronous communication, a connection between the transmitter and receiver is established before the communication begins. There is a process that decides which end should control the session. The transmitter, as well as the receiver, can exchange communication parameters and status information.

After the establishment of the connection between the transmitter and the receiver, the transmitter transmits the signal, and the receiver sends an acknowledgment of the data received along with the data. Synchronous communication takes a long time on low error-rate lines, but it is reliable.

Wired Media or Bounded Network Media

Bounded media are network media that travel in a dedicated conductor. It includes wires, cables, and fiber-optics. Copper cable is made of either stranded or solid core wire. Copper wire is affected by attenuation (signal degradation over long distances) and electrical noise. Fiber-optic cable is composed of a very thin glass core and needs to be protected. Fiber cables come in two categories: single mode and multimode.

As fiber cable uses light signals to transfer data, the rate of data transfer is very high. Single-mode fiber transfers data in a single direction, and only one signal at a time. Multimode fiber can be in the same direction or in opposite directions, carry more than one signal at a time.

Dedicated Line

A dedicated line is a communications cable dedicated to a specific application. It is active for and can transfer data for only one application. This is in contrast with shared resources.

Optical Remanence

After the removal of data from storage media, some residue of the information could remain on the media. Optical remanence deals with such residue information, which is the optical representation of information that remains on storage media after it is erased. It is possible to read information stored on CDs or DVDs even though it is erased. Thus, CDs and DVDs that are no longer being used should be destroyed.

Because optical media is not magnetic and cannot be erased by degaussing, destruction is the only choice for storage media such as CD-ROMs, CD-Rs, and DVD-Rs. It will help to fully erase the information stored on it. For media like CD-RWs and DVD-RWs, clearing the media by overwriting is a lengthy process, so these media should be destroyed.

Magnetic Remanence

Residual information can be found on magnetic storage media, such as hard drives and floppy disks, even after the removal of data. Magnetic remanence is the magnetic representation of residual information stored on hard drives, floppy disks, or magnetic tapes that may still be read even after the removal of data.

A degaussing device can remedy this issue. Degaussing is a process of thoroughly deleting data stored on magnetic media. It prevents data from being recovered.

Twisted-Pair Cable

Twisted-pair cable consists of two separately insulated copper wires twisted around each other to reduce interference from the other twisted-pairs in the cable. This is commonly used for telecommunications and modern Ethernet networks. The twisted-pairs in the cable provide protection against cross talk. When an electrical current flows through a wire, it creates a small circular magnetic field around the wire. When two wires in an electrical circuit are positioned close together, their magnetic fields are exactly opposite to each other. Thus, the two magnetic fields cancel each other out, eliminating the problem of cross talk. Cross talk can still be a problem at the ends of the cable when the wires are untwisted to insert into a terminal, such as an RJ-45 Ethernet interface.

There are two types of twisted-pair cable:

1. Unshielded twisted pair (UTP)
2. Shielded twisted pair (STP)

Unshielded Twisted Pair (UTP)

UTP is a cable that is composed of pairs of wires, as shown in Figure 1-10. It is used in different types of networks. It consists of eight individual copper wires, each of which is covered by insulating material, and wires in the pairs are twisted around each other. To reduce cross talk between pairs of UTP, the number of twists can vary between the pairs, with a tighter twist resulting in better transmission.

The quality of this cable may vary from telephone wire to high-speed network cable. These cables are easy to install and are less expensive than other network media.

UTP cable slowly relies on the cancellation effect generated by the twisted wire pairs to control signal degradation caused by electromagnetic interference (EMI) and radio frequency interference (RFI). It is installed using a Registered Jack-45 (RJ-45) connector. RJ-45 is an eight-wire connector used to connect computers in a local area network (LAN), as shown in Figure 1-11.

The features of UTP cable are as follows:

- *Speed and throughput*: 10 to 1000 Mbps
- *Average cost per node*: Inexpensive
- *Media and connector size*: Small
- *Maximum cable length*: 100 m (short)

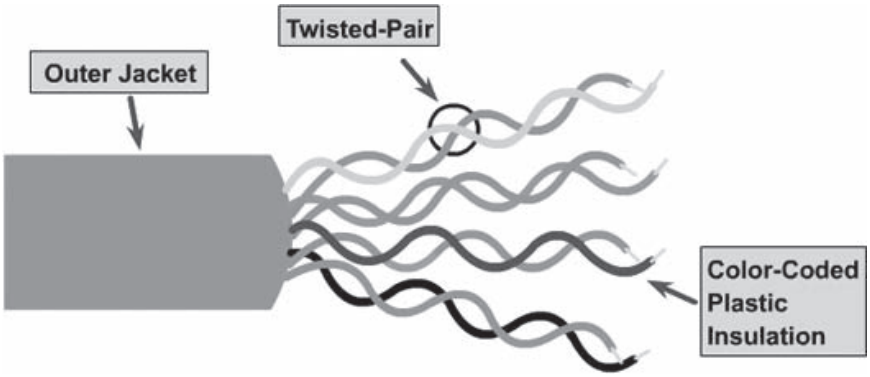


Figure 1-10 Unshielded twisted-pair cable has eight wires that are twisted in pairs.

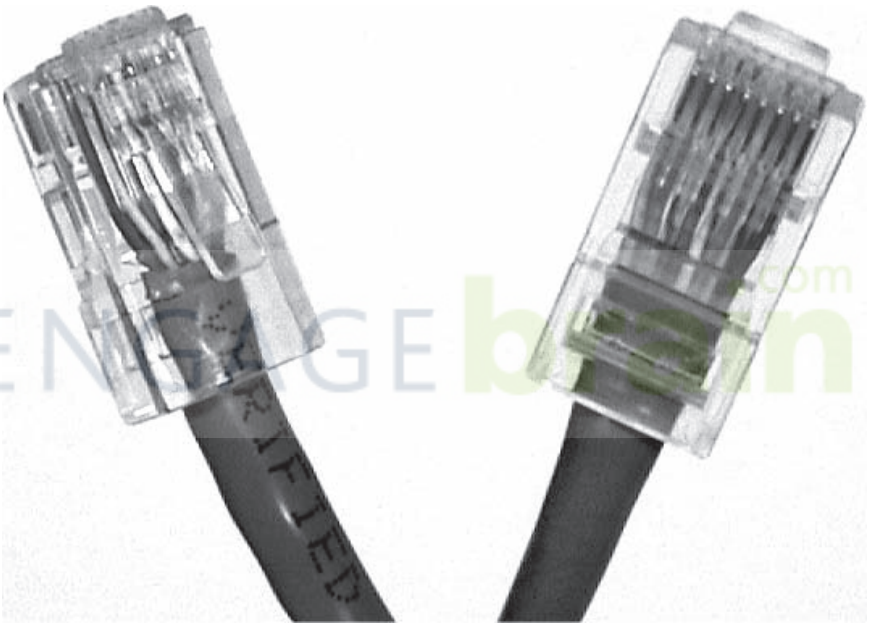


Figure 1-11 RJ-45 connectors are used to connect UTP cables.

The categories of commonly used UTP cabling are as follows:

- *Category 1*: This category is mainly used for telecommunications, not for transmitting data.
- *Category 2*: It is able to transmit data at speeds up to 4 Mbps.
- *Category 3*: It is used in 10BASE-T networks. It can transmit data at speeds up to 10 Mbps.
- *Category 4*: It is used in Token Ring networks. It can transmit data at speeds up to 16 Mbps.
- *Category 5*: It can transmit data at speeds up to 100 Mbps.
- *Category 5e*: It is used in networks running at speeds up to 1000 Mbps (1 Gbps).
- *Category 6*: This cable consists of four pairs of 24 American wire gauge (AWG) copper wires. It is currently the fastest standard for UTP.

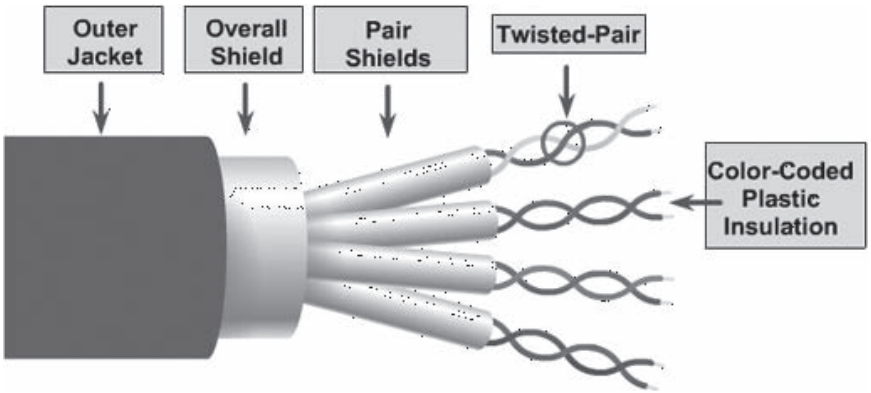


Figure 1-12 A shielded twisted-pair cable uses shielding to reduce electrical noise.

- *Category 7*: This cable standard was created to allow for 10-gigabit Ethernet over 100 m of copper cabling.
- *Category 7a (Augmented Category 7)*: This cable standard allows for operations at frequencies up to 1000 MHz, suitable for multiple applications in a single cable, including 40-gigabit Ethernet, 100-gigabit Ethernet, and CATV.

Shielded Twisted-Pair

STP is a cable that contains metal shielding over each pair of copper wires. It combines the techniques of shielding, cancellation, and wire twisting. Each pair of wires is covered in metallic foil. It reduces the electrical noise both within the cable (pair-to-pair coupling or cross talk) and from outside the cable (EMI and RMI), as shown in Figure 1-12. STP cable is installed with an STP data connector, which is specifically created for STP cables. It can also use the same RJ connector as UTP.

STP prevents interference better than UTP, but it is expensive and difficult to install. The metallic shielding must be grounded at both ends of an STP cable. If it is grounded improperly, the shield behaves like an antenna and picks up unnecessary signals. STP is rarely used in Ethernet networks because of its cost and difficulty with termination.

The following are some of the features of STP cable:

- *Speed and throughput*: 10 to 100 Mbps
- *Average cost per node*: Expensive
- *Media and connector size*: Medium to large
- *Maximum length of cable*: 100 m (short)

Coaxial Cable

Coaxial cable is a kind of copper wire that consists of a hollow cylindrical conductor that surrounds a single inner wire made up of two conducting elements:

1. A copper conductor located in the center of the cable. A flexible layer of insulation encases the copper conductor.
2. A woven copper braid or metallic foil over this insulating material acts both as a second wire in circuit and as a shield for the inner conductor, as shown in Figure 1-13. It can help reduce any outside interference.

Coaxial cable comes in different sizes. Because of its transmission length and noise-rejection characteristics, the diameter is specified to be 1 cm. This type of coaxial cable is referred to as *thicknet*. Thicknet cable is easy to install in some situations because of its thickness. This cable is used for special-purpose installations. A vampire tap is a device used to connect network devices to thicknet. The vampire tap is then connected to computers via a flexible cable, called the attachment unit interface (AUI).

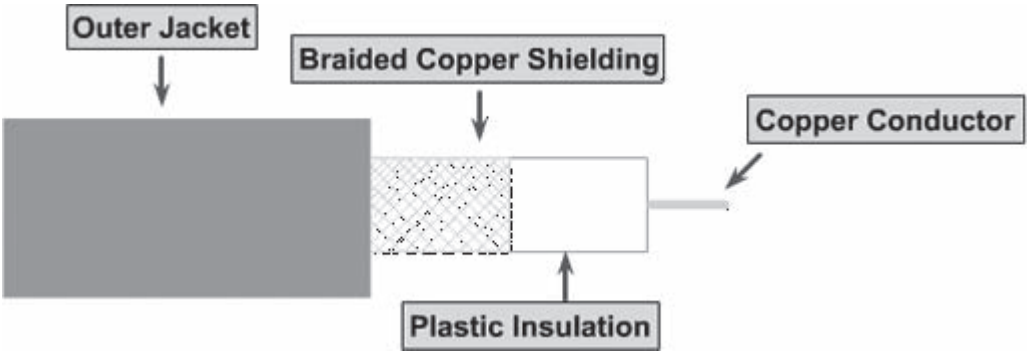


Figure 1-13 Coaxial cable uses plastic insulation over a single copper conductor.

Figure 1-14 BNC T-connectors are used to connect coaxial cables.

Coaxial cables with an outer diameter of 0.35 cm were used in Ethernet networks. Such cables were used especially when they had to be twisted and turned. These are referred to as *thinnet cables*.

A common connector used with thinnet is BNC (Bayonet Neill-Concelman). It is a male connector mounted at each end of the cable. A BNC connector has a center pin connected to the center cable conductor and a metal tube connected to the outer cable shield. The outside rotating ring locks the cable to any female connector. BNC T-connectors are female devices for connecting two cables to network interface cards (NICs), as shown in Figure 1-14.

The following are features of coaxial cable:

- *Speed and throughput*: 10 to 100 Mbps
- *Average cost per node*: Inexpensive
- *Media and connector size*: Medium
- *Maximum cable length*: 500 m (medium)

Fiber-Optic Cable

Fiber-optics is a technology that uses glass (or plastic) threads (fiber) to transmit data. It consists of bundles of glass threads, each of which is capable of transmitting messages modulated onto light waves. It is used for networking and consists of two fibers encased in separate sheaths. An outer jacket and many layers of protective buffer material, typically a plastic shield and reinforcing material made of a material such as Kevlar, cover each optical fiber. While the plastic meets fire codes, the outer jacket will protect the entire

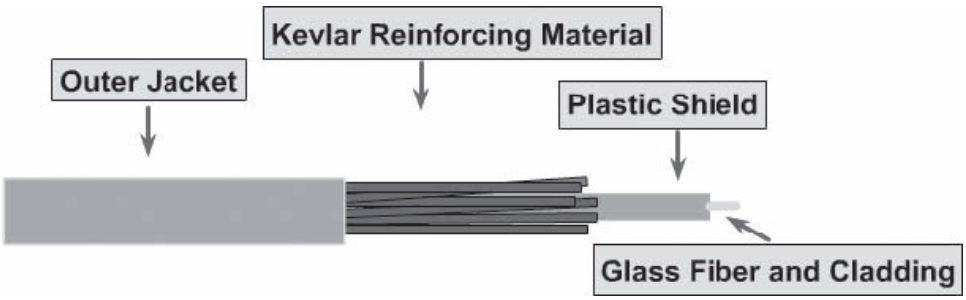


Figure 1-15 Fiber-optic cable uses a glass fiber to transfer data.

cable. The Kevlar furnishes additional cushioning and protection for the fragile, hair-thin glass fibers, as shown in Figure 1-15.

The light guiding of optical fiber parts is called the core and the cladding. The core is very pure glass with a high index of refraction. When a cladding layer of glass or plastic with a low index of refraction covers the core glass, light can be trapped in the core glass. This process is called total internal reflection. Fiber-optic media is more expensive than all other network media.

There are two types of fiber-optic cable:

1. Single-mode
2. Multimode

Single-Mode Single-mode cable allows only one mode (or wavelength) of light to propagate through the fiber. It is capable of higher bandwidth and greater distance than multimode. Single-mode is used for campus backbones. These types of fibers use lasers as a light-generating method. The maximum length of single-mode cable is 10 km (32,808.4 feet).

Multimode Multimode cable allows multiple modes of light to propagate through the fiber. It is also used for workgroup applications and intrabuilding applications, such as raisers. It uses light-emitting diodes (LEDs) as a light generating device. Multimode cable's maximum length is 2 km (6,561.7 feet).

The difference between single-mode and multimode connectors is the precision in the manufacturing process. A single-mode connector hole is smaller than a multimode connector hole. This ensures tighter tolerance in the connector assembly.

There are two types of fiber-optic connectors commonly used in the communications industry:

- *SC*: These types of connectors feature a push-pull connect and disconnect method. The connector is simply pushed into the receptacle to make a connection. Simply pull out the connector to disconnect.
- *ST*: This connector is a bayonet type of connector. The connector is fully inserted into the receptacle and is then twisted in a clockwise direction to lock it into place, as shown in Figure 1-16.

Plenum Cables

A plenum cable is a cable that runs into the plenum space of a building. As ordinary cables cannot withstand threats such as fire, these cables are built into the plenum area of the building. The outer material of a plenum cable is more resistant to flame, produces less smoke, and does not emit the toxic fumes other cables do when burning.

PVC Cables

Polyvinyl chloride (PVC) cables are the most commonly used electrical insulation material. They are primarily dominant in low-voltage applications. Telecommunication is also an important application for PVC. PVC cable includes the following features:

- It provides good electrical and insulation properties over a wide temperature range and provides safety from fire.
- It has excellent durability and long life expectancy.
- It is highly resistant to degradation from ultraviolet lights.

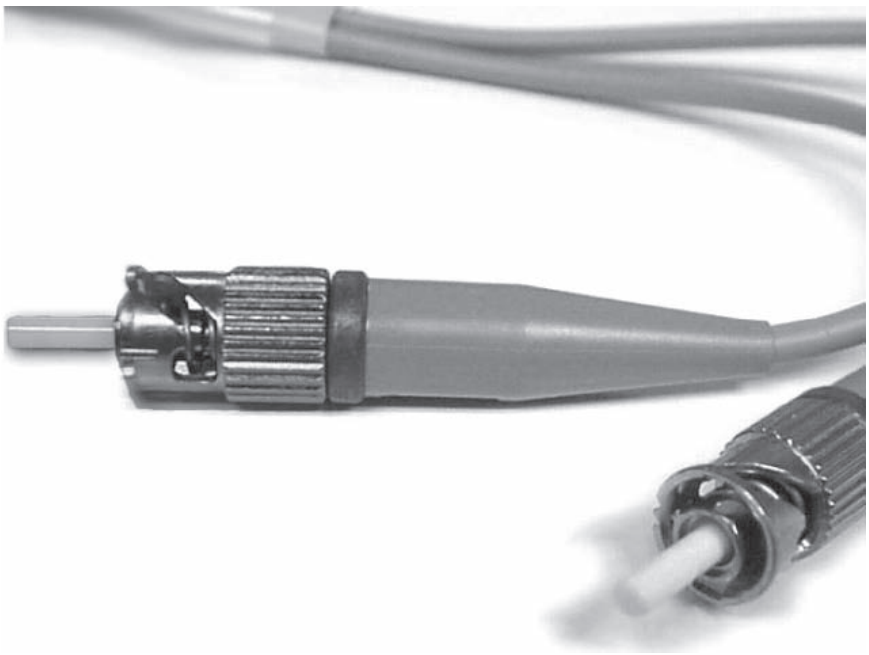


Figure 1-16 The ST fiber-optic connector is used to connect fiber-optic cable.

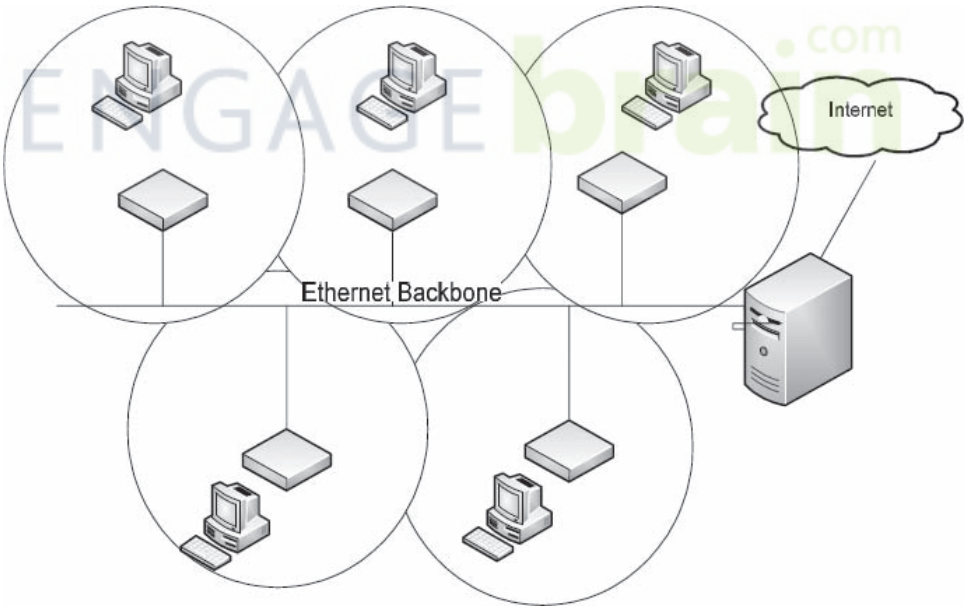


Figure 1-17 Wireless transmission utilizes an Ethernet backbone.

Wireless Transmission

Wireless transmission uses radio frequency (RF) and infrared (IR) waves to transmit data between the devices on a LAN. Components of a wireless network include antennas, amplifiers, and access points (APs), as shown in Figure 1-17.

The user must install a wireless adapter card (wireless NIC) on a PC/laptop in order to send and receive wireless signals. Wireless signals use portions of the RF spectrum to transmit voice, video, and data. Wireless frequencies range from 3 kHz to 300 GHz. The rate of data transmission ranges from 9 kbps to as high as 54 Mbps.

WLAN

A wireless LAN (WLAN) is made in accordance with Institute of Electrical and Electronics Engineers (IEEE) 802.11 standards. It uses radio waves (e.g., 902 MHz), microwaves (e.g., 2.4 GHz), and IR waves (e.g., 820 nm) for communication.

The following are some of the different types of wireless transmission:

- Infrared
- Microwave
- Satellite

Infrared Transmission The infrared transmission system is composed of three components: the transmitter, the infrared emitter (also called the radiator), and the receiver. The transmitter modulates the data signals onto a carrier frequency by using frequency modulation or digital techniques. The emitter converts this modulated signal into infrared light. The receiver decodes the infrared signal and converts it to a data signal.

The transmitter generates carrier waves for each channel in a multichannel system. All modulated carrier waves are mixed and sent via a coaxial cable from the transmitter to the infrared emitter.

Microwave Transmission Microwave transmission is a technique for transmitting information over a microwave link. It is used to transmit audio, video, and data using microwaves over distances ranging between a few feet to several miles. Microwave transmission is likely to be subject to attenuation caused by atmospheric conditions, especially at times of wet weather.

Satellite Transmission Satellite transmission offers consistently high transmission quality. It is extremely reliable, and it is used to receive virtually error-free digital transmission across the network. Satellite transmission is commonly used for television broadcasting, weather forecasting, radio communication, and Internet communications.

Line of Sight

Line of sight is one of the problems affecting wireless transmission. The path between the two antennas in wireless communication should be straight. Therefore, line of sight (LOS) is an unobstructed path between the sending and receiving antennas. LOS is easy to achieve for small distances, but difficult for large distances.

The Fresnel zone (an elliptical area immediately surrounding the visual path) is also taken into consideration. Fresnel zone clearance must be considered when determining the height of antennas.

To determine the line of site, the following two items must be identified:

1. Geographical change
2. Height of the antennas

Radio Frequency (Bandwidth)

A radio wave is an electromagnetic wave propagated by an antenna. These radio waves have different frequencies, which can be changed by tuning the radio receiver to a specific frequency (Figure 1-18).

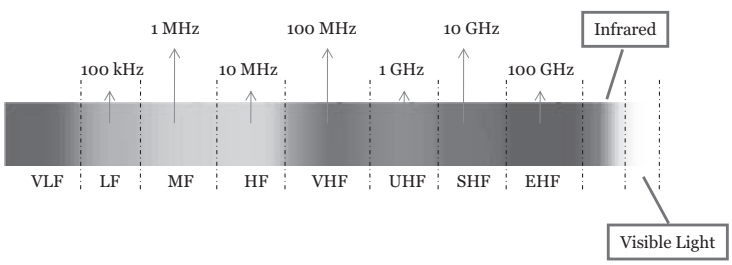


Figure 1-18 Radio waves are on the same spectrum as visible light.

Bandwidth Description	Frequency Range
Very low frequency (VLF)	3 KHz to 30 KHz
Low frequency (LF)	30 KHz to 300 KHz
Medium frequency (MF)	300 KHz to 3000 KHz
High frequency (HF)	3 MHz to 30 MHz
Very high frequency (VHF)	30 MHz to 300 MHz
Ultrafigh frequency (UHF)	300 MHz to 3000 MHz
Superhigh frequency (SHF)	3 GHz to 30 GHz

Table 1-2 This table illustrates the frequency ranges of various bandwidths

The Federal Communications Commission (FCC) determines the purpose of a particular frequency spectrum. In order to transmit on a particular frequency, a person has to obtain a license from the FCC; the fixed frequency will be reserved for the licensed person only. Table 1-2 lists the frequency ranges of certain bandwidths.

Public Switched Network

A public switched network (PSN) is a common carrier network that provides circuit switching for the general public. PSNs are usually telephone networks; they could also be data and packet-switched networks.

PSNs provide traffic routing from local users or from other switching centers, whereby a connection is established between the calling and called stations. The connection is released only when either the called or calling party hangs up. A PSN can be also defined as a network that can be accessed by the public for establishing and terminating telecommunications messages.

Emanations Security

Unwanted emanations result from computer technologies used for storing, calculating, and communicating data. These compromising emanations consist of electrical, mechanical, or acoustical energy intentionally or unintentionally emitted by any number of sources within equipment and systems that process information from information-handling devices. If unauthorized individuals utilize this information it could give way to a serious security breach. Emanation security involves taking measures designed to restrict unauthorized persons from obtaining that information.

The term TEMPEST is broadly used for the entire field of emanations security. The term was coined in the 1970s as a codename for a National Security Agency operation to secure electronic communications equipment from potential eavesdropping by unauthorized individuals.

Media Access Methods

Media access methods determine whether or not a particular node can place data on the network. They can be put into two categories: connection based or competitive media access. Nodes themselves determine media access time.

Token Ring

Token Ring was developed by IBM and designed for a consistent network architecture based on the token-passing access control method. It is incorporated into IBM mainframe systems, such as the AS/400, and could possibly be used with PCs, minicomputers, and mainframes. It performs well with Systems Network Architecture (SNA) to connect with mainframe networks.

FDDI (Fiber Distributed Data Interface)

FDDI is a type of Token Ring network. Its implementation and topology is different from IBM's Token Ring LAN architecture, which is managed by IEEE 802.5. FDDI is also used for metropolitan area networks (MANs) or larger LANs that extend between several buildings in an office complex or campus.

LocalTalk

LocalTalk was developed by Apple Computer, Inc. and is suitable for small networks of Macs. It permits linear bus, star, or tree topologies to use twisted-pair cable. It allows up to 32 devices (computers, printers, and file servers). It transmits data at only 230 Kbps. LocalTalk uses the CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) process for transmitting data.

Multiplexing

Time-Division Multiplexing (TDM)

TDM is a technique of placing multiple data streams in a single signal by dividing the signal into several segments, each with a short period. This data stream is reassembled at the receiving side, depending on the timing.

The circuit that merges signals at the transmitting end of a communication link is called a multiplexer. It takes the input from each user, divides each signal into several segments, and then allocates the segments to the combined signal in a rotating and repeating sequence. The composite signal then contains data from several senders. At the other end of the cable, individual signals are divided out by a circuit called a demultiplexer and routed to the proper users. Two-way communication circuits need a multiplexer/demultiplexer at every end of the long-distance, high-bandwidth cable.

Frequency-Division Multiplexing (FDM)

FDM is a method by which multiple signals are merged for transmission over a single communication line or channel. Each signal is allocated a separate frequency within the main channel.

An analog Internet connection on a twisted-pair cable needs 3 kHz of bandwidth for reliable data transfer. Twisted-pair cables are common in households and small businesses. But large telephone cables, which operate between large businesses such as government agencies and municipalities, are able to carry larger bandwidths.

If a long-distance cable has a bandwidth of 3 MHz, it means this is 3,000 kHz. Thus, it is possible to put 1,000 signals into a long-distance channel, each with a size of 3 kHz. The circuit that does this is known as a multiplexer. It takes the input from each end user and creates a signal on a different frequency for each of the inputs. This results in a high-bandwidth, complex signal that includes data from all of the end users. At the other end of the cable, the individual signals are divided by the demultiplexer and routed to the proper end users.

Polling

Polling is a method by which a central device contacts each node to see whether it has data to transmit. In the polling method, every node has guaranteed access to media, but network time can be wasted if polled nodes do not contain data.

Demand Priority

Demand priority is a polling method by which nodes will send their state to a hub as either ready to transmit or idle. The poll state of each node grants permission to transmit. A node can also tell the hub the priority of data that passes through it. The hub will favor high-priority transmission requests.

Token-Based Media Access Method

This is a media access method by which computers pass a special sequence of bits, called a token, between them. Only the node holding the token can transmit on the network. After transmitting data, or if it does not contain data, a node passes the token to the next computer on the network.

Advantages and Disadvantages

This method is said to be deterministic because every node has guaranteed access to the media. This is best for networks in which timing is critical. In addition, even when traffic is very high, every station has the same chance to transmit its data. However, token passing is ineffective when traffic is low because a station has to wait when other nodes hold the token and pass it on without transmitting data. Also, each node needs complex software to control the token-passing process and may need reconfiguring whenever a node is added to or removed from the network.

Carrier Sense Multiple Access/Collision Detection (CSMA/CD)

This is a contention-based media access method by which nodes can transmit whenever they have data to transmit. CSMA/CD must detect and manage expected collisions that take place when multiple nodes transmit at once.

In CSMA/CD:

1. A node has data to transmit.
2. The node determines whether the media is available or not.
3. If media is available, then the node transmits its data.
4. The node determines if a collision has occurred by detecting the fragmented data that results from the collision.
5. If there is a collision, the node waits for a random back-off time that is calculated in milliseconds, and then repeats the process until successful.

Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA)

CSMA/CA is a contention-based media access method by which nodes can transmit whenever they have data to transmit. However, they take the following steps before they transmit to ensure that the media is not in use:

1. A node has data to transmit.
2. The node determines whether the media are available or not.
3. If media are available, the node sends a jam signal to advertise its intent to transmit data.
4. The node waits until all nodes have time to receive the jammed signal.
5. The node then transmits its data.
6. When transmitting data, the node monitors the media for a jammed signal from another node. If a jammed signal is received, it stops transmitting the data and retries after a random delay.

Contention Domains

A contention, or collision, domain consists of nodes whose simultaneous transmission may interfere with that of another node. All devices in a contention domain compete for the right to transmit data. Any device in this domain transmits data if there is no other traffic on the media.

Automated Information Systems (AISs)

Automated Information Systems (AISs) are a combination of computer hardware, software, and firmware. AIS is specifically developed for critical information handling and protection. It is useful in processes such as communication, computation, dissemination, processing, and storage of information.

AIS is used in the following ways:

- *Management issues*: As more and more operations are dependent on computers, it has become important for a computer to fully manage all tasks. The need of management to handle critical issues creates the need for AIS.
- *Value of information and computing resources*: Processes such as communication and computation assure ready availability and high integrity, whereas confidentiality is a critical issue handled by AIS.

Historical Versus Current Technology

Hardware

Hardware is a general term used to refer to the physical components of a computer system. This includes keyboards, circuit boards, monitors, graphics cards, and mice.

Distributed Versus Standalone

Hardware that is offering its services to the whole system/organization is referred to as distributed hardware. It provides reliability, sharing of resources, and scalability. However, it lacks in its ability to provide security.

Hardware that restricts its services to a single computer is called standalone hardware. It offers security but provides limited benefits.

Microprocessors, Miniprocessors, and Mainframe Processors

Microprocessors

A microprocessor is a small and integrated version of a CPU (central processing unit). It combines the functions performed by the CPU into a small integrated circuit (IC). Previously, CPUs were so large that they were difficult to handle and consumed a large amount of space. The small size of the microprocessor makes it compact enough to fit in a small cabinet.

Microcomputers are differentiated on the basis of the following characteristics:

- *Instruction set*: The set of instructions that the microprocessor can execute.
- *Bandwidth*: The number of bits processed in a single instruction.
- *Clock speed*: The clock speed of the microprocessor determines how many instructions the processor can execute in one second. It is calculated in megahertz (MHz).

Miniprocessors

A miniprocessor is a low-cost logic circuit that uses integrated circuits (ICs). It has started a revolution in the computer field, as it is easy to handle and can be used to perform calculations in the engineering and science fields. It is very useful for scientific research and operations.

Mainframe Processors

Mainframe processors are large and expensive processors. The main advantage of this kind of processor is that it can handle complex calculations. It is useful for handling hundreds, or even thousands, of users simultaneously and can be placed just below supercomputers in power.

Components

Input and Output

Communication between the machine and user is possible when the machine sends output to a device based on the input the user provides. Basically, input is the signal or data received by the system, while output is the relevant signal or data sent from the system. Some devices are used to perform both operations. Modems and network cards fall under this category.

Central Processing Unit (CPU)

A central processing unit (CPU) is a device that carries out logical functioning and executes computer programs. Since their invention, CPUs have gone through logical and physical evolutionary changes. The CPU is now very compact and efficient. Today, the CPU is used in many applications for fast and appropriate functioning of appliances.

Memory

Memory is the capacity to store, retain, and subsequently retrieve information. It is the internal storage device in the computer where all data being used and currently running processes is stored.

There are several different types of memory:

- *RAM (random-access memory)*: It is possible to read stored data from, as well as write data to, RAM. However, this memory is volatile and requires a continuous power supply. Once the power supply is switched off, data stored in RAM is lost. Thus, it is also known as volatile memory.
- *ROM (read-only memory)*: This type of memory is present in almost all types of computers. ROM is typically used to hold the instructions to start the computer. Unlike RAM, ROM cannot be written to. It is only meant for reading instructions.
- *PROM (programmable read-only memory)*: PROM is a chip on which a program can be stored. It is permanent and cannot be wiped out. Once used, memory cannot be used for saving other data. Like ROM, PROM is nonvolatile.

- *EPROM (erasable programmable read-only memory)*: This is a special type of PROM that can be erased by exposing it to ultraviolet light.
- *EEPROM (electrically erasable programmable read-only memory)*: EEPROM is a special type of PROM that can be erased by exposing it to an electrical charge.

Sequential In a computer, sequential-access memory (SAM) is a data storage device that reads data in a sequence. It is completely different than RAM, where the data is accessed in any order. Though sequential memory is read sequentially, a certain location can be accessed by seeking that location.

Random This memory type is different than sequential memory. Random memory allows a user to access stored data in any order. It refers to the fact that any piece of data can be returned in a constant time. Accessing the memory does not depend on the physical location and previous data.

Volatile Versus Nonvolatile Volatile memory, also known as a primary storage device, is a memory type that requires a constant power supply to maintain the stored information. Most random-access memory is volatile storage, including dynamic random-access memory and static random-access memory.

Nonvolatile memory, then, is the opposite of volatile memory. It is not affected by a disrupted power supply. It stores and retains information even when there is no power. Nonvolatile memory includes ROM, flash memory, hard disks, floppy disk drives, and magnetic tapes.

Nonvolatile memory is mainly used for the purposes of secondary storage or for the long-term storage of data. Nonvolatile memory is more costly and performs worse than volatile random-access memory.

Critical Information Characteristics

Information systems security is concerned with three characteristics of information: confidentiality, integrity, and availability.

Confidentiality

Confidentiality is critical for the security of an information system. A security policy is a set of rules that determines whether to permit or deny access to a particular object. Confidentiality is the assurance of access granted only to the authorized party, process, or object.

All organizations require protecting certain information. It is also important to differentiate between important and less important data, which will help in deciding what data requires protection from others.

Integrity

Integrity focuses on the fact that though confidentiality focuses on data security, there is a need for an individual who is authorized to modify the data. Integrity also includes accuracy, relevancy, and completeness. Integrity also focuses on the quality of information and the assurance that the data has not been corrupted or changed.

Availability

Availability is also included and is as important as confidentiality and integrity. Security mainly focuses on ensuring that information is provided to authorized users whenever required and asked. Information systems security has become a science of the study of compromises, as security and utility often conflict.

Information States

Transmission

Transmission is the act of sending information from one system to another. This transmitting of information is only possible when the computer is using a data transmission protocol.

Storage

Storage is the process of saving and retrieving information that can be reproduced when the stored information is needed.

Storage Devices

The devices that store data or information are known as storage devices. Few storage devices have the ability to process the information stored in them. Storage devices store data either in analog or digital form.

Processing

The act of analyzing data and transforming raw data into useful information is called processing. A computer usually automates processing.

Operations Security (OPSEC)

Operations security (OPSEC) identifies, controls, and protects classified or sensitive information. While classified information comprises only a small part of the information and activities processed by organizations every day, its security is critical. If classified information becomes known to a competitor or adversary, it could become a problem.

OPSEC is the process that allows a manager to look for possible security breaches in a system. Hence, it provides all possible ways by which adversary elements can intrude and misuse an organization's sensitive information. It basically focuses on finding and correcting ways for compromising the information. It is used by government agencies and contractors in the development and acquisition of new equipment and in intelligence collection.

OPSEC Process

The OPSEC process involves the following:

- *Identifying critical information*: OPSEC focuses on information that needs to be protected. This may be a stream of information or a complete process.
- *Analyzing the threat*: This will help determine the ways that a possible adversary could intrude and steal information.
- *Identifying vulnerabilities*: Focusing on vulnerabilities is a way to determine which information an adversary could use against an organization. It helps to observe what data the adversary would be interested in and how he or she would be able to obtain it.
- *Analyzing risk*: Risk analysis allows the manager of an organization to determine the hazards caused by loss of information. In risk evaluation, vulnerabilities are weighed against the cost of the loss of data.
- *Countermeasures*: Finally, managers have deployable solutions to reduce risks by eliminating vulnerabilities. Another way to do this is to disrupt the effective collection of information, in which all important information is not stored in the same place and is mixed with other information to mislead the intruder. The factors that determine the use of countermeasures are cost, timing, feasibility, and the imagination of the person involved.

INFOSEC and OPSEC Interdependency

Previously, INFOSEC (information security) and OPSEC were considered to be two separate compartments of the information security system of the organization. It is now clear, however, that both of these are interdependent and can be handled simultaneously. Today, information-dependent organizations need risk management to be dealt with through INFOSEC and OPSEC simultaneously. Recently, legislation and regulations such as Basel II (for banks), the Turnbull report (for the London Stock Exchange), and the Sarbanes-Oxley Act (for the New York Stock Exchange) say that if an organization does not have adequate mechanisms in place for controlling and auditing its flow of information, then the organization could lose a great deal of money.

Information security specialists are familiar with network threats and vulnerabilities. Figure 1-19 shows five levels of information security from operational security to strategic planning.

Unclassified Indicators

Unclassified indicators can be used to reveal critical information that requires OPSEC measures for additional protection. OPSEC mainly focuses on removing, minimizing, or covering the unclassified indicators that can compromise classified information, especially critical information. While programs like information security protect classified information, they cannot prevent all indicators of critical information, especially unclassified indicators, from being revealed.

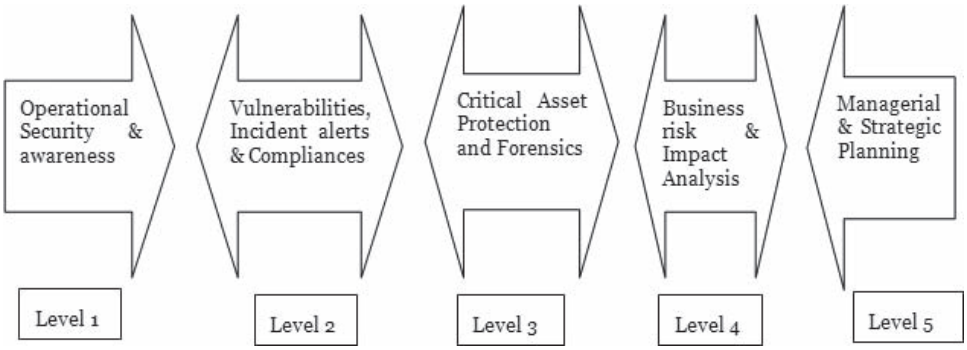


Figure 1-19 These are the five levels of information security.

OPSEC Surveys/OPSEC Planning

An OPSEC survey is a method for examining the sufficient protection of critical information during the planning, preparation, execution, and postexecution phases of any operation or activity. This survey will analyze all associated functions to identify sources of information, what they disclose, and what can be derived from the information.

An OPSEC survey is a time-intensive method, so it should only be conducted when necessary. Extremely sensitive programs, activities, or operations where the slightest compromise will result in mission failure and/or extreme damage to national security are rare examples where an OPSEC survey may be conducted.

Object Reuse

Object reuse focuses on the allocation or reallocation of storage objects. It is mandatory for security to avoid using a system resource that can be used to pass data from one process to another. This can be considered a violation of security policy. Objects normally use resources like buffers and caches. An operating system like UnixWare clears buffers and caches before assigning them to other processes. This ensures that no process inherits or reads the data of other processes, either intentionally or unintentionally. However, the controlled sharing of memory is a difficult task, as it allocates and reallocates the memory to different processes. UnixWare allows many processes to execute simultaneously in memory. This includes the allocation of memory to a process and again deallocating it, allowing the memory to be reallocated to another process. This reallocation may be a threat to security, as information may remain when a section of memory is reassigned to a new process.

Understanding the OSI Reference Model

In the early years of networking, communication between two different computers and different applications was difficult, as they adhered to different communication standards. Later, different standards bodies, users, and providers agreed upon a similar architecture for communication irrespective of the applications and operating systems that were being used.

The Open System Interconnection (OSI) model's protocol function is divided into separate layers, as shown in Figure 1-20. Each layer has specific functions. The design of the OSI model is based on the following principles:

- Each layer should have a fully defined function
- The boundaries of the layers are selected to reduce the flow of information in the interface
- When an additional level of abstraction is required, a layer is created
- Each layer contains the functions of the international standardized protocols

A type of system that implements the protocol behavior and consists of these layers is called a protocol stack. The OSI model contains the following layers:

- *Layer 1*: Physical layer
- *Layer 2*: Data-link layer

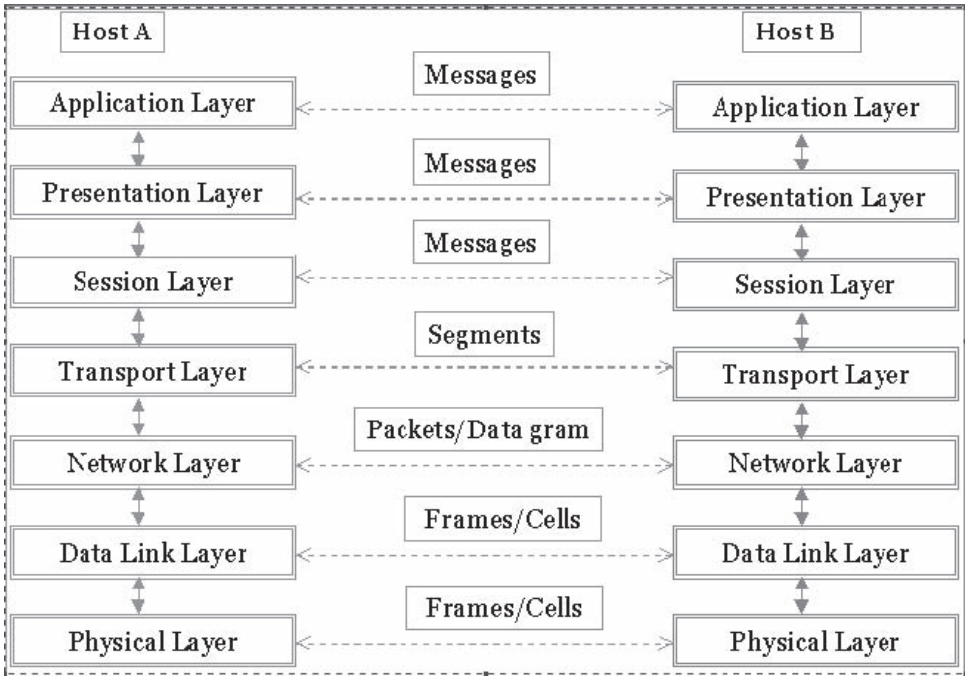


Figure 1-20 The OSI model is the standard networking model.

- *Layer 3*: Network layer
- *Layer 4*: Transport layer
- *Layer 5*: Session layer
- *Layer 6*: Presentation layer
- *Layer 7*: Application layer

Physical Layer

The physical layer manages the operations needed to send a stream of data over a physical medium, as shown in Figure 1-21. It deals with mechanical and electrical requirements. It also describes the methodologies and functionalities of the physical devices and interfaces to achieve the communication required.

The following are the responsibilities of the physical layer:

- *Features of the interfaces and media*: The physical layer defines the features of the interfaces between the devices and the communication media.
- *Depiction of data*: The data is depicted in the form of 0's and 1's without any encryption when passed through the physical layer. The data is encoded into signals that may be electrical signals or light signals.
- *Organization of data bits*: The sender and receiver must have their data organized at the bit-stream level.
- *Configuration of links*: The physical layer deals with the links of the devices to the medium. In a point-to-point connection, the devices are attached through a single link. In a multipoint design, a link is divided among many devices.
- *Topology of devices*: The topology deals with the position of devices through which they form a network. The devices can be connected in the network using mesh, star, ring, and bus topologies.
- *Mode of communication*: The physical layer also describes the mode of transmission between two devices. The available modes are simplex, full-duplex, and half-duplex types.

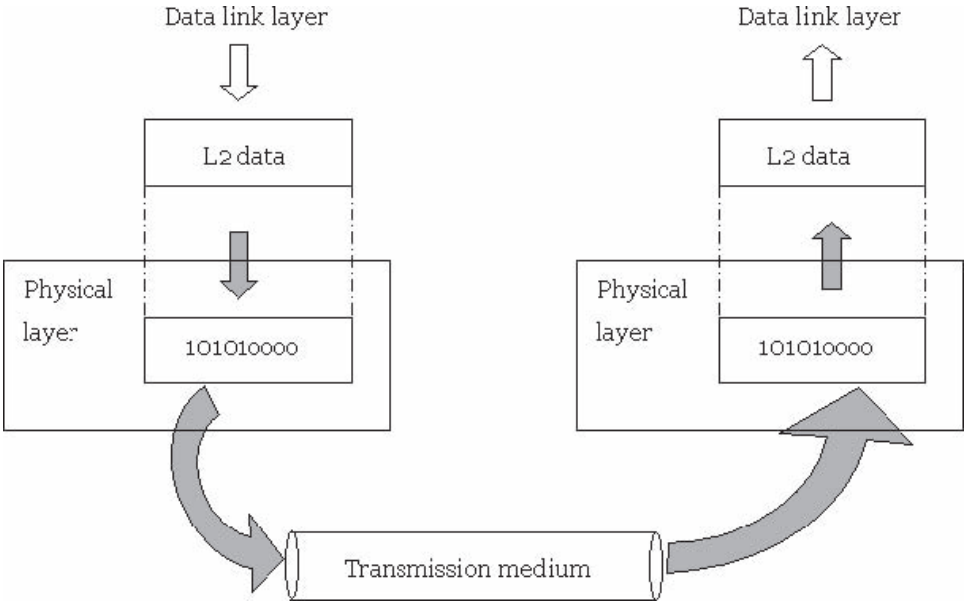


Figure 1-21 The data transmission path moves through the physical layer.

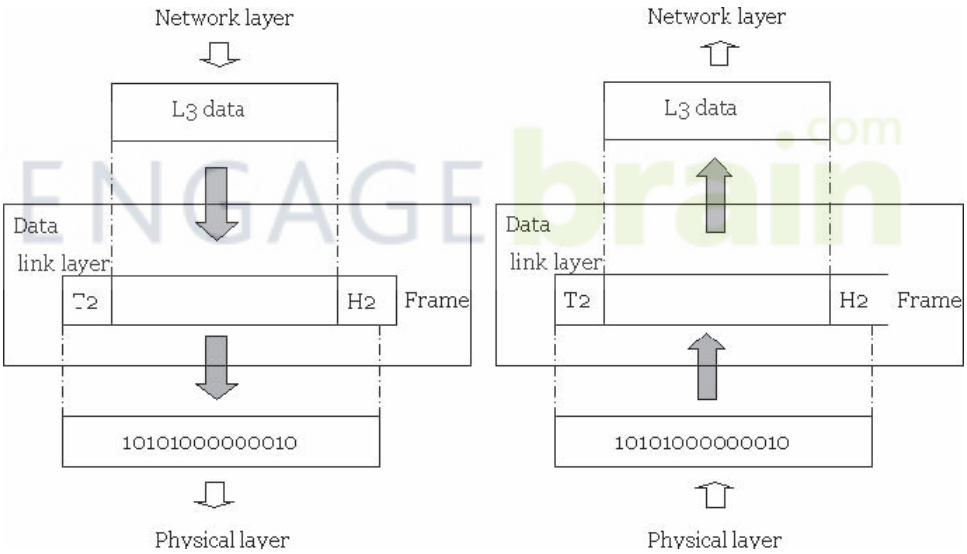


Figure 1-22 The data-link layer makes the physical layer secure.

Data-Link Layer

The data-link layer is responsible for device-to-device delivery. The objective of the data-link layer is to make the physical layer secure without any errors, as shown in Figure 1-22.

The following are the responsibilities of the data-link layer:

- *Grouping*: The data-link layer groups the bits of information received from the network layer into data packets, called frames.
- *Addressing*: The data-link layer adds a header to the packet to describe the original address of the sender or the receiver.

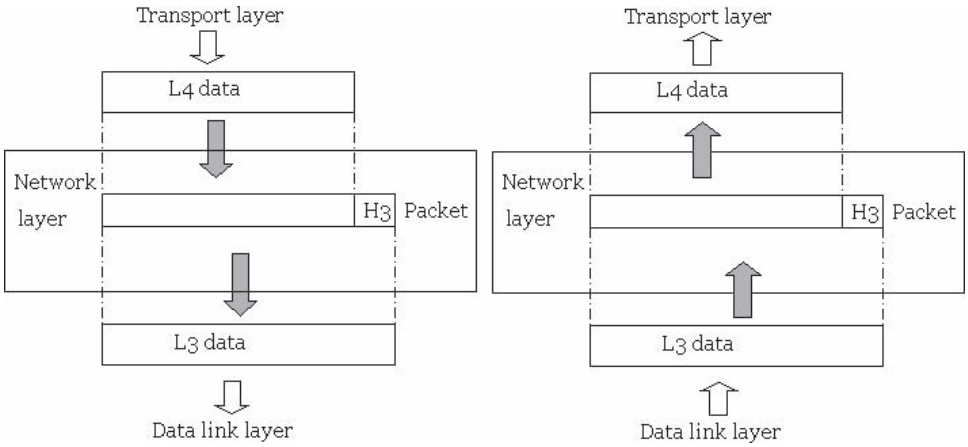


Figure 1-23 The network layer makes sure that packets are routed correctly.

- *Flow control*: Data taken by the receiver is received at a rate that is less than the rate generated by the sender. The data-link layer employs the flow-control mechanism to reduce data flooding at the receiver's end.
- *Access control*: When multiple devices share the same connection, the data-link layer employs certain protocols that are essential to determine the devices that have authority over other devices.

Network Layer

The network layer is useful for source-destination transmission of packets across multiple networks. The network layer makes sure that individual packets initiated from the source reach the destination, as shown in Figure 1-23.

The following are the responsibilities of the network layer:

- *Global addressing*: Global addressing is executed through the data-link layer, which deals with the addressing problem locally. If the packet passes the network border, another addressing system is essential to separate the source and destination systems. The network layer supplies a header to the packet that originates from the upper layers and includes the global address of the sender and receiver.
- *Routing of data packets*: The network layer is linked together to create an internetwork, which is a huge network, through which the linking devices route the packets to the final destination.
- *Fault handling*: The network layer is useful for fault control from source to destination. The sending network layer ensures that the whole message arrives at the receiving device without any errors.
- *Traffic control*: The network layer is useful for controlling the flow of traffic from source to destination so that the end user is not overwhelmed.

Transport Layer

The transport layer is useful for sending packets from the source to the destination. The transport layer makes sure that the entire message is transmitted without any deletions or modifications by helping in fault control and transmission control. For security enhancement, the transport layer can maintain a connection between the end points, as shown in Figure 1-24.

The following are the responsibilities of the transport layer:

- *Addressing*: The transport layer's packet has a header that is useful for holding the address of the service point address. The network layer transmits the exact packet to the transport layer and makes the whole message arrive at the exact process on that device; the transport layer gets the whole message to the exact process on the computer.

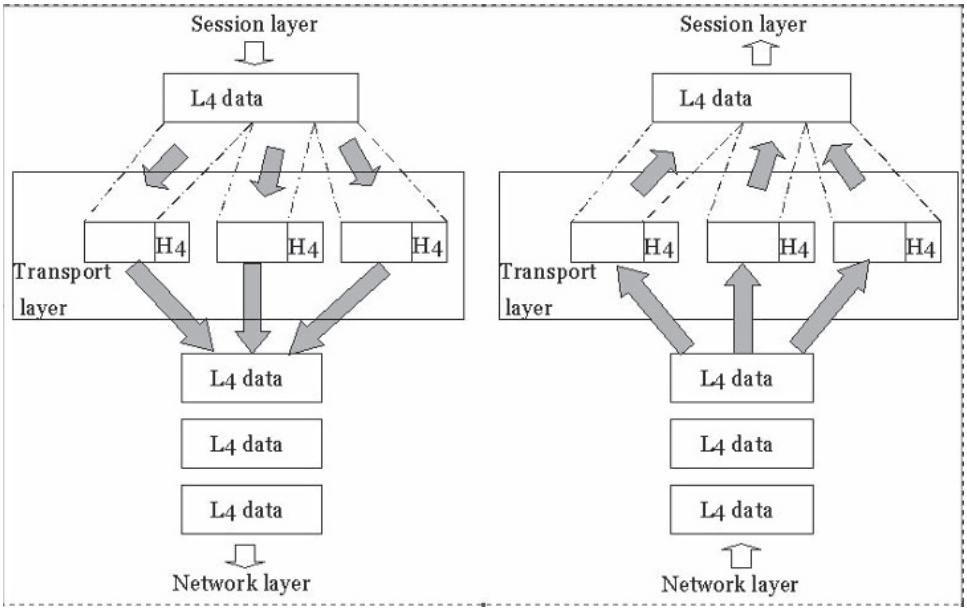


Figure 1-24 The transport layer ensures the correct transmission of data.

- *Isolation and reconstruction*: A message is broken into many segments for transmission, and each segment holds a sequence number. These numbers permit the transport layer to reconstruct the message appropriately at the destination and to recognize and replace packets that are lost during communication.
- *Link control*: The protocols are either connectionless or connection oriented. A connectionless transport layer considers each segment as an individual packet and sends it to the transport layer at the destination. A connection-oriented transport layer initially establishes a connection with the transport layer at the end machine before sending any packets.
- *Transmission control*: Fault control is performed from destination to destination through a single link. The sending transport layer ensures that the whole message arrives at the receiving device without any errors.
- *Error control*: The transport layer is useful for fault control from source to destination.

Session Layer

The session layer monitors the communication between two devices, as shown in Figure 1-25. The following are the responsibilities of the session layer:

- *Communication control*: The session layer permits two devices to establish a dialog between them. It permits communication between the devices to take place in full-duplex or half-duplex form.
- *Data organization*: The session layer permits the process to employ checkpoints. If a system is sending a file of 1,000 pages, checkpoints are inserted after every 100 pages to make sure that each 100-page unit is received. An acknowledgment for each unit is sent individually.

The advantage of the checkpoint system is that if a failure occurs, the entire file does not have to be retransmitted.

Presentation Layer

The presentation layer deals with the syntax and semantics of the data interchanged between two devices, as shown in Figure 1-26.

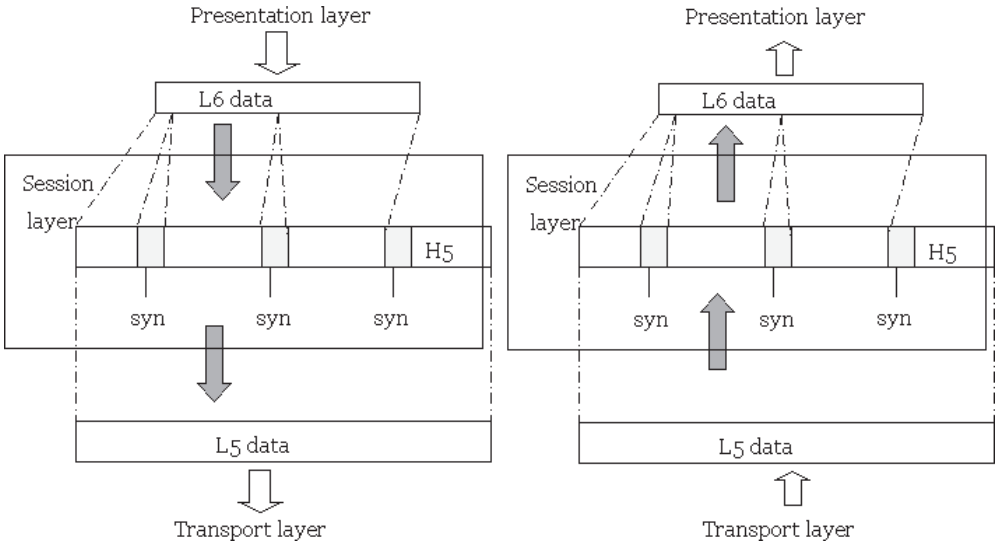


Figure 1-25 The session layer monitors the communication between two devices.

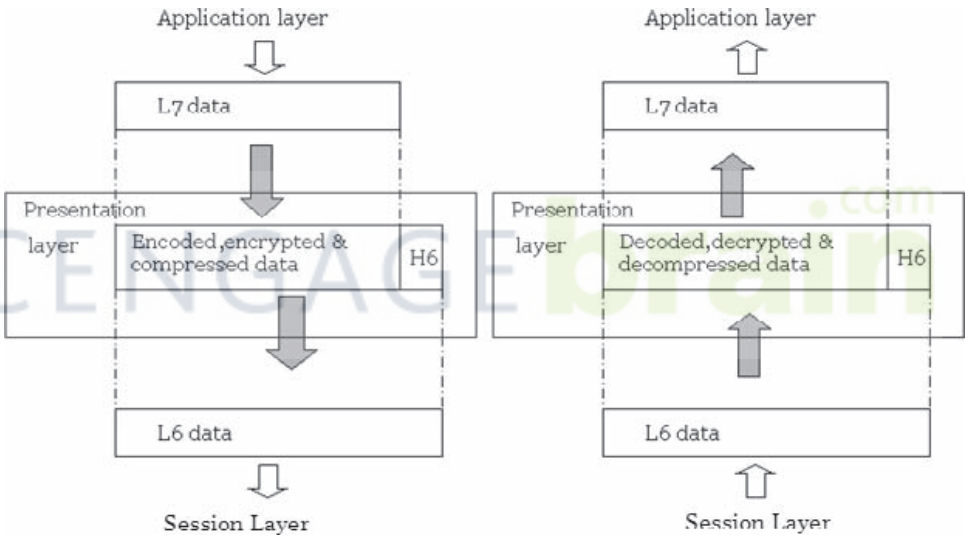


Figure 1-26 The presentation layer deals with the syntax and semantics of the data interchanged between two devices.

The following are the responsibilities of the presentation layer:

- *Translation*: Information must be converted into streams of data before it is sent. As different computers have different encoding systems, the presentation layer deals with the interchange between the various systems of encoding. The data are translated into a common format that the presentation layer at the receiving end will be able to understand. The format of the received data is dependent on the receiver's format.
- *Encryption*: To transmit confidential information, the system must be able to provide security. In encryption, the sender of the data changes the exact information into another format and broadcasts the resultant information.
- *Compression*: The compression of data reduces the number of bits sent. Data compression becomes significant in the transmission of information such as images, sound, and video.

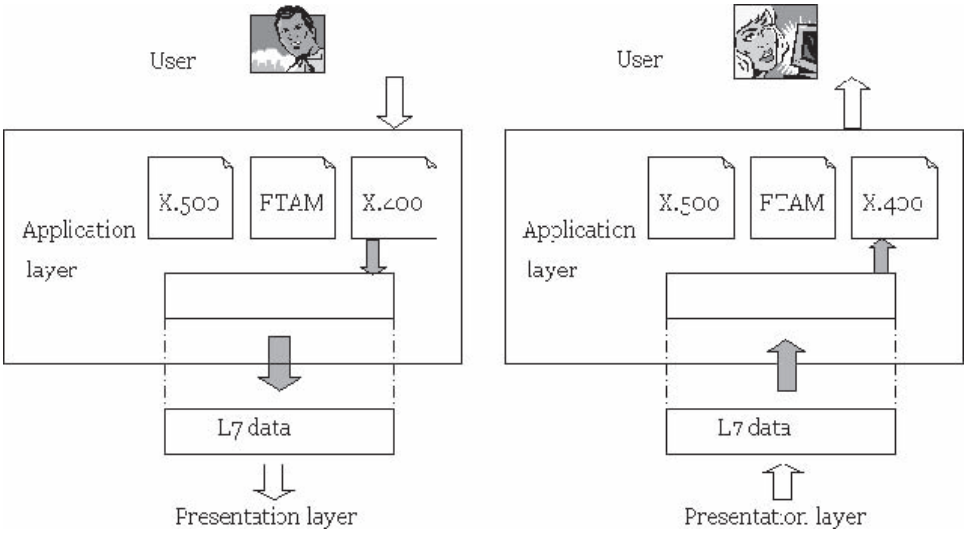


Figure 1-27 The application layer provides users with access to any network.

Application Layer

The application layer provides users with access to any network, as shown in Figure 1-27. It provides services such as interface and help services for e-mail distant file access. It also provides database management for shared systems and many other kinds of distributed systems.

The application layer provides many services, such as the following:

- *Network virtual terminal*: A network virtual terminal is a software system representing a terminal. It permits users to access remote systems. To achieve this, the application generates a software model of a terminal at the remote host. The user's terminal communicates with the software terminal, which again communicates with the original terminal that allows the users to log on to the system.
- *File transfer, file management, and file access*: The application layer permits a user to access files in distant places to get the files from remote computers and to administer the files in an isolated computer.
- *Directory services*: The application layer provides distributed database facilities and access for retrieving the information worldwide.
- *Mail services*: This application provides the foundation of e-mail sending and the storage of e-mail received.

Data Transmission Methods

Data Transmission Modes

A transmission mode is the term used to define the direction of a signal or the flow between two linked devices.

Data transmission modes include:

- Simplex transmission
- Half-duplex transmission
- Full-duplex transmission

Simplex Transmission

This is a type of data transmission in which information is transferred by only one device at a time. It is similar to a one-way road, as shown in Figure 1-28.

Figure 1-28 Simplex transmission is one-way data transmission.

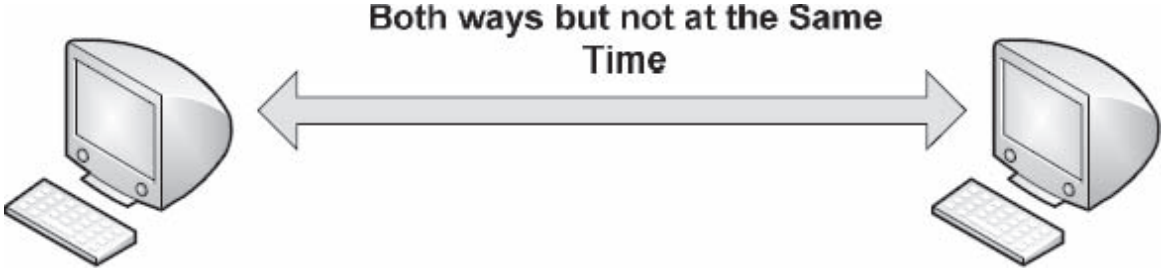


Figure 1-29 Half-duplex transmission can transmit information both ways, but not at the same time.

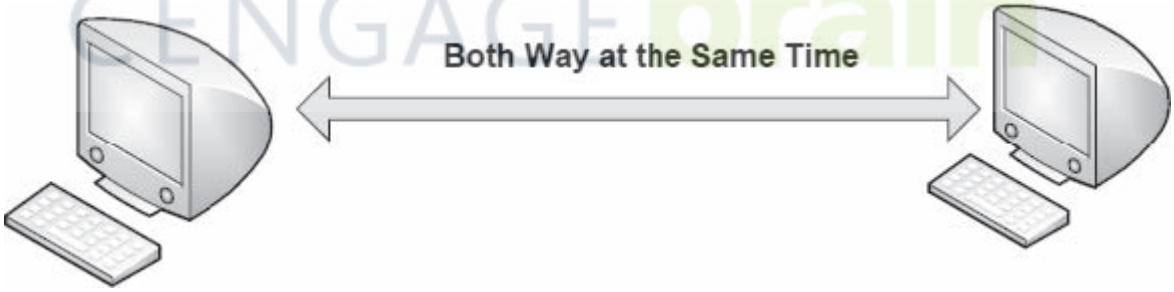


Figure 1-30 Full-duplex transmission can transmit information both ways simultaneously.

Half-Duplex Transmission

In half-duplex mode, data typically transmit in only one direction at a time. Both stations can transmit and receive data, but not at the same time. When one station is sending data, the other can only receive the data, and vice versa. For most LANs, half-duplex mode is efficient.

In half-duplex transmission, the channel transmitting at a particular time uses the entire capacity of a channel. A broadband network supports half-duplex communication. Walkie-talkies and band radios are examples of a half-duplex system, as shown in Figure 1-29.

Full-Duplex Transmission

In full-duplex mode, data can be transmitted in both directions at the same time. Both stations can transmit and receive data simultaneously, as shown in Figure 1-30.

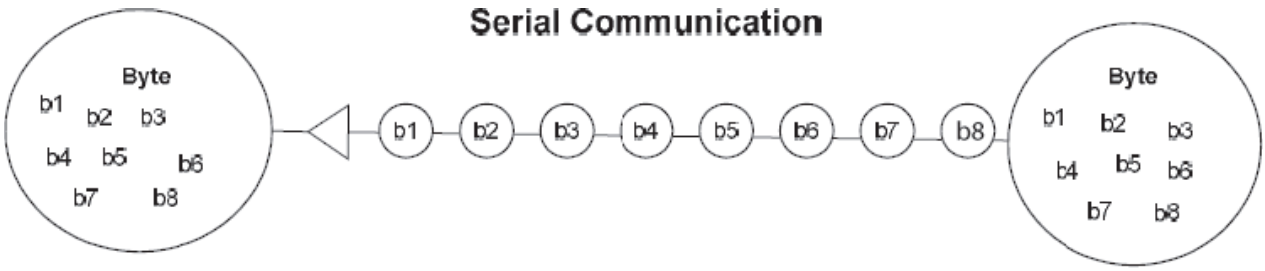


Figure 1-31 In serial data transmission, data bits are transferred over a single medium.

In full-duplex transmission, sharing can be done in two ways:

- The link must contain two physically separate transmission paths for sending and receiving.
- The capacity of the channel is divided between signals traveling in opposite directions.

Some manufacturers are making Ethernet equipment that makes it possible to convert half-duplex mode to full-duplex. Full-duplex Ethernet essentially doubles the throughput of the existing network. The most common example of this is a telephone network, where two people can talk and listen at the same time.

Types of Transmission

A transmission is a channel capable of carrying data from one terminal to another terminal. There are four different types of transmission:

- Serial data transmission
- Parallel data transmission
- Unicast transmission
- Multicast transmission

All these transmissions are used to transfer data, but in a different manner.

Serial Data Transmission

In serial data transmission, data bits are transmitted at a rate of one per clock cycle over a single transmission medium, as shown in Figure 1-31. The synchronization of bits, start/stop bits, and error correction bits are transmitted serially by limiting the overall throughput of data.

Data must pass through a serial interface to exit a computer as serial data. This communication is also called a "one-at-a-time transmission" because bits are transferred one after the other.

Figure 1-31 illustrates the flow of data from one terminal to another in a serial manner. Here, data is transferred in terms of bits.

Parallel Data Transmission

In parallel transmission, multiple bits are transmitted across multiple transmission lines, as shown in Figure 1-32. Many data bits or multiple bytes are also transferred per clock cycle. During this transmission, synchronization of bits, start/stop bits, and error correction bits are transmitted in a line of data bits, which in turn improves overall throughput of data by using additional parallel data lines.

Unicast Transmission

Unicast transmission is a type of transmission method in which information or data is transferred from a specific host address to a specific host destination address, as shown in Figure 1-33. In this transmission, there is only one sender and one receiver. The most familiar standard applications of this transmission are HTTP, FTP, SMTP, and telnet.

All LANs, like Ethernet and IP networks, support unicast transmission. This is an inefficient method as it carries the same information multiple times, which requires more bandwidth. Each unicast transmission over a

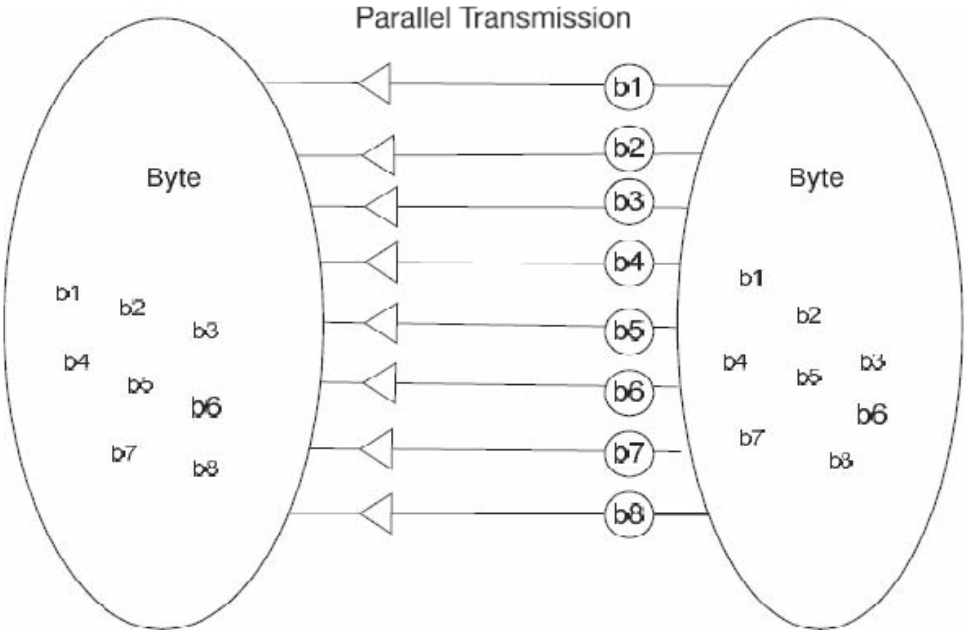


Figure 1-32 Parallel data transmission transfers data across multiple lines.

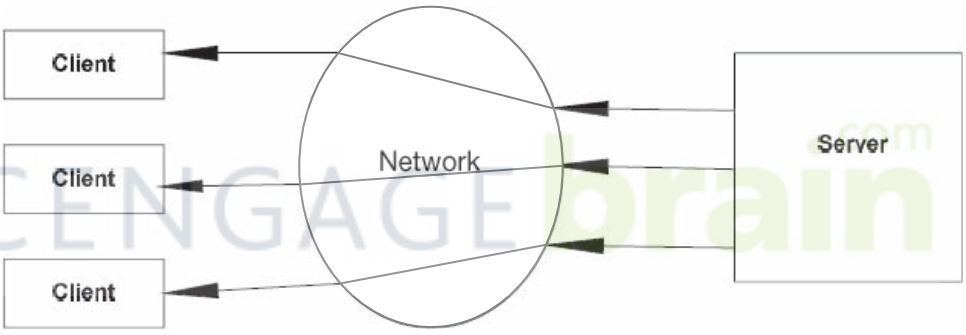


Figure 1-33 Unicast transmission transmits data from one address to another.

network must touch each point or node on the entire network to get to the intended receiver. This transmission is also called a point-to-point network.

Multicast Transmission

In the multicast transmission method, data is transmitted or sent from a server to a specific node that is defined as a member of a multicast group, as shown in Figure 1-34. In these transmissions, a piece of information is sent from one or more points to a set of other points.

Classifying the Network

This classification mainly deals with the logical connection of networks and concentrates on how a network is connected. A logical network combines together a set of entities (e.g., users) that are somehow connected.

There are three different network classifications:

1. Client-server networking
2. Peer-to-peer networking
3. Mixed-mode networking

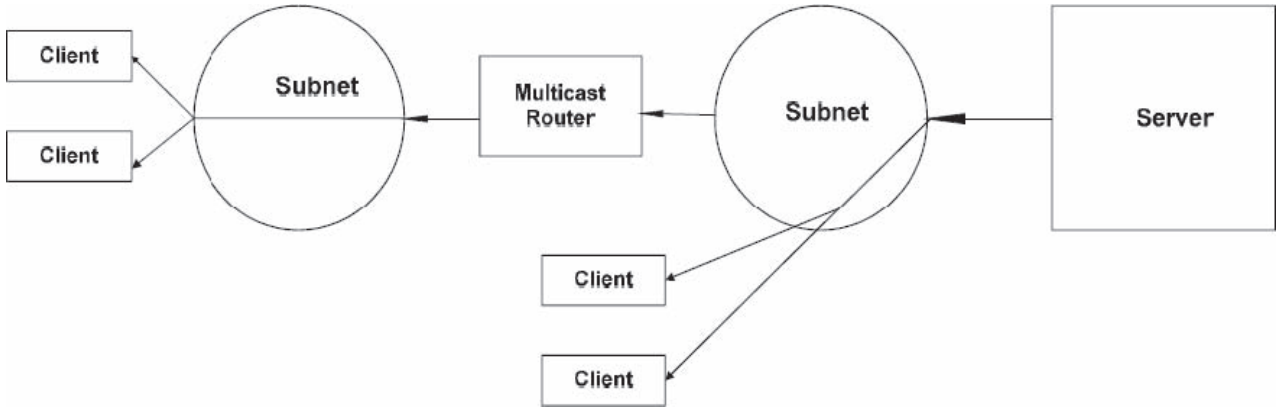


Figure 1-34 Multicast transmission sends data from a server to a specific node.

Client-Server Networking

In a client-server network, some computers act as clients and some act as servers. Clients are those computers who use services that a server provides. A server is a high-powered computer that provides services to computers on a network. It provides back-end support (i.e., all databases are present on the server side). It stores e-mail, Web pages, files, and/or applications.

The following are some of the different kinds of servers that control the sharing of data:

- File servers
- Print servers
- Application servers
- E-mail servers
- Web servers
- Database servers

A client-server network can be constructed by designating one or more of the networked computers as a server and the rest as clients, even when all of the computers can perform both functions. In most LANs and WANs, client-server technology is more useful. However, it is preferable to keep more than one computer as a server because if the server fails in a single server system, the entire system goes down.

A client-server network typically uses a directory service as a database to store information about the network and its users. Users (who use client computers) who want to use a service can log on to the directory service instead of logging on to individual computers, and administrators (who use the server computer) can control access to the entire network using the directory service as a central resource.

Server computers provide the necessary network security and control. The network manager functions as an administrator and manages the client-server network. The administrator determines which resources should be made available and sets permissions on the resources, as shown in Figure 1-35.

A server generally has large hard drives, additional random access memory, and additional hardware installed to manage all network functions. Client-server networks are much more common in businesses.

Peer-To-Peer Networking

In ***peer-to-peer networks***, every computer operates as a client and a server (i.e., any computer can share its resources with the network and access the shared resources on other computers). Peer-to-peer networks are easy to set up and require no special hardware or software or an expensive central computer.

The following are some disadvantages of peer-to-peer networks:

- This type of network can only be applied in some LANs because each system has to maintain its own user accounts and other security settings.
- There is no centralized management of the network.

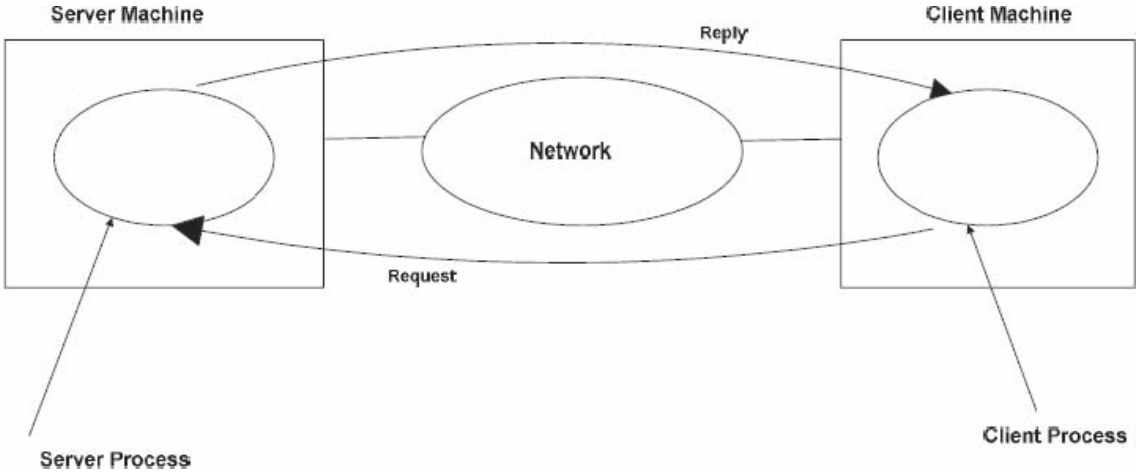


Figure 1-35 Client-server architecture uses a request-and-reply method of communication.

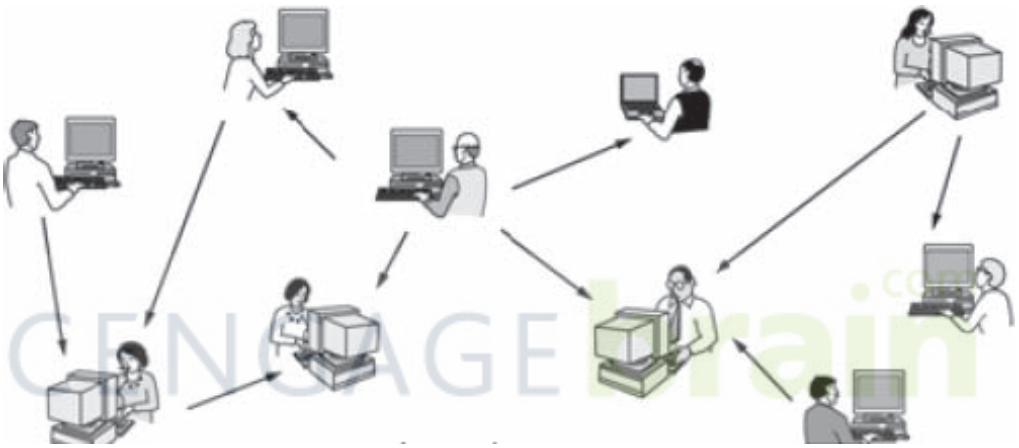


Figure 1-36 Peer-to-peer networking shares data equally among users.

- Each user has to make regular backups of data, because the data and software are located on several different computers.

Peer-to-peer networks are much more common in homes and small offices.

Figure 1-36 illustrates how peer-to-peer networks work. The data or information is shared among different users equally. This network gives equal importance to all the users.

Mixed-Mode Networking

A mixed-mode network is a combination of a client-server network and a peer-to-peer network. This network has elements of both of these two types of networks. One of the major uses of a mixed-mode network is a workgroup created to share local resources within a client-server network.

Network Topology

Network topology deals with the way in which connections are made within a network. Two or more devices connected to two or more links form a topology. Topology deals with a network's overall design and data flow. A physical topology is a topology that deals with the configuration of cables, computers, and other peripheral devices.

There are seven different types of topologies:

- Bus
- Star or hub
- Star-wired
- Mesh
- Ring
- Tree
- Hybrid

Data Sharing

A storage area network (SAN) improves the concept of data sharing. Though LANs allow the application and end user to access data at a central location, a SAN moves the data to a much faster infrastructure. This helps to transfer large files in parallel to multiple computers without affecting the corporate LAN.

Participating computers must be able to find and use the contents of a file while sharing the data. Thus, participating computers with different operating systems are required to use protocols for the transmission of data between protocol translation modules. This helps establish a common communication between the systems.

Data sharing is associated with primary storage devices but can be done with secondary storage as well. Storage devices, such as robotic tape libraries, contain multiple tape devices. More than one computer can access a large quantity of media using SANs. This increases the capability to share data on secondary storage devices.

Device Sharing

Consider an example: A ring-topology network includes adjacent stations that are attached in series independent of each other. Each station in the topology has the capacity to selectively receive data. This same data will not be received by any other station in the topology. Again, each station coordinates the received data with another station, which ensures that the device receives all the data.

File Servers

File servers have a large impact on backup performance. Backup performance can be calculated on the basis of a faster exchange of data. The faster the elimination and distribution of data across the wire, the larger the megabyte-per-minute backup rate will be.

A file server backup can be affected by the following:

- *Hard disk drives (HDDs)*: Most disks have an access time ranging from 10 to 40 ms. The access time affects the overall performance of the file server.
- *Network interface cards (NICs)*: Slow NICs also affect the performance of file servers. NICs may also take up large amounts of CPU utilization.
- *System memory*: The amount of RAM affects the file server backup when it is shared between the file server processes and the backup process. Most file server based backup systems require adding additional amounts of memory.

Bus Topology

Bus topology is a multipoint topology that consists of a long cable that acts as a support structure for the entire network, as shown in Figure 1-37. The long cable is called a bus, and it connects all devices in the network. In bus topology, all the devices in the network are connected to the bus cable using links, such as drop lines and taps. A tap is a connector that slices the bus cable to establish a contact with the metallic part. As the signals pass through the cable, some of the energy is converted into heat. As a result, it becomes fragile in the long run.

Bus topology has the following advantages:

- Installation is effortless.
- The bus cable can be set up through a best path, and in turn, the other connectors can be connected to the devices.

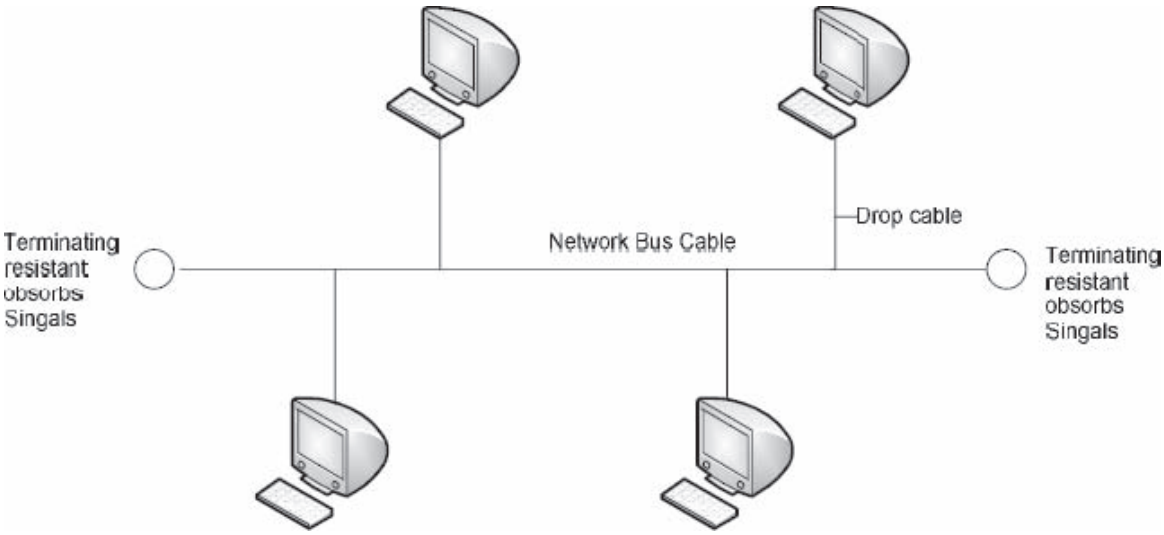


Figure 1-37 Bus topology uses a single cable as the support for the network.

- It requires less cabling compared to mesh, star, and tree topologies.
- Repetition is avoided in bus topology, as the same cable extends throughout the network irrespective of the other topologies.

Bus topology has the following disadvantages:

- It involves a rather difficult design.
- The defect separation is also difficult.
- Since the installation is difficult in the case of a bus, it is also very difficult to add new devices to the bus.
- Sometimes, mirroring of the signals occurs at the tap regions, which can cause signal quality to deteriorate.
- Defects in the bus cable can suspend all communication between devices on the same side.

Bus topology is further categorized into two types:

1. Linear bus
2. Distributed bus

Linear Bus

A linear bus is a type of bus topology that consists of a cable and a terminator at each end, as shown in Figure 1-38. This topology is mainly used in Ethernet and LocalTalk networks.

Linear bus topology has the following advantages:

- It requires fewer cables to connect various devices.
- This topology uses peer-to-peer LANs, coaxial cables, and 50- to 93-ohm terminators for connecting various systems at each end.
- A single cable supports the entire network.
- It is easy to connect new peripheral devices and systems to a linear bus.
- It requires less cable length when compared to a star topology.

Linear bus topology has the following disadvantages:

- Breakdowns in the main cable disable the entire network.
- The main cable uses terminators at both ends of the device.

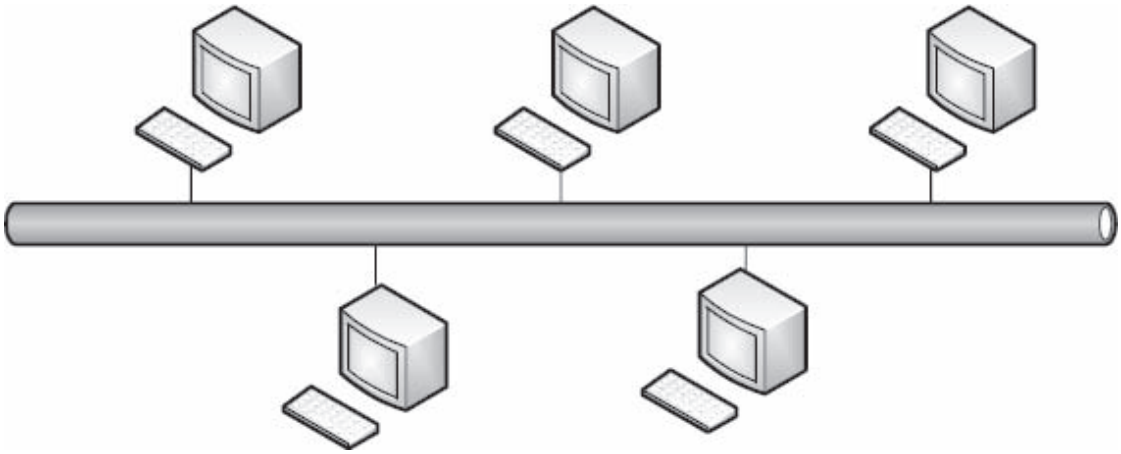


Figure 1-38 A linear bus uses a cable with a terminator at each end.

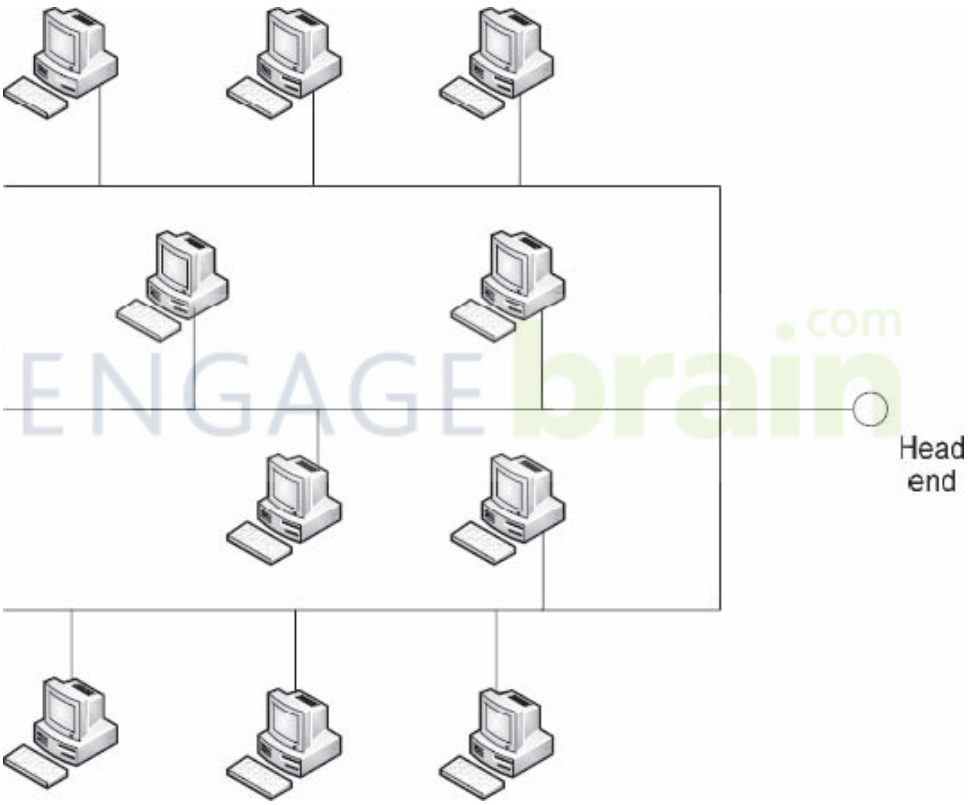


Figure 1-39 A distributed bus uses a single node with links.

- It is difficult to identify problems in this topology in case of network failure.
- This topology is not suited for large buildings that use more devices and systems.

Distributed Bus

Distributed bus is a complex topology. It uses a single node from the trunk cable, called a root or head end, which contains various links in the network.

Figure 1-39 illustrates a distributed bus that has different nodes connected at various branches. If the root fails, then the entire network goes down. All the nodes are connected to a common transmission medium,

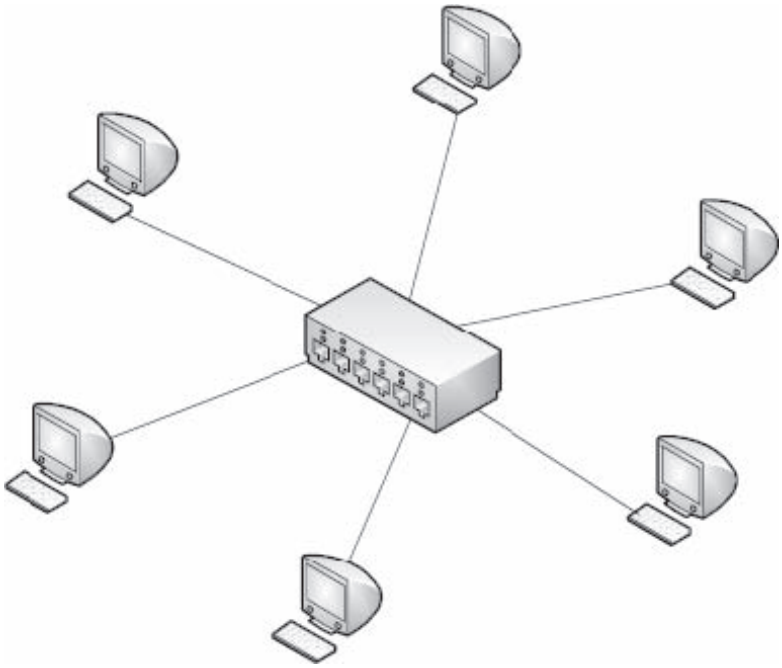


Figure 1-40 Star topology uses a single central computer as a router.

which has more than two endpoints created by adding branches to the main node. This topology is sometimes called a tree topology, as the structure looks like a tree, but it differs in that there is no central node connecting the other nodes.

Star Topology

Star topology is one of the more popular network topologies. Star topology consists of a central, or hub, computer that functions as a router to send messages, as shown in Figure 1-40. In star topology, each device has a devoted point-to-point communication to a central monitoring unit called a hub. The devices are not directly connected to each other. Star topology also does not permit direct traffic between the devices in the network. If one device wants to send data to another device, then the device has to send data to the central hub, which diverts the data to all the other devices in the network.

Star topology is comparatively cheaper than mesh topology, as each device needs only one cable and one I/O device to link to any of the other devices. This fact makes setting up and redesigning the topology more simple. This also leads to less wiring between the already existing devices and the newly installed devices. One of the biggest advantages of the star topology is its strength. If one link is lost, only that particular link is affected. All the other links continue working. This factor results in easy recognition and effortless detection of defects. The hub, as long as it is functioning properly, can examine connection problems and circumvent defective links.

Star topology has the following advantages:

- It is easy to execute and extend in large networks.
- It is adaptable for short-term networks.
- The destruction of a node other than the central node will not have significant effects on the operation of the network.

Star topology has the following disadvantages:

- It has a restricted cable length and supports a small number of stations.
- The cost of maintaining it may become higher in the future.
- Loss of the central node can disable the whole network.

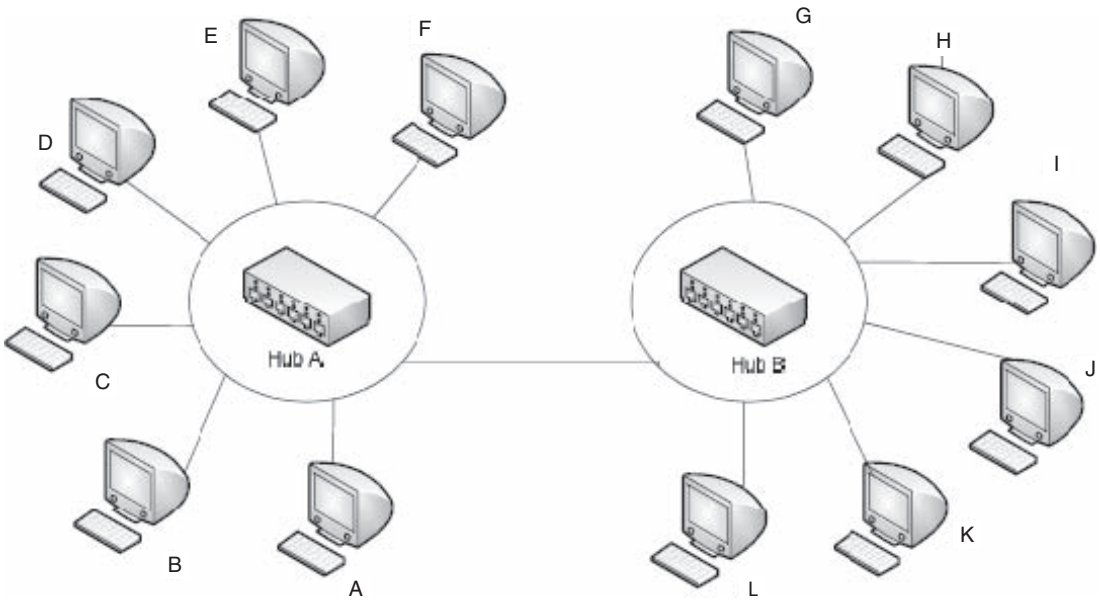


Figure 1-41 Star-wired ring topology combines elements of physical star and logical ring topologies.

Extended Star Topology

In the extended star topology, two or more networks that are arranged in physical star topology are connected using repeaters. The central node of one star network is connected to the terminal node of the other star network. The extended star topology connects multiple hubs of different stars.

Distributed Star Topology

In this kind of topology, two or more networks that are arranged in physical star topology are connected in a linear fashion, with no other nodes that explicitly connect them.

Star-Wired Ring Topology

A star-wired ring topology is the combination of physical star topology and logical ring topology. Devices arranged in this topology form a physical star, as shown in Figure 1-41. A single communication channel exists in the topology, forming a logical ring. Sent messages are forwarded from one device to another in the ring.

The following are advantages of star-wired ring topology:

- Troubleshooting is easy
- Expansion of the network is easy due to the modular design
- The connection of the hub is flexible

The following is a disadvantage of star-wired ring topology:

- Due to extreme flexibility of arrangement, configuration and cabling is difficult

Ring Topology

In ring topology, each device has a dedicated point-to-point communication with only one other device on each side of the device, as shown in Figure 1-42. A signal is sent along the ring in a unidirectional manner through each device until it reaches its destination. Each device in a ring has a router integrated in it. When a device receives a signal meant for another device, the repeater reproduces bits and sends them along the network. In ring topology, a signal keeps traveling through the network until it reaches its destination.

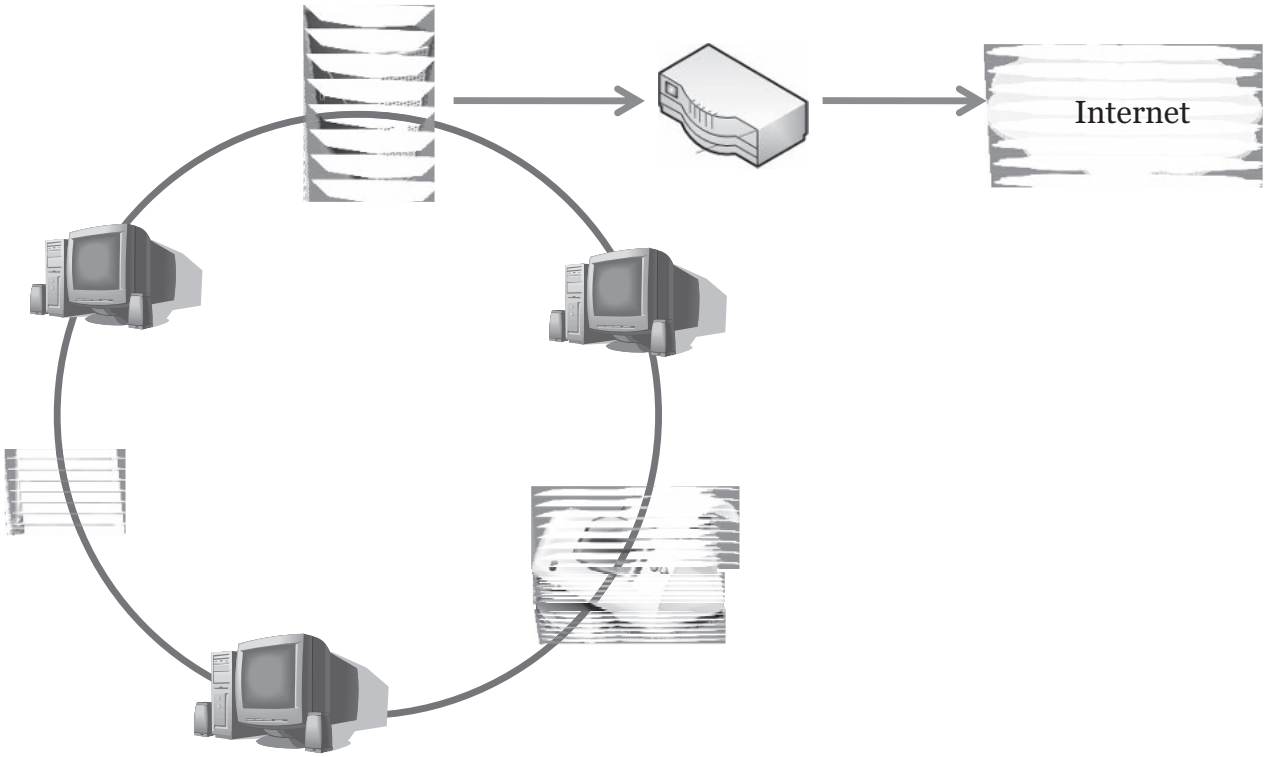


Figure 1-42 In ring topology, signals are sent point to point.

Ring topology has the following advantages:

- The ring is comparatively easy to set up and configure
- Addition or deletion of devices mandates shifting only two connections
- It is easy to find faults in ring topology

Ring topology has the following disadvantage:

- Unidirectional communication can be a defect, as a loss in the ring can cripple the entire network

Mesh Topology

In mesh topology, every device has a point-to-point link to all the other devices, as shown in Figure 1-43. A completely connected mesh network has $n(n-1)/2$ channels to connect n devices. To cater to all the connections, each device on the network needs to have $n-1$ input/output ports. The mesh has many advantages over other topologies. The usage of dedicated point-to-point links ensures that every connection can broadcast its data, reducing the traffic related issues that arise when connections are shared by more than one device. Physical boundaries prohibit unauthentic users from accessing the devices.

Point-to-point devices simplify fault detection and fault isolation. Routing of traffic can be done to reduce the links, which are vulnerable to certain security violations. This functionality enables the network administrator to find out the specific location of errors and helps in detecting the root of the problem and provides solutions.

Mesh topology has the following advantages:

- Mesh topology is strong, and if one of the links is lost, the others are not affected
- Mesh topology makes the network secure

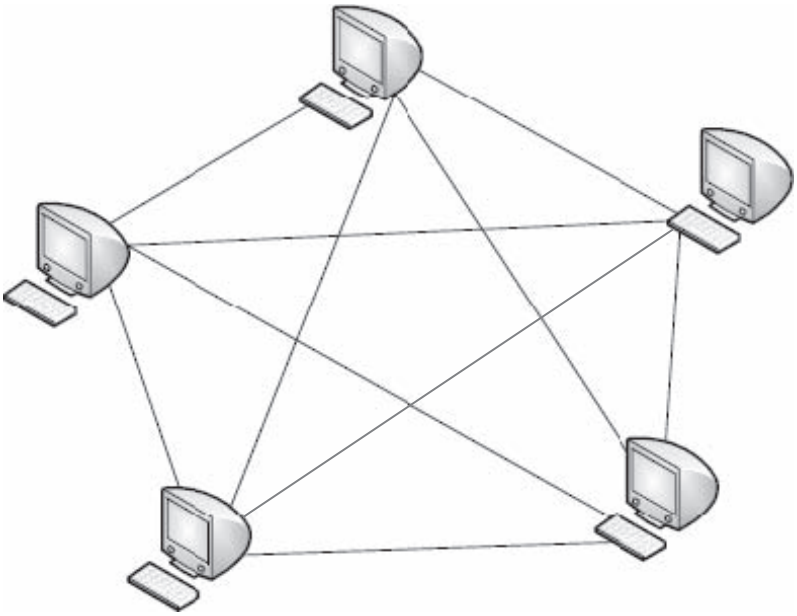


Figure 1-43 Mesh topology connects every unit in a network.

Mesh topology has the following disadvantages:

- A lot of cabling is involved, and more ports are needed
- Every device must be linked to every other device
- The setup and design are tedious
- More space is also required to accommodate all the wiring
- The hardware needed to connect all the links is also very costly
- The mesh topology is executed limitedly for linking the primary computers of networks that use several other topologies

Tree Topology

The tree topology is a version of star. The devices in a tree are connected to a central hub that monitors network traffic, as shown in Figure 1-44. The auxiliary hub is linked to several devices; the auxiliary hub in turn connects to the central hub. The central hub contains a repeater that reproduces the bit streams before sending them. Repeaters make the transmissions robust and enhance the distance signals travel. The auxiliary hub can be active or passive. A passive hub has simpler connections between the linked devices.

Cable-television technology can be considered a typical example of a tree topology. The primary cable is divided into many auxiliary cables, and each cable is further divided into subcables and so on.

Tree topology has the following advantage:

- It permits more devices to be linked to a central hub and thus increases the signal distance between two devices

Tree topology has the following disadvantages:

- If the root fails, the network fails
- It is complicated to configure
- There are slow access times when the network grows

There are two types of fundamental tree topologies:

1. *Minimum spanning tree*: It costs little to connect all the nodes in the topology.
2. *Steiner tree*: This is a least-cost tree that can connect a subset of all the nodes.

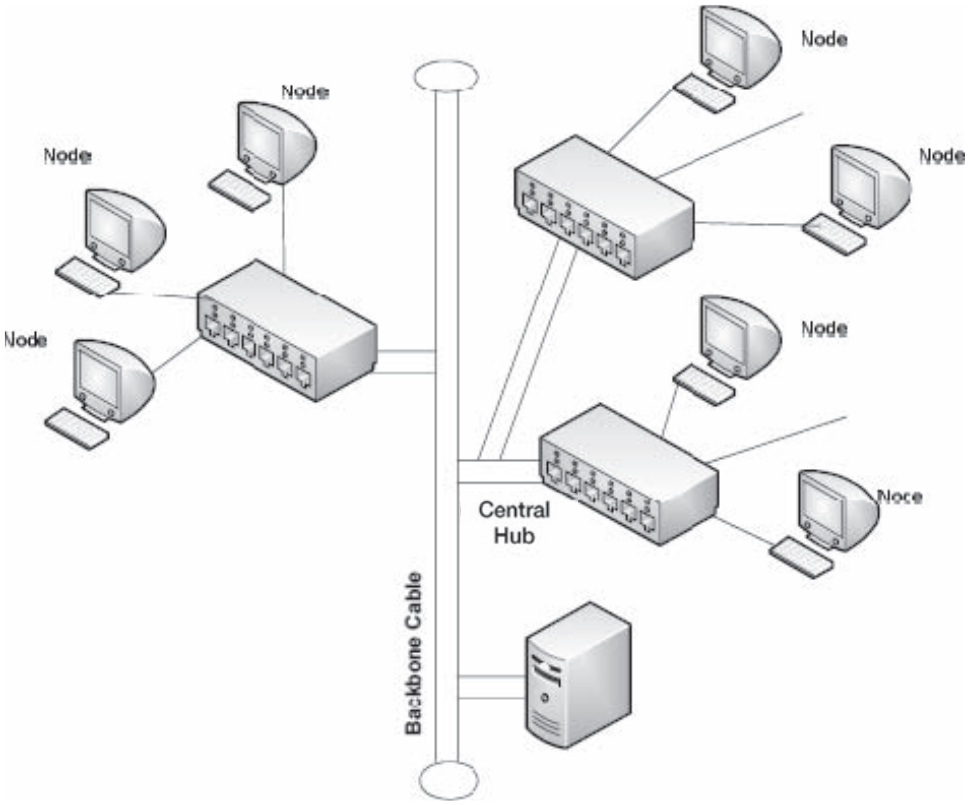


Figure 1-44 In tree topology, a central hub monitors traffic.

Hybrid Topology

The hybrid topology is the combination of any two or more different topologies. The most commonly used topologies are star-bus, as shown in Figure 1-45, or star-ring. A multistation access unit is used in a star-bus.

Physical Network Classification

Networks are classified according to their physical location or their geographical boundaries. The physical location of the network affects its throughput. The arrangement of devices is made according to the needs of the organization and the standards of the network. The following arrangements are among the many network classifications:

- Local area network (LAN)
- Wide area network (WAN)
- Metropolitan area network (MAN)
- Personal area network (PAN)
- Campus area network (CAN)
- Global area network (GAN)

Local Area Network

A local area network typically exists in private organizations and connects the nodes in a single organization or location, as shown in Figure 1-46. LANs usually vary based on the requirements and the type of technology used. A simple LAN consists of only PCs and some hardware devices, such as printers, for domestic purposes such as in homes.

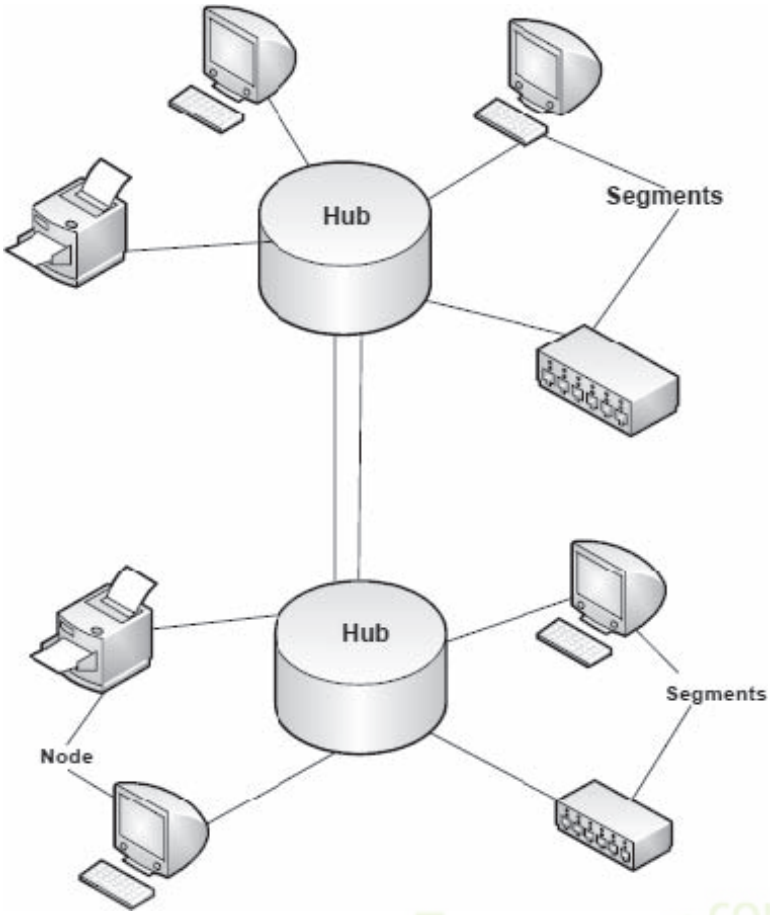


Figure 1-45 Hybrid topologies use one or more topologies together, such as star and bus.

LANs are designed to facilitate the sharing of resources between PCs or workstations. The assets to be shared include hardware devices, such as printers, and software. LANs in organizations are useful for linking the computers, which are allotted identical functionalities. In such a scenario, some of the computers are given higher storage capacities so they can act as servers and the others can act as clients. LANs are also differentiated from other types of networks based on their communication media and topology. Typically, a LAN uses only one type of communication medium. The most popular LAN topologies are bus, ring, and star.

Early LANs had data rates ranging from 4 to 16 Mbps. Now, speeds from 100 Mbps to 1 Gbps (1000 Mbps) are common. The protocols used by LANs also distinguish them from other kinds of networks. LANs can use client-server architecture or peer-to-peer architecture.

The following are some LAN technologies:

- Ethernet
- Token Ring
- FDDI (Fiber Distributed Data Interface)

Ethernet

The original Ethernet was developed by the Xerox Corporation and operated at a rate of 3 Mbps using the CSMA/CD protocol. In later years, three companies (Xerox Corporation, Intel Corporation, and Digital Equipment Corporation) jointly developed Ethernet version 1.0.

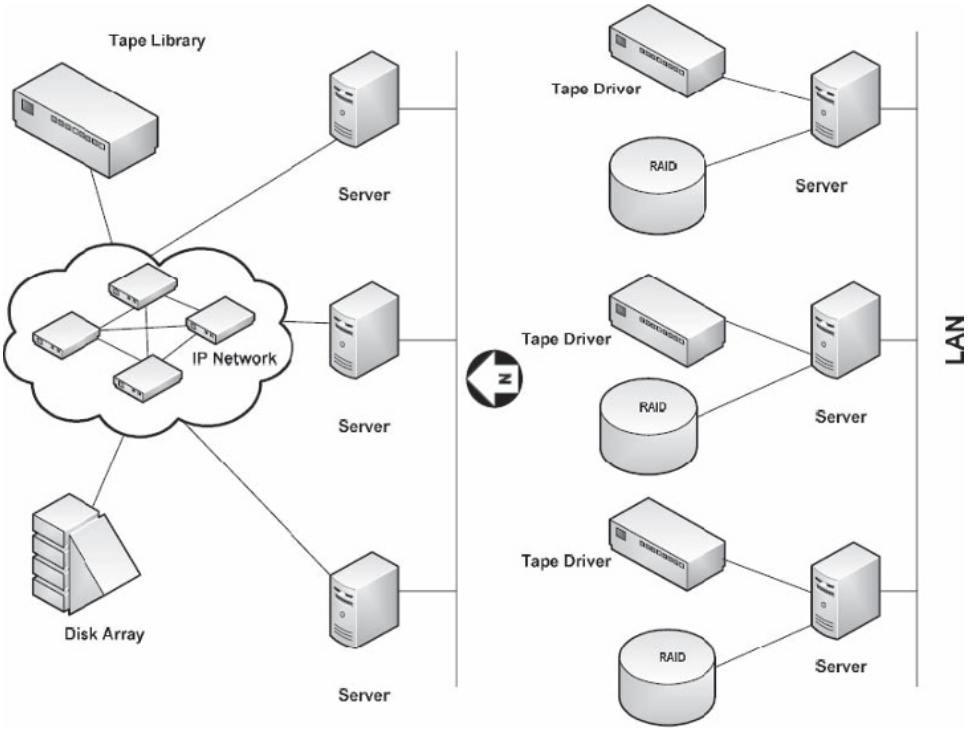


Figure 1-46 Local area networks connect the nodes in a single organization.

Ethernet Elements The Ethernet consists of network nodes and the interconnecting media. There are two major classes of network nodes:

1. *Data terminal equipment (DTE)*: DTEs are devices like PCs, workstations, and file servers.
2. *Data communication equipment (DCE)*: Repeaters, network switches, routers, interface cards, and modems are DCEs. These devices forward and receive data frames from the network.

Basic Ethernet Frame Format In the IEEE 802.3 standard, a data-frame format is provided for media access control implementation and other optional formats, which can extend the capability of the protocol, as shown in Figure 1-47.

Intranet

Intranet is the term for a group of private computer networks. With the help of an intranet, data and resources can be shared within an organization. Intranet uses technologies like Ethernet, Wi-Fi, TCP/IP, Web browsers, and Web servers. Users outside the intranet cannot access the intranet directly.

Wide Area Networks (WANs)

WANs are built to provide transmission solutions for companies or groups who need to interchange information such as data, voice, and images between two distant locations, as shown in Figure 1-48. As the distance involved is great, telecommunication organizations play a role in WAN communications. In fact, leased and public communication companies usually sustain WANs.

The major purpose of a WAN is to provide trustworthy, quick, and secure communication between two or more places with short delays and at low costs. WANs enable an organization to have one basic network between all its departments and offices, even though they are not present in the same building or city, facilitating communication between the organization and other locations worldwide. WANs are subject to a country's public communication department policies and rules.

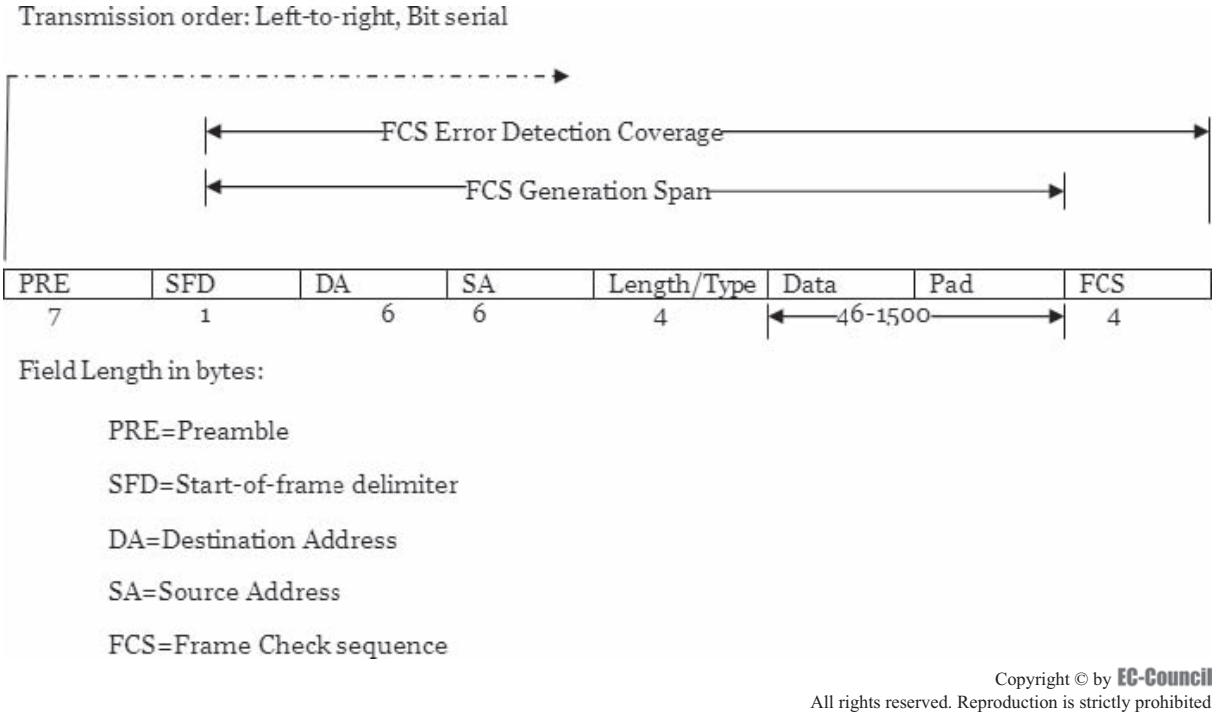


Figure 1-47 A data-frame format is provided for the media access control implementation.

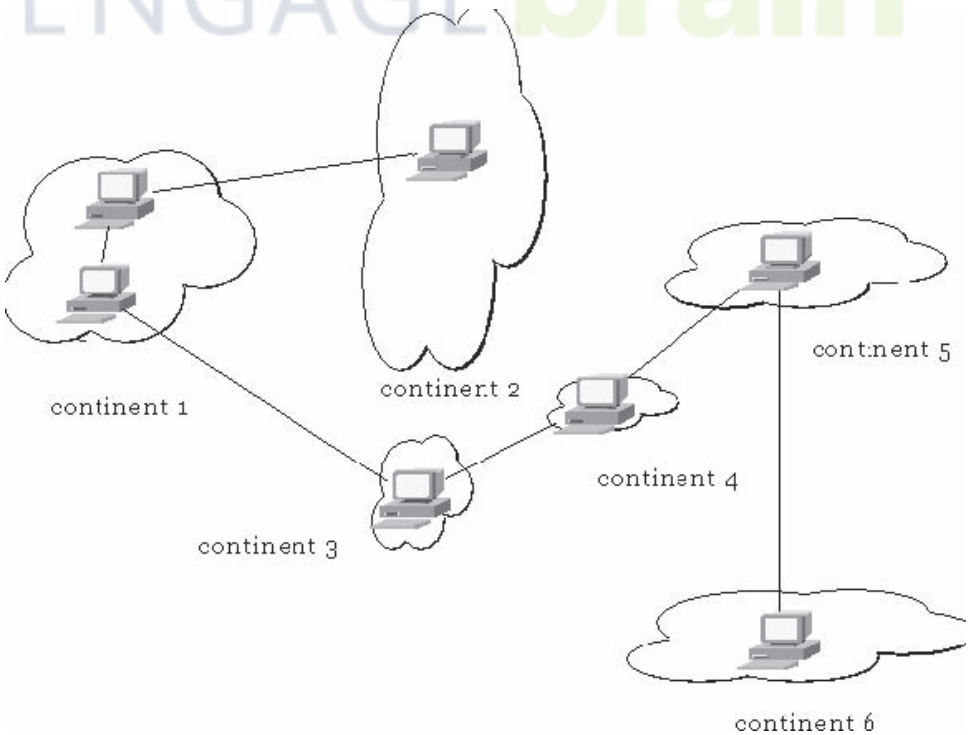


Figure 1-48 WANs facilitate data transmission between distant geographic locations.

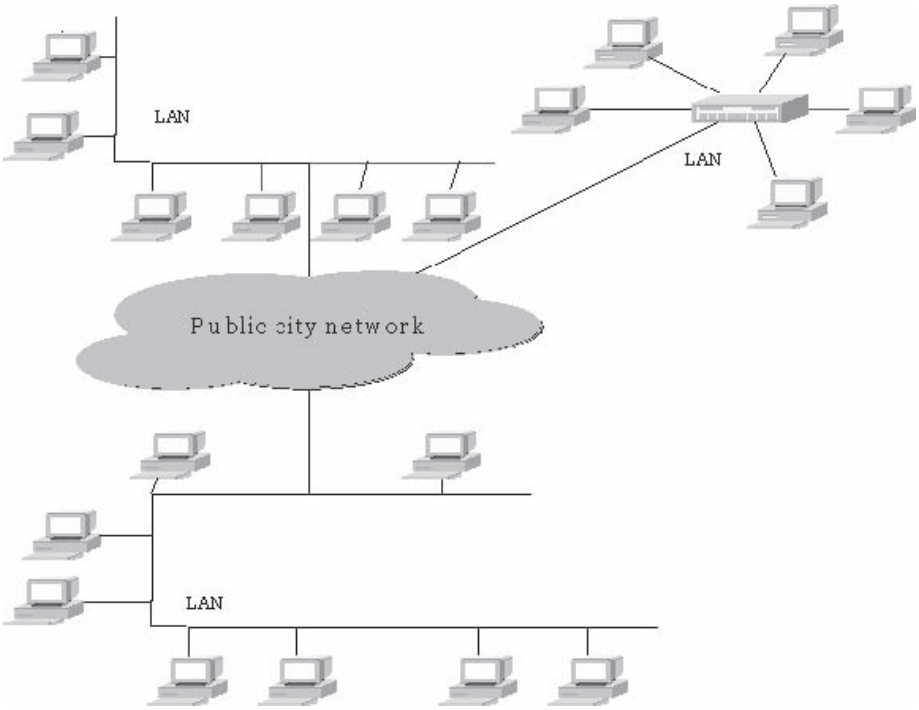


Figure 1-49 MANs are used for public networks.

WAN technologies include the following:

- Packet-switched WANs
- ATMs
- B-ISDNs

Metropolitan Area Networks (MANs)

Metropolitan area networks (MANs) are large computer networks ranging over an entire city. They use wireless communication or fiber-optic cables to connect their areas, as show in Figure 1-49.

For example, large educational institutions may have a MAN that links together many of its local area networks (LANs), which covers a distance that is less than a kilometer. The MAN can in turn link several WAN links to other educational institutions or the Internet. The MAN may be a single network or it can be a huge network, which may involve a number of LANs, facilitating the sharing of assets between the various devices on the network. An organization can communicate with its branch offices throughout a city using a MAN.

MAN technologies include the following:

- Ethernet-based MANs (Metro Ethernet)
- DQDB (Distributed Queue Dual Bus)
- SMDS (Switched Multimegabit Data Services)

Some LAN technologies used for this purpose are ATM, FDDI, and SMDS. These earlier technologies are on the verge of being replaced by Ethernet-based MANs (e.g., Metro Ethernet) in the majority of areas. MAN links into LANs that have been built without wires, using communication links such as optical fibers.

A MAN can be completely owned and monitored by a private organization, or it can be provided as a service by any public organization, such as a telecommunications company.

Personal Area Networks (PANs)

PAN refers to wireless communication that uses both radio and optical signals. PAN is quite similar to WLAN. PANs usually range in tens of feet. For specific PAN hardware, the range is typically up to 10 meters

(approximately 33 feet). PANs cover an individual's work area or workgroup; hence, PAN is known as a room-size network. Bluetooth is a PAN technology. PAN provides the following two different types of systems:

1. *Lower data-rate systems*: These types of systems are used to control and access larger systems like personal computers (PCs) or cell phones. The main use of PAN includes wireless audio, keyboards, mice, and inter-system (PC–cell phone) data links.
2. *Higher data-rate systems*: These types of systems are used for audio distribution and household video.

Campus Area Networks (CANs)

CANs cover a limited geographical area. This kind of network is appropriate for university campuses.

Global Area Networks (GANs)

A GAN is a combination of different interconnected computer networks. A GAN covers an unlimited geographical area. The Internet is an example of a GAN.

Network Equipment Functions

Network Interface Cards (NICs)

A network interface card, more commonly known as a NIC, is a device that allows computers to be linked together in a LAN, or local area network. Networked terminals communicate with each other using an existing protocol, or compliant language, for sending data packets between the different terminals, known as nodes. The network interface card acts as the connection for the machine to both transmit and receive data on the LAN. These cards normally use an Ethernet connection, and are available in 10Base-T, 100Base-T, and 1000Base-T configurations.

The most popular language, or protocol, for LANs is Ethernet, sometimes termed IEEE 802.3. When structuring a LAN, a NIC must be set up in each workstation on the network, and all NICs in the network must be of the same structural design.

An Ethernet NIC is fixed in an available opening inside the computer. The NIC allocates a distinctive 48-bit address, called a MAC (media access control) address, to the machine. The MACs on the network are used to send traffic between the computers. The back plate of the network interface card hosts a port that looks similar to a phone jack, but it is a little larger. This port lodges an Ethernet cable, which looks like a thicker version of a typical telephone line. An Ethernet cable must extend from each network interface card to a central hub or switch. The hub or switch passes information between computers using MAC addresses.

Wireless Ethernet cards are installed like their wired equivalents; but instead of a port for an Ethernet cable, the card hosts a small antenna. The card exchanges data with the central wireless switch or hub via radio waves. Wireless LANs may have some limitations depending on the materials used in the structures that house the equipment. For example, lead in walls can obstruct signals between the network interface card and the hub or switch.

NICs have the following advantages:

- A network interface card does not have to be fixed with physical cable.
- A NIC is used to send as well as receive data.

Access Points

An access point is a piece of wireless communications hardware that creates a central point of wireless connectivity. Similar to a hub, the access point is a common connection point for devices in a wireless network.

Switches

A networking switch is the fundamental device in a wired or wireless LAN. It receives signals from each terminal on the network through Ethernet cables in a wired network and through radio waves in a wireless LAN. In both cases, the networking switch sends traffic across the LAN, permitting the computers to communicate with each other and share resources. Whether wireless or wired, the networking switch acts as a relay, analyzing traffic packets as they arrive from the various machines and sending the packets to the indicated MAC address.

Switch Functions

A networking switch functioning in full-duplex mode implies a machine on the LAN that can receive and send data simultaneously. This is quicker than a networking hub, an alternating device that serves the same function as a switch but functions in half-duplex mode, allowing each machine either to send or receive at any given time. Another discrete difference between a networking switch and a hub is that the switch sends traffic separately, using MAC addresses to send traffic packets accurately to where they are supposed to reach. On the other hand, a networking hub sends all traffic on the network to all nodes, depending on filters within each machine to reject packets not sent to it. Doing so makes the network vulnerable to eavesdropping and loss of available bandwidth for regular network traffic. Network switches are low-priced devices that rise in price with the number of ports featured.

Switches have the following advantages:

- A networking switch is more advanced than a networking hub.
- Antisniffing software can be used on a switched network to sense packet sniffers.

Switches have the following disadvantages:

- A networking switch is not infallible. It can be misled into employing packet sniffers.
- Methods used to mislead the switch will leave traffic signatures, unlike the passive methods that can be used on a hub.

Concentrators/Hubs

Acting as a common connection point for devices in a network, hubs are commonly used to connect segments of a LAN. A hub contains multiple ports. When a packet arrives at one port, it is copied to the other ports so that all segments of the LAN can see all packets.

Hubs are generally classified in the following ways:

- *Passive hubs*: Passive hubs do not intensify the signal strength of the data prior to transferring the data packets, but they act as a means to transfer data between the devices on the network. They are also known as concentrators.
- *Active hubs*: Active hubs strengthen the signal prior to transferring it to other devices on the network. Active hubs are referred to as multiport repeaters, as they have multiple ports.
- *Intelligent hubs*: Business-critical hubs need additional features. Those hubs to which additional features are added are called intelligent hubs.
- *Switching hubs*: Switching hubs view the destination address of each data packet before transferring it to the specified destination port.
- *Repeater hubs*: Repeater hubs relay inbound traffic. However, active (or switching) hubs transmit the data that is addressed for that specific host. Performance is also improved.

Certain hubs can be arranged for security at the MAC level (such that only specified MAC addresses are hooked up to specified ports). The latest hubs contain HTTP servers as a built-in feature; if feasible, they block access to a specified IP address/port.

Hubs have the following advantages:

- They are flexible and economical devices.
- Every port can make maximum use of the bandwidth without use of CSMA/CD.
- Adding hubs increases the number of ports.
- Hubs organized through SNMP provide tools and statistics for better management.
- Hubs are a low-cost solution.
- Hubs are used to route network traffic and prevent network crashes. They can also combine relatively slow Ethernet devices with those of higher speeds. This facilitates the addition of a variety of devices with a variety of speeds.
- Hubs are not used to control traffic.

Hubs have the following disadvantage:

- If hubs are not monitored, they can be compromised.

Modem

The term *modem* refers to a MOdulator-DEModulator. It is a device that converts digital signals into analog signals and vice versa. The signals from a computer are in digital form, and signals that are transferred over telephone lines are in analog form. The modem performs this conversion. Modulation is performed prior to sending the data, and demodulation is performed after receiving the data. A modulator is a device that converts a digital signal to an analog signal. A demodulator, then, is a device that reconverts an analog signal to a digital signal using the same carrier frequency. The functions of both devices are merged into a single device called a modem.

The following are some of the different types of modems:

- Internal devices that plug into expansion slots in a computer
- External devices that plug into serial or USB ports
- PCMCIA cards intended for use in laptops
- Specialized devices designed for use in handheld computers
- Integrated modems in laptops
- Rack-mounted modems for dial-up ISPs

Modems provide slow speeds for data access and communication. The fastest modem has a maximum speed of 56 kbps. The speed of a modem depends on certain factors, which include the quality of the phone line.

Modem speeds can be presented in either baud rate or bits per second (bps). The baud rate refers to the number of times a signal changes in each second. The bps rate is the number of bits of data that can be sent or received in one second. In some modems the figures are identical, whereas in others, the bps rate is higher than the baud rate.

Router

Routers are more complicated than devices like repeaters and bridges. Routers can access the Internet Protocol (IP) addresses of the network layer and can have incorporated software that helps them identify which of multiple paths are possible between the addresses and which channel is appropriate for the transmission of data.

Routers function in the physical, data-link, and network layers of the OSI model. Routers transmit packets among several interconnected networks. They send packets from a network to other important destinations. A packet sent from one destination to another traverses through the router initially and then moves to the destination network. The destination router, in turn, transmits the packet until the final destination is reached. Routers behave as stations on the network, as shown in Figure 1-50.

Routers receive packets from a linked network and transmit them to the next connected network. If a received packet contains the address of a node of a network to which the router does not belong, the router is capable of

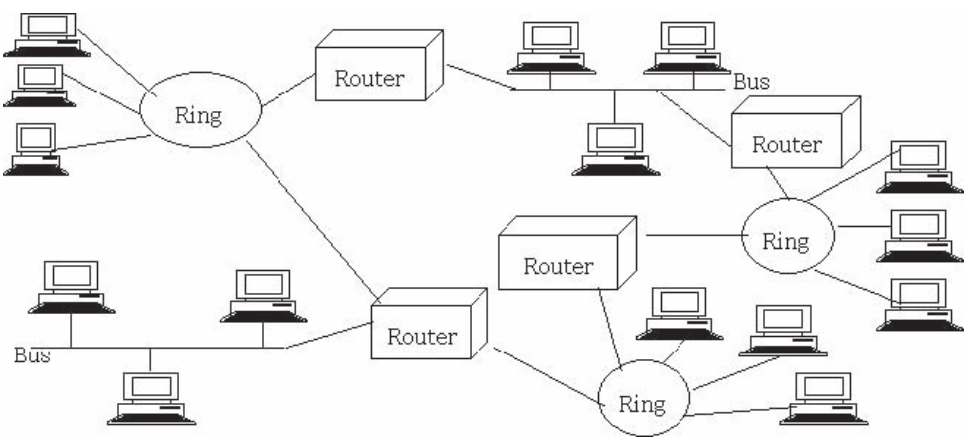


Figure 1-50 Routers act as stations on a network.

identifying which of the linked networks is the next best option for the packet. After identifying the appropriate route for the packet, the router transmits the packet to the other network.

A router maintains a routing table through which it can maintain the paths through which routing occurs as well as the cost of routing across the network. Static routing is a type of routing through which the network administrator monitors the entire routing process. Routing includes many concepts, such as least-cost routing, which shows which path is the shortest available (shortest, in terms of routing, also implies a path that is secure and fastest).

Routers can associate different networks, such as LAN and WAN, and can broadcast data. Routers prevent the collision of data during broadcast. Routers can also act like other devices, such as bridges, which can broadcast packets for a single protocol or group of protocols. When a router receives packets from a multiprotocol router, it receives the packets that correspond to one of the protocols for which they are configured and then sends the packets depending on the addresses of the network layer.

Routers have the following advantages:

- Routers operate at the protocol level.
- Routers provide remote management and design via SNMP.
- Routers support intricate networks.
- The more filtering done, the lower the performance.
- Routers provide security.
- Administrators are able to section networks reasonably.
- Broadcast collisions can be avoided.
- Routers regularly provide bridge functions.
- Routers use complicated routing protocols such as RIP, IGRP, and OSPF.

Routers have the following disadvantages:

- The security issues that routers face are that they do not have security controls that are very efficient, which leads to system compromises.
- Routers cause long delays in initializing sessions for protocols such as FTP. The following aspects must be checked before router transmissions:
  - Mapping between the ports
  - Internal addresses
  - External addresses
  - The port numbers of the internal and external addresses
- Routers are more expensive than other devices.
- Routers need protocols designed for routing.
- Routers are slower than other devices.
- Routers lead to overhead, as they are not capable of separating sent packets.

Brouter

A brouter operates as both a bridge and a router. It is a short name for bridge router because it combines features and operations of both. Normally, it routes routable protocols like TCP/IP and bridges nonroutable protocols.

Brouters operate like routers by relaying data transmission between nodes in a network. However, they also operate like bridges that forward data to the next segment using its physical address if it is found that the data is using an unfamiliar protocol.

Brouters perform the following functions:

- They have routing tables that enable TCP/IP packet traversals.
- Brouters operate without protocol restrictions.
- Brouters look at incoming frames and check the network-layer protocol of that frame. If the brouter recognizes the protocol, it acts like a router and establishes the shortest path. If it doesn't, it acts like a bridge and passes the frame to the next segment.

Brouters have the following advantages:

- They use physical addresses to perform routing.
- They route traffic that uses mixed protocols.
- Brouters efficiently replace routers and bridges.
- Brouters save the cost of installing routers and bridges separately.

Bridges

A bridge filters traffic at the network boundaries. Bridges can send data packets called frames between two segregated LANs at the data-link layer. Bridges are logical devices that can maintain each segment's traffic separately. Through this, bridges prevent congestion and segregation problems. Bridges that operate in the data-link layer permit access to the physical addresses of the terminals linked to it.

When a bridge receives a data packet, it checks the destination address against a lookup table, which contains the physical addresses of all the workstations linked to the bridge. When an address is found, the bridge determines which network segment the packet belongs to and sends the packet to the appropriate segment. Bridges use the MAC address to make decisions on relaying network packets. Bridges also act as filters, determining whether the packets have to be relayed to a segment or not.

Bridges can be classified into the following categories:

- Simple bridges
- Multiport bridges
- Transparent bridges

Transparent Bridging

A transparent bridge contains a forwarding table. Entries are added to the table whenever the bridge receives an incoming packet. If a packet's destination address is in the table, the bridge forwards the packet directly to the destination. If the address isn't in the table, the packet is forwarded to all the devices in the network except the source.

A system with a transparent bridge must satisfy three criteria:

1. Each station should forward frames from one station to another.
2. A forwarding table should be built up from incoming frames.
3. Loops are to be avoided.

Loop Problem Transparent bridges work efficiently if redundant bridges do not exist in the network. If there are two LANs and they are connected via two bridges, then a loop exists in the network, whereby frames can travel endlessly around the network.

ISDN Terminal Adapter

An ISDN terminal adapter is an interfacing device that allows a non-ISDN terminal or other computer device at the physical layer to communicate with an ISDN network. It is employed at the R reference point in ISDN network terminology.

It switches automatically between analog and digital depending on the type of call. An ISDN terminal adapter supports RJ-11 telephone connection plugs for voice access and RS-232C, V.35, and RS-449 interfaces for data.

Terminal adapters have the following advantages:

- Terminal adapters are used in ISDN when a user wants to access the Internet speedily, or for data and video transmission.
- Terminal adapters are available as: add-in expansion cards, which the user can install into computers; external devices like those that connect to the serial interfaces of PC systems; or modules in a router.

Terminal adapters have the following disadvantage:

- The major disadvantage of a terminal adapter is that information from the D-channel of the ISDN line does not pass fully through the terminal adapter. For this reason, non-ISDN equipment is unable to take full advantage of ISDN facilities.

Network Adapter

Each computer should have a network adapter through which it can be connected to the network.

How to Determine the Presence of a Network Adapter

Some computers have a built-in network adapter through which they can be connected to a wired network. To check for a network adapter, look for the network port on the back of the computer, as shown in Figure 1-51. The network ports have eight pins.

To see what kind of network may already be installed on a computer, use the following steps:

1. Click **Start**, then click **Control Panel** (Figure 1-52).
2. Click **Network and Internet Connections** (Figure 1-53).
3. Select a Control Panel icon and then click **Network Connections** (Figure 1-54).

The network adapter will be displayed. If a red cross appears over the icon, it means the network adapter is disconnected (Figure 1-55). If the network connection is blank, then there is no network adapter.

How to Install a USB Network Adapter

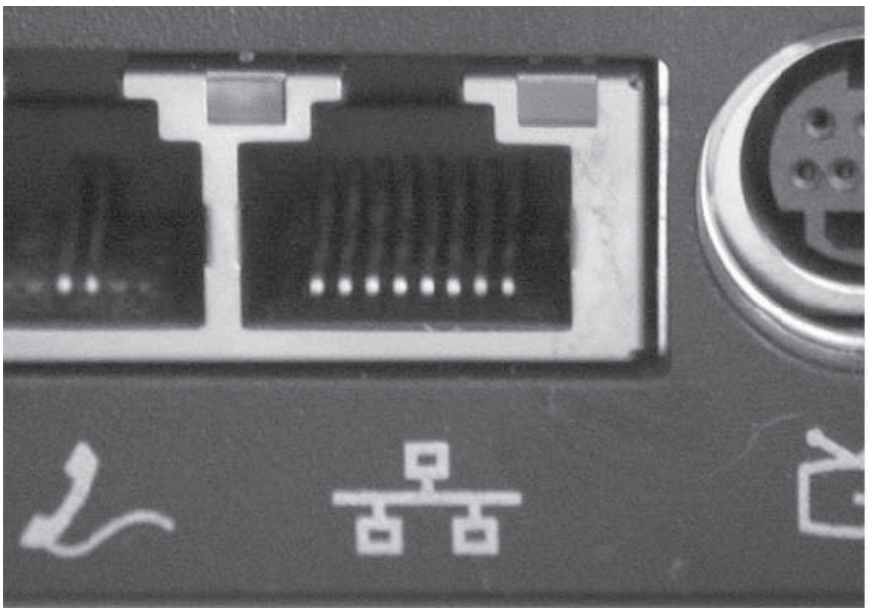
1. If the USB network adapter came with software, insert the CD or floppy disk and follow the manufacturer's instructions to install the software.
2. Find an available USB port on the computer. If there is no unused USB port, connect a USB hub to add additional ports. Then connect the USB network adapter to the unused USB port (Figure 1-56).
3. Connect the network cable to the network adapter (Figure 1-57).
4. Connect the other end of the network cable to the networking equipment (Figure 1-58).

Network Load Balancer

A network load balancer shares Web traffic between Web servers. The Zeus, Apache, and Microsoft Web server environments have basic clustering abilities built in, but software-based load balancing may not be as strong. Hardware load balancers are very expensive, though there are some affordable ones.

Repeaters

A repeater is used to connect two segments on a network cable, as shown in Figure 1-59. This is used to regenerate incoming signals and strengthen the signal without noise.



Source: http://www.microsoft.com/library/media/1033/windowsxp/images/using/networking/setup/68571-ethernet-small.jpg. Accessed 2004.

Figure 1-51 Many computers have built-in network adapters.

In cable systems, repeaters look very simple and consist of an amplifier and a transformer. The purpose of an amplifier is to optimize the reflections of the signal during transmission. In wireless systems, the repeater contains a receiver, an amplifier, a transmitter, an isolator, and two antennas. In a fiber-optic network, a repeater consists of a photocell, an amplifier, and an LED or IRED for amplification. This fiber-optic repeater consumes

Figure 1-52 Click **Start** and then click **Control Panel**.

Figure 1-53 Click **Network and Internet Connections**.

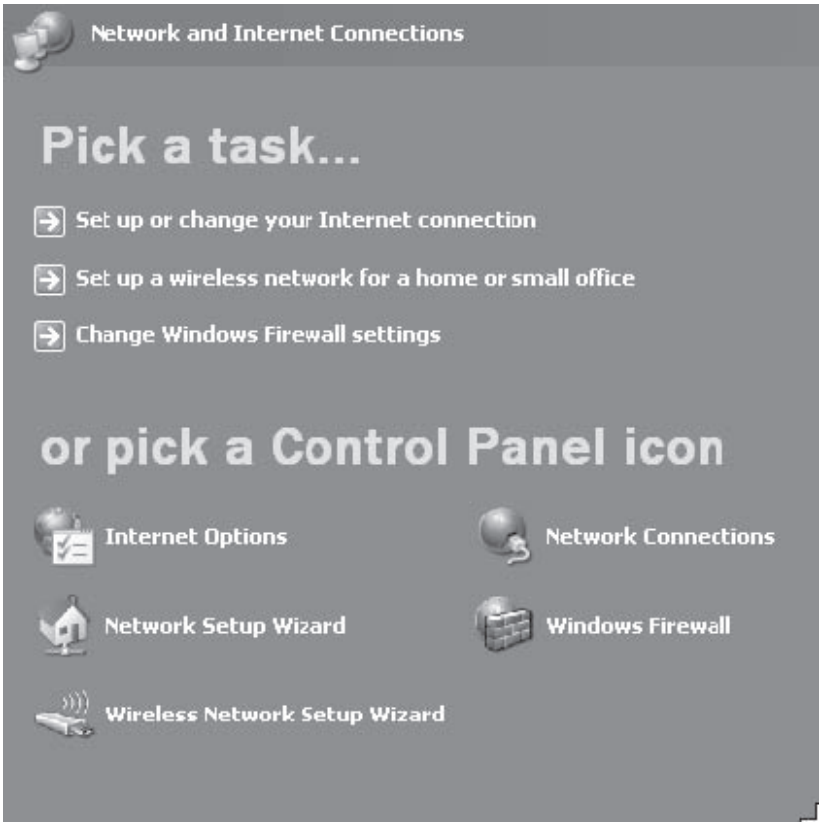


Figure 1-54 Click **Network Connections**.

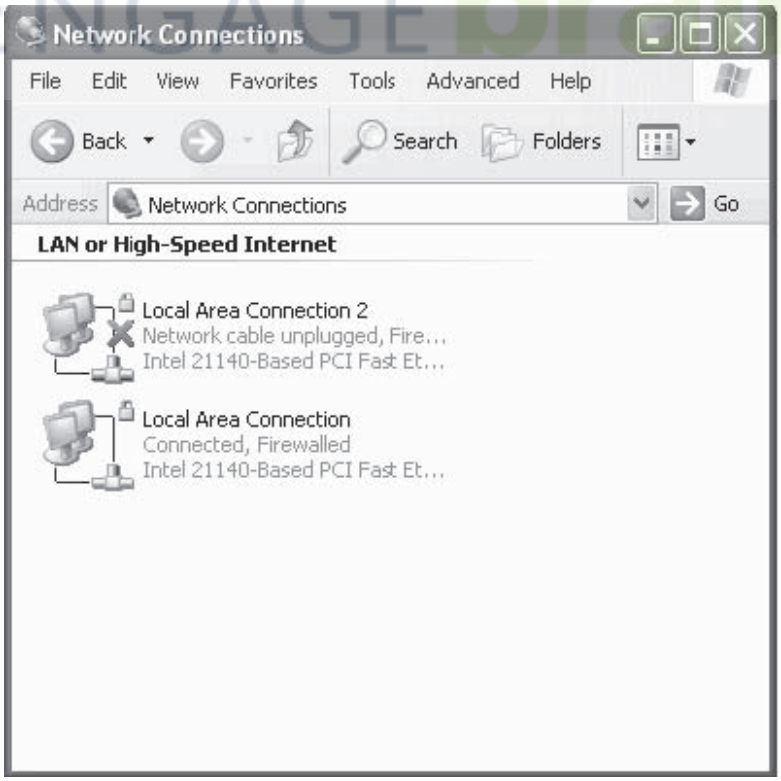
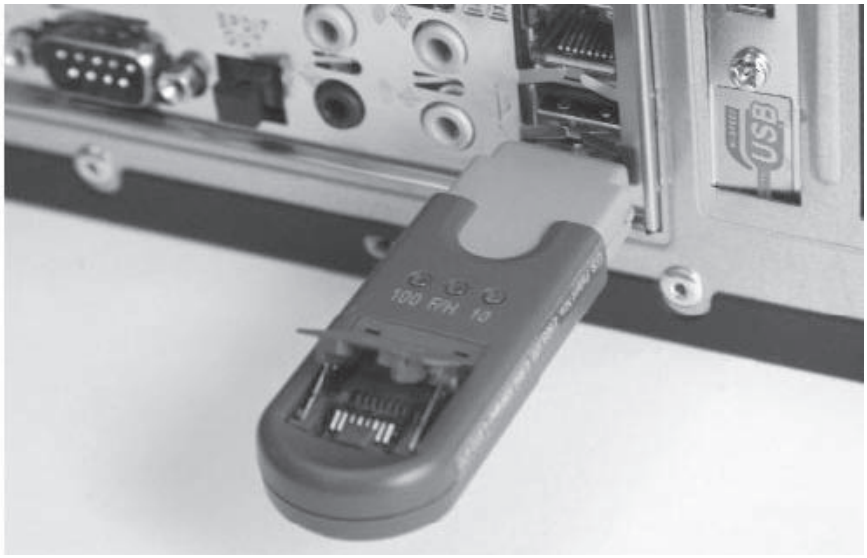
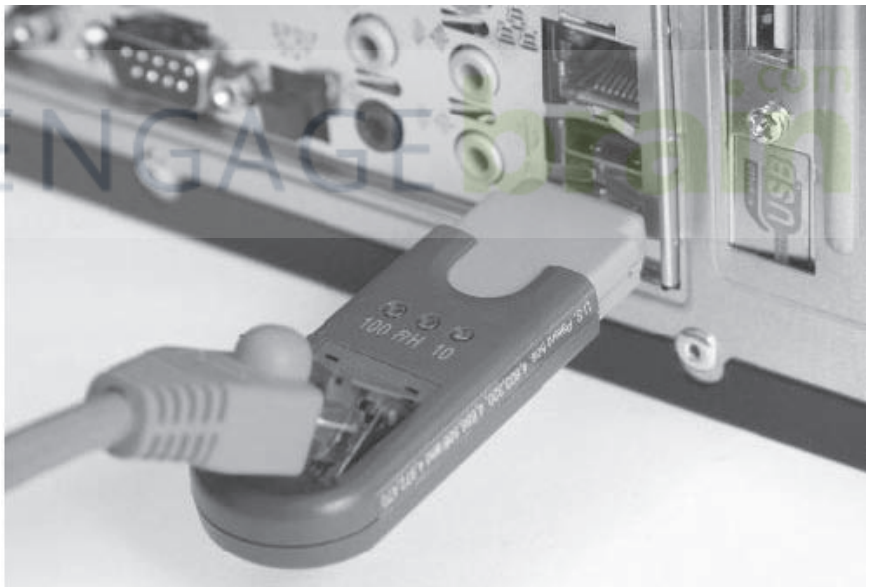


Figure 1-55 If a red cross appears over the icon, then the adapter is disconnected.



Source: http://www.microsoft.com/library/media/1033/windowsxp/images/using/networking/setup/68571-wired-usb-no-cable-small.jpg. Accessed 2004.

Figure 1-56 USB network adapters can be used on most computers.

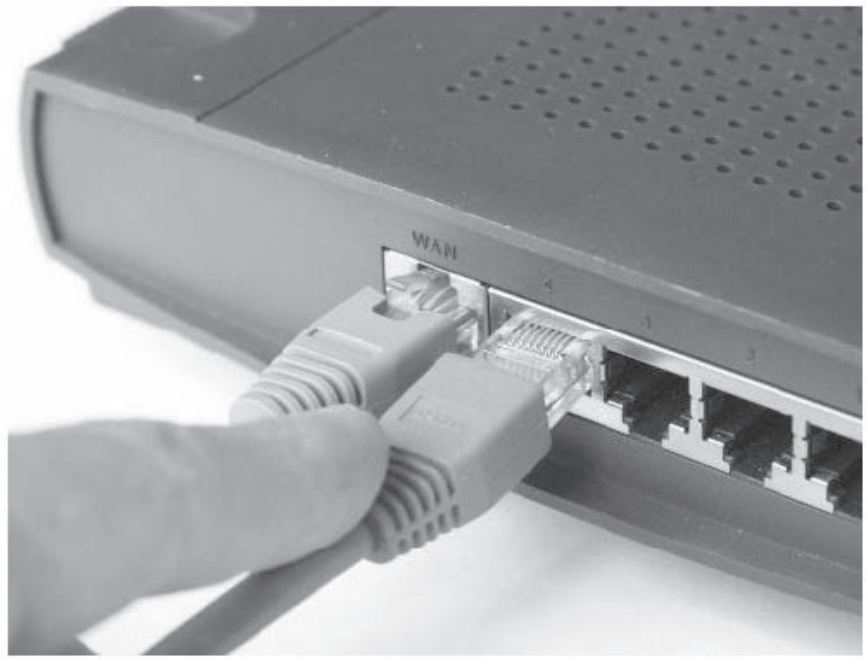


Source: http://www.microsoft.com/library/media/1033/windowsxp/images/using/networking/setup/68571-wired-usb-with-cable-small.jpg. Accessed 2004.

Figure 1-57 Connect the network cable to the adapter.

less power than wireless repeaters. These repeaters are simple and inexpensive. A bus repeater is used to connect one computer bus to another system.

A repeater reproduces the actual bit sequence and places the renewed copy of the signal back on the connection medium. This allows a network to extend farther. A repeater does not alter the operation of the network. A repeater is sometimes compared to an amplifier, which is not accurate. An amplifier cannot differentiate between the original signal and noise. It amplifies all the signals that it produces. A repeater amplifies the original signal only.



Source: http://www.microsoft.com/library/media/1033/windowsxp/images/using/networking/setup/68573-connect-to-router-small.jpg. Accessed 2004.

Figure 1-58 Connect the other end of the cable.

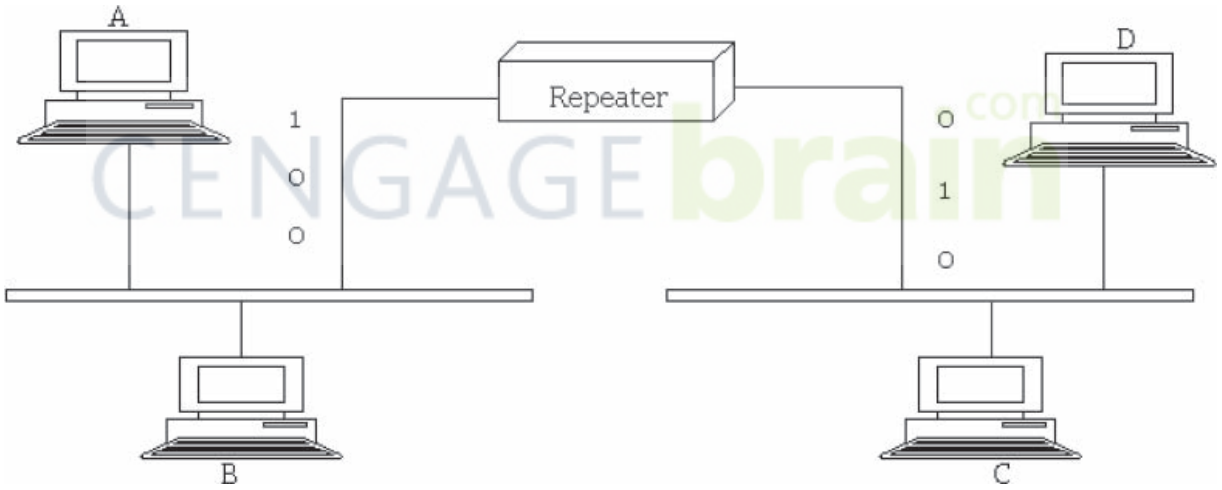


Figure 1-59 A repeater is used to connect two segments on a network line.

The positioning of a repeater is crucial. The repeater must be positioned in a place where signals reach it before any disturbance changes the original bit sequence. A minor disturbance can alter the accuracy of the voltage levels of the bits without corrupting its identity. If such compromised signals travel greater distances, the gathered disturbance can change the entire meaning of the bit sequence. If that happens, the original signal cannot be recovered, and the only way to correct the fault is to resend the signal.

Repeaters have the following advantages:

- Repeaters can increase the physical length of a network by increasing the signal power.
- Repeaters have the capability of transmitting signals through different appended segments.
- Some repeaters join multiple ports and can facilitate data transfer between the different segments of different media.

Repeaters have the following disadvantages:

- Repeaters augment the traffic on the network.
- There are restrictions on the number of repeaters that can be used in a single network.
- Repeaters broadcast errors on the network.
- Repeaters cannot be monitored or controlled through remote access.
- Repeaters cannot filter traffic.

Multiplexer

A multiplexer joins multiple inputs into a single output. In electronics, multiplexers integrate several signals into a single signal. Mutiplexers are useful for transmitting both digital and analog signals. In digital signal processing, a multiplexer uses several isolated data channels and combines them into a single channel. This data channel that is obtained is of higher intensity. The several data channels are transmitted from one place to another over one physical channel, which reduces costs.

At the destination end of the data channel, a counterpart called a demultiplexer, or demux, is generally required to break the high data-intensity stream into the actual lower-intensity streams. In some cases, the distant end system may have more responsibilities than a normal demultiplexer.

In general, it is common to combine a multiplexer and a demultiplexer together into one unit of equipment. Both pieces of equipment are required at both ends of a link, as most channel systems broadcast in both directions.

The following are the two types of multiplexing:

1. Frequency-division multiplexing
2. Time-division multiplexing

Gateway

A gateway is a device that is used to connect two different networks. A gateway allows users to protect, share, store, and access data over a network.

Gateway devices have two major functions:

1. *Connecting devices with each other*: In this function gateway devices help the users to connect different PCs and allow it to connect a printer and a scanner.
2. *Connecting devices to other networks*: Gateways connect devices and also connect devices to public and private networks.

Gateways are divided into three functional categories:

1. Data gateways
2. Multimedia gateways
3. Home-control gateways

Transceivers

A transceiver is a network device that is both a transmitter and a receiver. The transmitter transmits analog or digital signals, and the receiver receives analog or digital signals. Transceivers are available in three different configurations:

1. A chip-style device is the smallest type of transceiver that can be easily fixed and removed from a network system.
2. Board-style devices are directly fixed to a network board or card.
3. A module-style device is an external transceiver that is fixed outside the network and functions similarly to a standalone device.

Converters

Converters are used to connect several types of cables within an existing network. They get data from one type of cable and convert the signal for analog transmission on the other type of cable. Usually, network media converters are used to connect newer gigabit (1000 Mbps) Ethernet cabling to older 10Base-T or 100Base-T

networks. Some types of network media converters are separate devices that convert data between two different media. Others types are chassis-based models that are used to connect several media types in a single housing. These chassis-based devices are modular, stackable, and rack mounted. They contain an uplink or crossover switch to permit connections to either a workstation or a hub without the use of a cross-pinned cable.

Network media converters with an integrated circuit (IC) or printed circuit board (PCB) form factor are also available. The type of the network is important when choosing network media converters. Common types of networks contain asynchronous transfer mode, Ethernet, Token Ring, optical carrier, single-mode fiber, and multimode fiber. Choosing network media converters requires an analysis of port connectors. Attachment unit interface (AUI) connectors are used to connect Ethernet network stations and transceivers.

Terminals

Terminals are hardware devices used to enter data into a computer or to display data from the computer. Older terminals had a typewriter keyboard for input and a printing device for alphanumeric output. Newer variants contain a keyboard for input and a television-like screen for displaying the output.

Chapter Summary

- A network is a group of computers connected together so that information can be exchanged among the computers.
- A backbone combines many networks and subnets into a single channel.
- Large networks are divided into segments to improve the performance of the network.
- A subnet is a logical grouping of the devices in a network.
- The IP address space is divided into Classes A, B, C, D, and E.
- A gateway is a node that routes traffic from one workstation to an outside network on the Internet.
- There are three primary types of network cables: twisted-pair, coaxial, and fiber-optic.
- Operations security (OPSEC) identifies, controls, and protects generally classified or sensitive information.
- The OSI reference model is a standard networking model with seven layers.

Review Questions

1. What is a network backbone?

_____

_____

_____

_____

2. What is a subnet?

_____

_____

_____

_____

3. How are IP addresses assigned?

_____

_____

_____

_____

4. Name three domain naming conventions.

5. What are the types of threats to DNS?

6. What is a data gateway?

7. What are the types of twisted-pair cables?

8. What is a coaxial cable?

9. What are the types of wireless transmission?

10. What is Token Ring?

11. What is polling?

12. What are the layers in the OSI model?

13. Explain the flow of data in transmission modes.

14. Describe client-server networking.

15. Describe star topology.

Hands-On Projects

1. Perform the following steps:
   - Navigate to Chapter 1 of the Student Resource Center.
   - Open Asynchronous Transfer Mode Fundamentals.pdf and read the content.
2. Perform the following steps:
   - Navigate to Chapter 1 of the Student Resource Center.
   - Open What Is A LAN.pdf and read the content.
3. Perform the following steps:
   - Navigate to Chapter 1 of the Student Resource Center.
   - Open Lan Guide.pdf and read the content.