Major
Training Report
At
Smriti Netcom Pvt. Ltd.

Submitted By:

Gaurav Mendiratta

VII SEM
ELECTRONICS & COMMUNICATION
UNIVERSITY INSTITUTE OF TECHNOLOGY
BHOPAL

ABOUT THE COMPANY

Smriti Netcom, a company engaged in imparting customized comprehensive training and providing trained engineers for networking projects and for the projects on IP telephony. Engineers trained at Smriti Netcom, on the above subject are trained by US based technical trainers or by US trained India based trainers as per the customer's requirement. However, in either case the training is imparted on the systems and methodology adopted by renowned American training firms, using audio video systems and slides.

In today's fast growing technical market place, powerful IT Solutions are required in the shortest possible time. Global deregulation and emerging broadband standards have served as catalysts for the convergence of voice data and video, ultimately creating new opportunities for IT companies in the areas of computer telephony and equipment manufacturers. These advancements in technology, especially in the field of networking, paved the way for **Smriti Netcom** (S-Net), a company with specialized focus on systems integration, delivering quality solutions in area of IT enabled services, remote services or teleservices, constituting a broad gamut of technologies enabling information delivery services.

S-Net was founded in January 2001 by **Mohammed Alavi** , CEO & **Vivek Dhawan**, CTO who shared the same vision. Both Mohammed & Vivek have more than 5 years of experience in developing & designing Networking Solutions & Providing High-End Networking Training.

Smriti Netcom offers integrated planning and implementation, including co-ordination of organizational initiatives, human resources and training plan, design process, re-engineering, technical specification, vendor selection and facility design.

It offers one of the most comprehensive product lines, providing :-

CONSULTANCY
LAN SOLUTIONS
SYSTEM INTEGRATION
APPLICATION DEVELOPMENT
TRAINING
WAN SOLUTION
VPN SOLUTION
SYSTEM RELOCATION
BUSINESS RECOVERY
MAINTENANCE & SUPPORT

Smriti Netcom has added a new dimension by introducing for the **FIRST TIME IN INDIA** a **Professional Training Program in 'VOIP/IP Telephony / IP-TV** for busy networking professionals. As we are aware that w.e.f. 1st April, 2002 the Govt. of India is permitting voice over internet protocol (Internet Telephony) to all long distance telephone carriers. Some of the companies like BTNL, BSNL, Birla-AT&T & Reliance have even got license for the same. The training program mentioned above will be extremely beneficial for your company as it will facilitate you to provide solutions to your customers.

INTRODUCTION

We began our training with learning how to assemble a Personal Computer then ,learnt definitions of common networking terms, and then describe types of network servers and networks. Next, we reviewed types of communications methods and the OSI reference model. Then we took an overview of the IEEE standards for Ethernet and Token Ring networks and discussed the NDIS and ODI network standards. Then we learned about the connectivity devices, protocols and WAN connection Services. We went through a disaster recovery plan and methods for resolving any hardware conflicts and naming the schemes for the computers on the network. We also got training on LAN Setup, User/Group Administration and Managing Network Servers like DHCP, DNS and WINS.

Taking Up all these in detail:

ASSEMBLING OF PERSONAL COMPUTER

General requirement :
When handling or working near static sensitive PCBA's / HDAs / Drives always wear an ESD wrist strap worn directly contacting the skin (not over the gloves) and attached to an ESD mat or properly grounded work bench.
At the beginning of each shift , the operator is instructed to test the condition of the ESD wrist strap.

Cabinet preformation :

Ensure that the power supply unit , is installed on the cabinet with all supporting screws.

Check that the voltage setting switch is set to 230VAC if this setting switch is available.

Mother board assembly :

Place plastic spacers in the oval apertures. If the motherboard chasis does not have pre-fixed metal spacers , place and thread the metal spacers into the circular apertures.

Align the key board connector end of the motherboard with the rear end of the chasis identified by several rectangular slots.

Ensure that all spacers placed have their corresponding apertures on the motherboard .If less , remove extra spacers or if more , provide additional spacers.

Fit the motherboard using screws\ plastic locks. Do jumper \switch settings as per motherboard layout \ manual and configuration.

CPU INSTALLATION :
Take cpu as per configuration , if cpu is without fan\heatsink ,fit fan \ heatsink with cpu with locks.
Install cpu supporting kit (Retention Mechanism) on the cpu slot on the motherboard with metal screws \ plastic locks.

Fit the cpu in to the cpu slot on the motherboard and lock the cpu. Connect cpu cooling fan connector with the cpu fan connector on the motherboard. (cpu cooling fan is not require for the BIG heatsink).

Memory module installation :
Insert memory module on the memory slot of the motherboard firmly , as per configuration. Ensure that the memory module is properly installed.

Floppy Disk Drive assembly :
Take Floppy disk drive as per configuration , check it for any damages.
Fit the Floppy disk drive with four screws on its location in the cabinet. Ensure that the front of the floppy disk drive is align with the front of the cabinet.

Hard Disk Drive assembly:
Take Hard disk drive from HDD copying station as per configuration & check it for any damages. Fit the Hard disk drive with four screws on its location in the cabinet. Ensure that the hard disk drive is properly fixed.

Cd-Rom Drive assembly :
Take Cd-Rom drive as per configuration , check it for any damages. Fit the Cd-Rom drive with four screws on its location in the cabinet .Ensure that the front of the Cd-Rom drive is align with the front of the cabinet.

Front panel connector assembly :
Connect the front pannel connectors onto the motherboard as indicated on the mother- board \ manual . Tidy up the cables with cable ties.

Data cable connection :
Connect the data cables for Floppy disk drive , Hard disk drive and Cd-Rom drive onto the motherboard \ controller card. Tidy up the cables.

Power supply unit connection with drives \ board :
Connect the power supply cables of the power supply unit on to the motherboard connectors , Floppy disk drive p/s connector , Hard disk drive p/s connector , Cd-Rom drive p/s connector.

Connect audio signal connector between cd-rom audio connector and cd audio in connector on sound card \ motherboard (with on board sound) for system with cd-rom drive and sound. Tidy up the cables with cable ties.

Ports fitment (for mother boards with out external port connector) :
Fit the port brackets on cabinet with screws and connect data cables on the motherboard. Tidy up the cables with cable ties.

Procedure for installing VGA \ AGP (display card) card as per configuration :

Mount the Vga \ Agp card on to the slot on the motherboard. The slot to be used will be advised by the Engineer on a case to case basis. Secure the Vga \ Agp card with screw.

Procedure for installing Sound card as per configuration :

Mount the sound card on the slot on the motherboard. The slot to be used will be advised by the Engineer on a case to case basis. Secure the sound card with screw.

Procedure for installing Ethernet \ Lan card as per configuration :

Mount the Ethernet \ Lan card on the slot on the motherboard. The slot to be used will be advised by the Engineer on a case to case basis. Secure the Ethernet \ Lan card with screw.

Device Driver checking and installation :

Make all connection & switch ON the pc-system. Do CMOS-SETUP as per sample given and pc-system configuration. Enter current date & time.Save CMOS-SETUP & exit the setup. After display comes switch OFF the pc-system.

WINDOWS 95/ WINDOWS 98 O S LOADING\DRIVER CONFIRMANCE:

Make all connection & switch ON the pc-system .Allow pc-system to boot from the Hard Disk Drive .Check for start up sound for Multi-Media pc-system .Check for all drivers (as per pc-system configuration) loaded in the pc-system . If any driver is missing then load appropriate driver. Check for all device resource setting .

Check 1024 x 768 bit with High color resolution .Play audio -CD for Multi-Media pc-system .Check lan connectivity for pc-system with lan card only.

Check MODEM detection for pc-system with fax/modem card only. Shut down the pc-system & remove all connection. Send pc-system for BURN IN. After Burn-In the two tests are performed.

DEFINING NETWORKING TERMS

We studied about the common terms in four categories: network description, network topology, network protocol, and networking service.

Network Description Terms

The following are the terms commonly used when describing a network, beginning with the most basic one:

Network: A group of interconnected computers that share resources and information. For example, some hardware resources typically shared on a network are printers, fax-modems, and hard disks.

Transmission media: The physical pathway on which the computers are connected. Cable and wireless media can connect the computers in a network.

Stand-alone computer: A computer that is not connected to a network.

Local area network (LAN): A group of computers interconnected within a building or campus (see Figure I.I). For example, a LAN may consist of computers located on a single floor of a building or it might link all the computers in a small company.

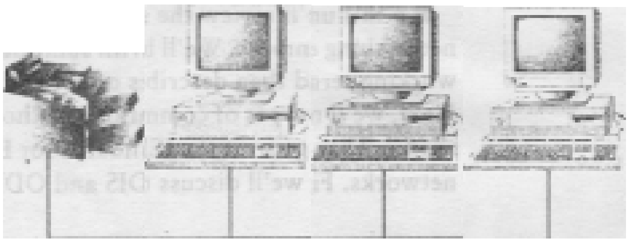


FIGURE 1.1: An example of a local area network (LAN)

Metropolitan Area Network (MAN) : A network of LANs that covers a city or large campus environment (see Figure 1.2).

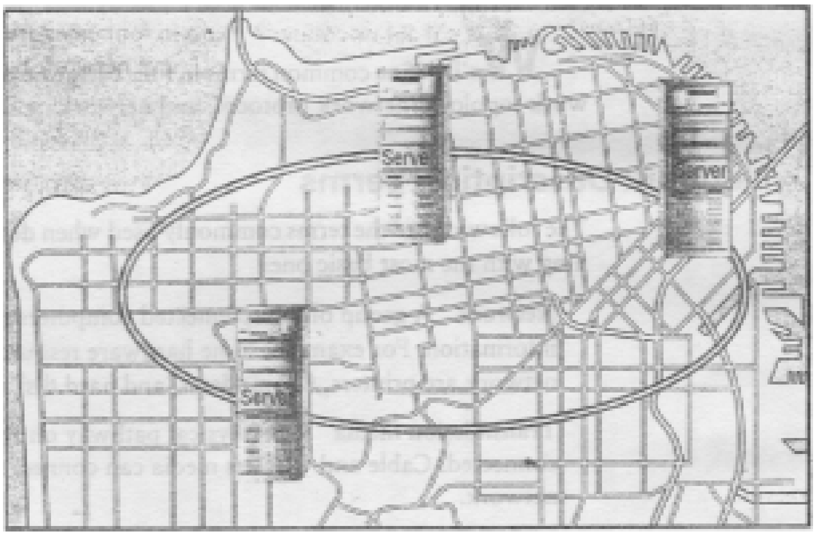


FIGURE 1.2 An example of a metropolitan area network (MAN)

Wide Area Network (WAN): A network consisting of computers or LANs connected across a distance using different physical topologies, such as telephone lines, fiber-optic cabling, satellite transmissions, and microwave transmissions

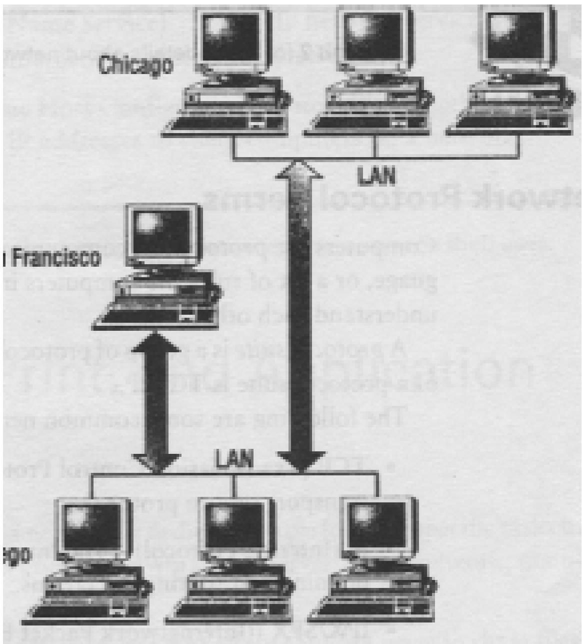


FIGURE 1.3: AN EXAMPLE OF WIDE AREA NETWORK (WAN)

Network Topology Terms

Network *topologies* are the physical cable or transmitters on the network.The following are the different types of physical topologies:

Bus: All computers are connected with a single cable with a terminator one ach end. An example is an Ethernet network connected with Thinnet coaxial (IOBase2) cable.

Star: All computers arc connect to a central device, typically a hub or switch. An example is an Ethernet network connected with twisted-pair (lOBaseT) cable.

Ring: All computers or network devices are attached directly to each other in a ring fashion. An example is an FDDI (Fiber Distributed Data Interface) network, where all the hubs connect to each other in a ring.

NETWORK PROTOCOL TERMS:

Computers use *protocols* to communicate with each other. A protocol is a language, or a set of rules the computers in a network need to follow in order to understand each other. A *protocol suite* is a group of protocols that are loaded together. An example of a protocol suite is **TCP/IP**.

The following are some common network protocols:

TCP (Transmission Control Protocol): The Internet protocol suite's transport service protocol.

IP (Internet Protocol): The Internet protocol suite's protocol for defining and routing datagrams.

IPX/SPX ((Internetwork Packet Exchange/Sequenced Packet Exchange): Routable protocols created by Novell for NetWare networks.

NetBEUI (NetBIOS Extended User Interface): A protocol created by IBM for small workgroups.

HTTP (Hypertext Transfer Protocol): The WWW (World Wide Web) protocol used to transfer Web pages across the Internet.

Networking Service Terms

The following are three terms related to TCP/IP networking services:

WINS (Windows Internet Name Service): A TCP/IP network service for Microsoft networks that resolves NetBIOS names and facilitates browsing across subnetworks.

DNS (Domain Name Service): A TCP/IP network service that translates host names to Internet Protocol (IP) addresses.

DHCP (Dynamic Host Configuration Protocol): A method for automatically assigning IP addresses to client computers on a network.

Comparing File, Print, and Application Servers

A server in a network is dedicated to performing specific tasks in support of other computers on the network. In a server-based network, not all servers are alike:

File servers-offer services that allow network users to share files. File services include storing, retrieving, and moving data. File and print servers do not do processing for the client computers.

Print servers manage and control a single printer or a group of printers on a network. The print server controls the queue or spooler. Clients send print jobs to the print server, and the print server uses the spooler to hold the jobs until the printer is ready.

Application servers allow client PCs to access and use extra computing power and expensive software applications that reside on a shared computer. Application servers offload work from the client by running programs for the client and sending the results back to the client. For example, when a client asks a Microsoft SQL Server to find a record, SQL Server does all the processing to find the answer, and then sends the results back to the client.

Running applications from an application server rather than from separate client machines can reduce your licensing costs. With this setup, we can purchase licenses for every connection to the application. For example, if you have 100 users but only 50 users use the application at a time, you would buy a 50-user license.

File, print, and application services are the main services that servers provide. Although you can dedicate a server to a particular service, such as having a computer that serves only as a print server, you do not need a different server for each type of service. One server can function as a file, print, and application server.

Comparing Client-Server and Peer-to-Peer Networks

There are three roles for computers in a network:

- A c*lient* is a workstation used only to request services from a network service provider, such as a dedicated server or another workstation
- A *server* provides services to service requestors (see Figure 1.4).A *dedicated* server functions only as a server; it is not used as a client or workstation. The use of a dedicated server is recommended for networks with more than ten clients.
- A *peer* both requests and provides network services.

In a server-based *(client-server)* network, a dedicated server is used to provide services to clients. For example, the server might provide file, print, message, database, and application services to the clients in the network.

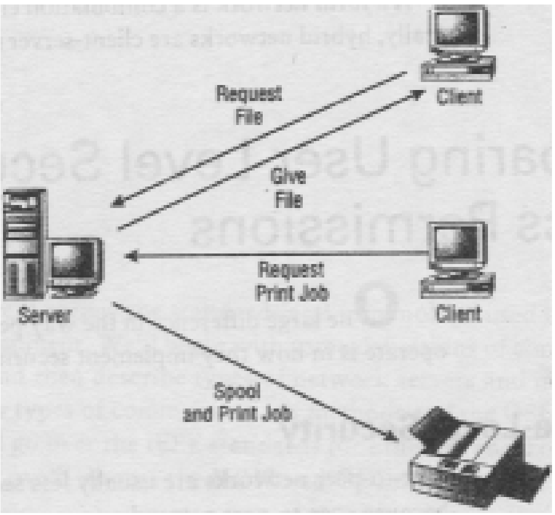


FIGURE 1.4: A server provides services to service requestors

In a peer-to-peer network, each computer is equal (peer) in the sharing of resources (see Figure 1.5). A peer-to-peer network does not have a dedicated server, and there is no hierarchy among the computers. Each peer is responsible for its own security. Usually, the computer users determine what data on their computer will be shared on the network.

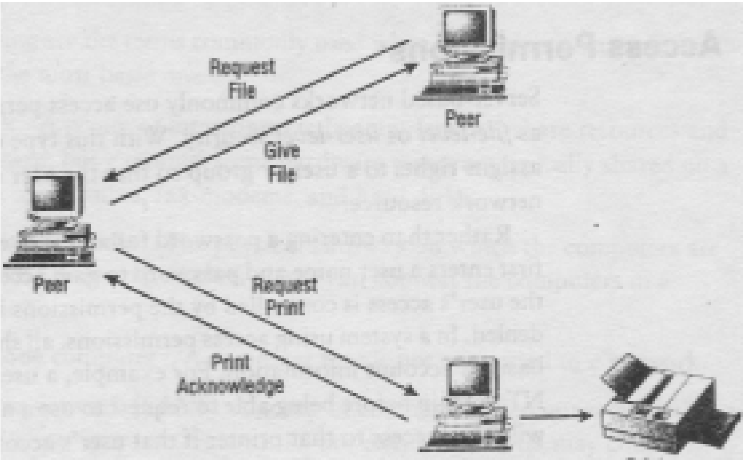


FIGURE 1.5: An example of a peer- to-peer network

A *hybrid* network is a combination client-server/peer-to-peer network. Typically, hybrid networks are client-server networks that also include some peers.

Comparing User-Level Security with Access Permissions

One large difference in the way peer-to-peer and server-based networks operate is in how they implement security.

Share-Level Security

Peer-to-peer networks are usually less secure than server-based networks because peer-to-peer networks commonly use *share-level security,* also known as *password-protected security.*

With share-level security, each network resource can be assigned a password. For example, on a Windows 95 system, you can assign a password to a certain directory. Then, before a user can gain access to that directory, he or she must enter the correct password. Share-level security can be used with both FAT and NTFS partitions. This type of security works at the directory (folder) level, which means that it applies to all the files within the specified directory.

Access Permissions

Server-based networks commonly use access permission security, also known as *file-level* or *user-level* security. With this type of security, an administrator assigns rights to a user or group so that the user or group can access a certain network resource.

Rather than entering a password for access to each shared resource, the user first enters a user name and password to gain access to the network itself. Then the user's access is controlled by the permissions he or she has been granted or denied. In a system using access permissions, all share access is evaluated on the basis of account information. For example, a user must log on to a Windows NT domain before being able to request to use a network printer, and that user will have access to that printer if that user's account has permissions for that network resource. Access permission security works only with NTFS partitions and can apply to individual files.

Comparing Connection-Oriented with Connectionless Communications

There are two ways that communication between computers can be arranged: connectionless methods and connection-oriented methods.

Connectionless Communications

Connectionless methods do not guarantee delivery, and thus are faster than connection-oriented methods. An analogy is using the postal service to send a postcard or letterit will probably get to its destination but there is no guarantee.

Examples of protocols that use connectionless communications are IP (Internet Protocol), UDP (User Datagram Protocol), and IPX (Internetwork Packet Exchange).

Connection-Oriented Communications

Connection-oriented methods guarantee delivery, but they are slower than connectionless methods. An analogy is sending a registered letter, where extra steps are taken to ensure that it arrives at its destination.

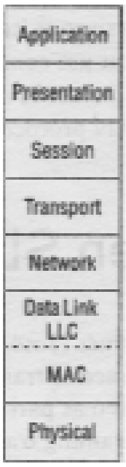
Distinguishing between SLIP and PPP

SLIP (Serial Line Internet Protocol) and PPP (Point-to-Point Protocol) are two common protocols used to transmit IP packets over serial line and telehone connections, most often as part of a dial-up Internet connection. SLIP, the original serial framing transport for TCP/IP, and PPP, the newer serial protocol, are similar. There are, however, some key differences that make PPP a more efficient and secure transport option. Table I.I shows these differences.

SLIP	PPP
Supports TCP/IP only	Supports multiple protocols
Does not provide error checking for bad frames (very little overhead)	Provides error checking for each frame (more overhead)
Requires manual IP addressing	Provides dynamic addressing
Does not support encrypted authentication	Supports encrypted authentication, both login and password

Defining Communications at the OSI Model Levels

There are seven layers that define the OSI reference model (see Figure 1.7). Table 1.2 lists the layers, from bottom to top.



File, Print, Message, Database, and Application Services

Data Translation

Dialog Control

End to End Connection

Routing

Error Correction

Framing

Responsible for Sending 1s and 0s Between Hosts

FIGURE 1.7: The OSI reference model and its functions

T ABLE1.2
OSI Reference Model Layer

LAYER	FUNCTION	COMMUNICATION
Physical	Handles sending bits (ones and zeros from one comouter to another.	Hubs, switches, repeaters, cables connectors, trans mitters, receivers multiplexers
Data Link LLC sublayer MAC sublayer	Provides for the flow of data over a sinale link from one device to anothel	Switches, bridge' intotUriont liilltC
Network	Makes routing decisions and forwards packets (also known as *datagrams)* for devices that could be farther away than a single link	Routers, brouters fiatout/au coruiriat
Transport	Ensures that packets are delivered error-free, in sequence, and without losses or duplication	Routers, brouters gateway services
Session	Allows applications on separate computers to share a connection (called a *session)*	Application interfaces, gateways
Presentation	Translates data between the formats the network requires and the formats the computer expects	Application interfaces, gateways
Application	Provides services that directly support user applications, such as database *access email* and file transfer	Application interfaces, gateways

The Application, Presentation, and Session Layers

The top three layers in the OSI reference model Application, Presentation, and Session deal mostly with functions that aid applications in communicating with other applications. They specifically deal with tasks like filename formats, code sets, user interfaces, compression, encryption, and other functions that relate to the exchange occurring between applications.

The Transport and Network Layers

The middle layers in the OSI reference model Transport and Network deal with the logical transmission of data. They take care of the sizing of packets, also called *datagrams'* sent and received from each application, and then handle the routing of those packets. These layers also set the degree of reliability for packets reaching their destination and the logical addressing of each machine.

Several connectivity devices work at these levels:

Gateways can rebuild a complete protocol stack, as explained in the description of the upper layers. If you are running a TCP/IP network and want to communicate with an IPX network, you need a gateway to be able to communicate between the two networks.

Routers route packets through an intranetwork and the Internet. A router is a lot like a postman; he needs to know all the streets to be able to deliver mail. A router keeps track of all the network segments and communicates this information with other routers.

Brouters are used when you have move then one type of protocol on your network, but one of the protocols is not routable. For example, the Net-BEUI protocol cannot be routed, so it would be bridged instead. Brouters are typically run with software in a router.

The Data Link and Physical Layers

The bottom layers in the OSI reference model Data Link and Physical handle the physical transmission of data. They take what is passed down to them and put it into a format that can be sent over a variety of physical transmission media.

The Data Link layer, which packages the data units into *frames,* is divided into two sublayers:

LLC (Logical Link Control): Top sublayer; establishes and maintains links between communicating devices. This sublayer is also responsible for frame error correction and hardware addresses.

MAC (Media Access Control): Bottom sublayer; controls how devices share a media channel. There are two main methods:

With *contention,* all devices attached to the network can transmit whenever they have something to communicate. Ethernet is an example of a contention network.

With *token passing,* computers on the network cannot transmit onto the network cable until they are given a frame or token. Token Ring, ARCnet, and FDDI arc examples of networks that use token-passing media access.

Some of the hardware devices that communicate at the Data Link and Physical layers are hubs, switches, repeaters, cables, connectors, transmitters, and receivers. Also, *bridges,* which are devices that connect network segments, operate at the Data Link layer. Bridges can selectively determine the appropriate segment that should receive a signal, and they are used with nonroutable protocols, such as NetBEUI.

Defining the Media Used in IEEE 802.3 and IEEE 802.5 Standards

In February 1980, the Institute for Electrical and Electronic Engineers, Inc.(IEEE) formed a project called project 802 (after the year and month) to helpdefine certain Standards. The 802 specifications fall into 12 categories that areidentified by the 802 numbers:

802.1	Internetworking and Management
802.2	Logical Link. Control
802.3	Carrier Sense with Multiple Access and Collision Detection(CSMA/CD or Ethernet)
802.4	Token Bus LAN
802.5	Token Ring LAN
802.6	Metropolitan Area Network (MAN)
802.7	Broadband Technical Advisory Group
802.8	Fiber-Optic Technical Advisory Group
802.9	Integrated Voice/Data Networks
802.10	Network Security
802.11	Wireless Network
802.12	Demand Priority Access LAN, lOOBaseVG-AnyLAN

IEEE 802.3 (Ethernet) and 802.5 (Token Ring) are the most commonly used standards for physical and logical topologies.

Ethernet

The Ethernet protocol implements a logical bus network that can transmit at 10 or lOO Mbps. Every computer receives the information, but only the intended destination acknowledges the transmission.

CSMA/CD

Ethernet uses the CSMA/CD access method to share network media. The CSMA /CD protocol can be broken down as follows:

CS (Carrier Sense)

Before transmitting, listen for a signal; if none is found, it is okay to transmit.

MA (Multiple Access)

All computers share the same cable and signaling techniques.

CD (Collision Detect)

Detect collisions, wait, and retransmit.

Ethernet Cabling Systems

There are four commonly used Ethernet cabling systems, which are listed in Table 1.3.

TABLE 1.3
Ethernet Cabling

CABLE	DESCRIPTION
10Base5	Also known as RG-8 or Thicknet coaxial cable; carries signals up to 500 meters (1640 feet) at 50 ohms
10Base2	Also known as RG-58 or Thinnet coaxial cable; carries signals 185 meters (607 feet) at 50 ohms
lOBaseT	Also known as twisted-pair; the most popular of alt Ethernet topologies, categories include 3, 5, and 6 (UTP, or unshielded twisted pair) cable at up to lOOMbps speeds; carries signals up to 100 meters (330 feet)
lOOBaseT	Also known at twisted-pair; uses category 5 for speeds up to lOOMbps and category 6 for speeds up to 155Mbps; carries signals up to 100 meters (330 feet)

802.5: TOKEN RING

Token Ring is a logical ring network that looks like a star network (because the ring is actually formed inside a central hub). Token Ring devices can transmit at 4Mbps or 16Mbps.

Hubs in a Token Ring network are called MSAUs or MAUs (both for multistation access units).

TOKEN PASSING

Token Ring networks use token passing to determine who may transmit at any one moment. Unlike an Ethernet network, computers in a Token Ring network can transmit only when they receive a frame known as a *token.* The token goes around the logical ring, and only the computer that has the token can transmit. Since the computer must have a token before transmitting, no collisions occur.

Active monitors, sometimes referred to as *token masters'* are in charge of keeping track of where the token is and making sure that there is only one token on the network at a time.

Token Ring is a very resilient network. Network interface cards in Token Ring networks can run diagnostics on themselves and take themselves off and on the network.

TOKEN RING CABLING TYPES

Standard Token Ring cable types for include Types I through 6, 8, and 9, as listed in Table 1.4.

TABLE 1.4

CABLE	**DESCRIPTION**
	STP (shielded twisted-pair), used to connect terminals and distribution panels
	STP, used to connect terminals located in the same physical area or room
	UTP (unshielded twisted-pair), which has four pairs, each twisted two times for every 3.6 meters (12 feet) of length
	Optical cable used only on the main ring path
	STP that does not carry signals as far as Type 1 or 2, used as patch cable or extensions in wiring closets
	Used for runs under carpets
	Plenum-rated, used for runs in ceilings

UNDERSTANDING NDIS AND NOVELL ODI STANDARDS

Co*mpu*___ter___ users want to able to load multiple protocols on their work- station but install only one network interface card. The solution to this problem is driver interfaces, which allow multiple cards to be bound to multiple transport protocols. Two such driver interfaces exist: NDIS and ODI.

NDIS

In Windows NT, Windows 95, OS/2, and Windows for Workgroups, the network driver is implemented by NDIS (Network Driver Interface Standard) 3.0. NDIS is a small code wrapper that controls the interface between NDIS-compliant drivers and transport protocols. NDIS 3.0 allows multiple adapter drivers to be bound to an unlimited number of transport protocols.

ODI

ODI (Open Data Link Interface) was developed by Apple and Novell to simplify driver development and to provide support for multiple protocols in a single network adapter card. Similar to NDIS, ODI allows Novell NetWare drivers to be written without concern for the protocol that will be used on top of them.

Token Ring Cabling Type 1

Type 2

Type 3

Type 5
Type 6

Type 8

Type 9

SELECTING THE APPROPRIATE MEDIA

Computers must communicate through some form of transmission media. The most common types of media are twisted-pair and coaxial cable (copper media), followed by fiber-optic cable (glass media). Wireless media include radio wave, microwave, and infrared. These types are still much slower than copper of glass media, but they are the most suitable choice for certain situations.

First we will look at an overview of communication technologies and the problems that degrade transmissions through various types of media. Then we will review the specific characteristics of different media.

Communication Technologies

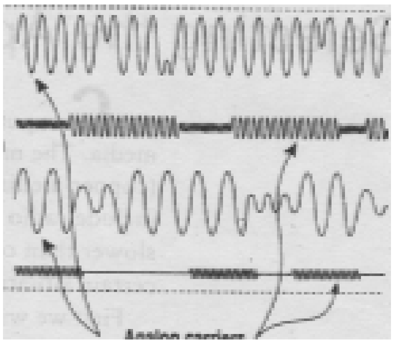
The following are some technologies that apply to communications:

Broadband transmission enables two or more communication channelsto share the bandwidth of the transmission media (see Figure 2.1). Broad band.networks can simultaneously accommodate video, voice, and data.ISDN is an example of a WAN communication service that can provide broadband transmissions.

Bandwidth is basically the difference between the highest and lowest frequencies in a given range. This refers to the capacity of the media. The greater the bandwidth, the faster the data-transfer capabilities. For example, Ethernet has a bandwidth of 10 megabits per second (Mbps) and Token Ring has a bandwidth of either 4Mbps or 16Mbps.

- *Baseband transmission* uses digital signals over a single frequency (see Figure 2.1). With baseband transmission, the entire communication channel capacity is used to transmit a single data signal. Most LANs use baseband technology.

Broadband



Analog carrier
Figure 2.1 :Broadband And Baseband Technology

- *Multiplexing* divides a transmission facility into two or more channels (see Figure 2.2). The two main ways to sha " a channel are time-division multiplexing (TDM) and frequency-division multiplexing (FDM). *Demultiplexing* recovers the original separate channels from a multiplexed signal. A *multiplexer,* also called a *mux,* can perform both multiplexing and demultiplexing.

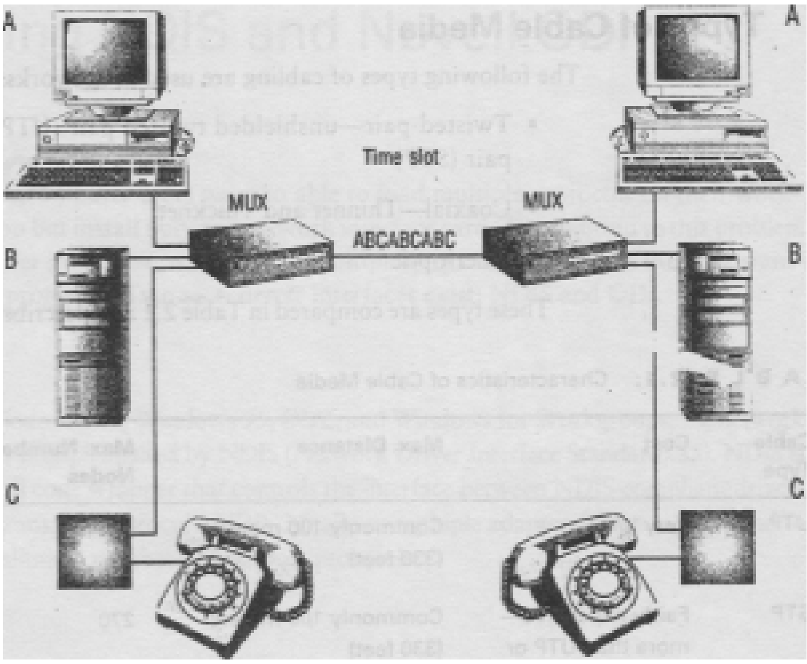


FIGURE 2.2 Multiplexing and demultiblexing

TRANSMISSION DEGRADATION

Depending on the media type, the following problems can affect the quality of transmissions:

- *Attenuation* refers to loss of signal as it goes through the transmission medium, measured in decibels (dB).

- *Electromagnetic interference* (EMI) is electrical background noise that disturbs or distorts a signal as it travels down the 'transmission media. Fiber-optic cable is usually immune to EMI because it uses light rather than electronic signals to transfer data.

- *Crosstalk* is a form of EMI caused by wires next to each other interfering with signals as they travel through the transmission media.

- *Dispersion* applies to fiber-optic cables. Chromatic dispersion occurs when light enters the core at different angles and spreads apart slightly as it travels to the destination.

TYPES OF CABLE MEDIA

The following types of cabling are used in networks:

- Twisted-pair unshielded twisted pair (UTP) and shielded twisted pair (STP)

- Coaxial-Thinnet and Thicknet

- Fiber-optic

These types are compared in Table 2.1 and described in the following sections.

TABLE 2.1 Characteristics of Cable Media

CABLE TYPE	COST	MAX. DISTANCE	MAX. NO. OF NODES	COMMON USAGE
UTP	Very Low	Commonly 100m	1024	Star Networks 2 to 155Mbps
STP	Fairly More Expensive	Commonly 100m	270	IBM Token Ring 4 or 16Mbps
Thinnet	Relatively inexpen--sive less than STP or UTP	185m	30	Thinnet Ethernet 2 to lOMbps
Thicknet	Fairly expensive more than Thinnet, STP, or UTP; less than fiber-optic	500m	100	Thicknet Ethernet 2 to lOMbps

TWISTED-PAIR CABLE

Twisted-pair cable uses one or more pairs of two twisted copper wires to transmit signals. The twists in twisted-pair cable decrease crosstalk because the radiated signals from the twisted wires tend to cancel each other out. Twisted-pair cable is commonly used as telecommunications cable and has become the most popular type for LANs that use copper cables. It is very inexpensive and easy to install.

UTP cable consists of a number of twisted pairs with a simple plastic casing (see Figure 2.3). Transmissions across copper wire tend to attenuate rapidly. However, engineers have reduced UTP's problems of radiated noise and susceptibility to EMI, and some categories of UTP are capable of speeds up to 100 Mbps. UTP is available in six categories, which are listed in Table 2.2.

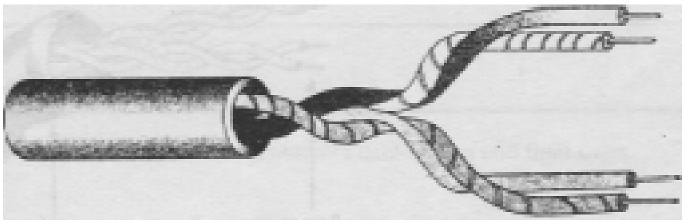


FIGURE 2.3 Unshielded twisted-pair (UTP) cable

TABLE 2.2 UTP CATEGORIES

CATEGORY	DESCRIPTION
1 and 2	Voice grade; very low data rates
3	Four-twisted pairs with three twists per foot; data rates up to lOMbps
4	Four twisted pairs; data rates up to 16Mbps (not commonly used)
5	Four twisted pairs; data rates up to lOOMbps (currently the most popular UTP)
6	Four twisted pairs; data rates up to 155Mbps (soon to be the most popular UTP)

STP

The only difference between STP and UTP is that STP cable has a shield between the outer jacket or casing and the wires (see Figure 2.4). The shield, which is usually made of aluminum/polyester, makes STP less vulnerable to EMI because the shield is electrically grounded; however, STP is not much less susceptible to attenuation than UTP.

A *ground is* a portion of the device that serves as an electrical reference point.

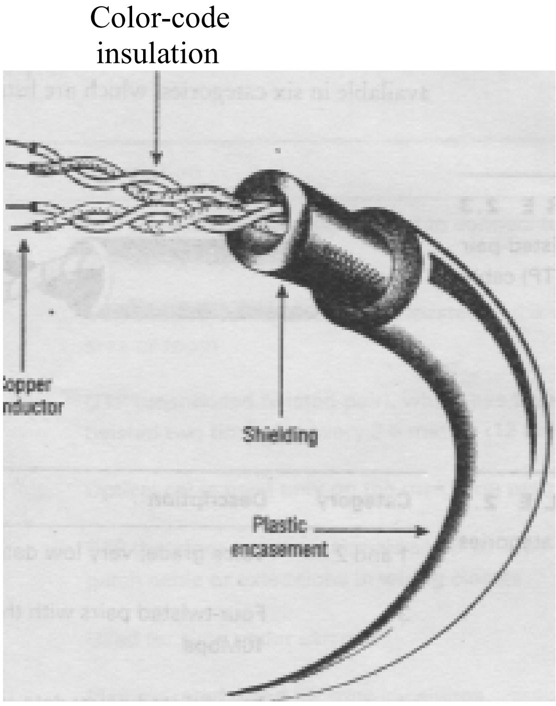


FIGURE 2.4 Shielded twisted-pair (STP) cable

COAXIAL CABLE

Coaxial cable, commonly called *coax,* has two conductors that share the same axis. A solid or stranded copper wire runs down the center of the cable, and this wire is surrounded by plastic foam insulation (see Figure 2.5). Coax cable suffers less attenuation than either UTP or STP cable. Coaxial cable comes in different sizes, which are listed in Table 2.3.

TABLE 2.3 COAXIAL CABLE SIZES

SIZE	**DESCRIPTION**
50-ohm, RG-8, and RG-11	Used for Thicknet Ethernet, also known as lOBaseS
50-ohm, RG-58	Used forThinnet Ethernet, also known as 10Base2
75-ohm, RG-59	Used for cable TV
93-ohm. RG-62	Used for ARCnet

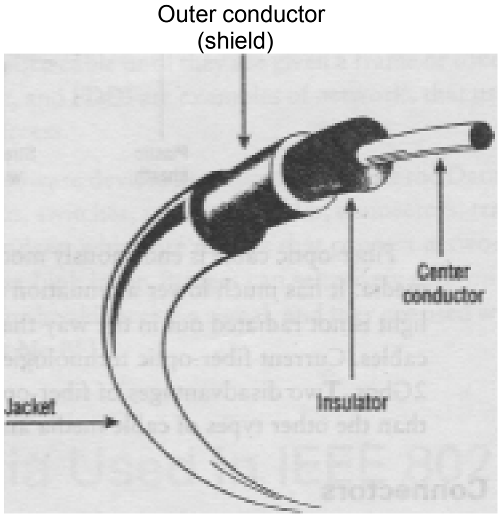


FIGURE 2.5 Coaxial cable

FIBER-OPTIC CABLE

.Fiber-optic cable transmits light signals rather than electrical signals. Each fiber has an inner core of glass or plastic that conducts light. A layer of glass that reflects the light back into the core, called *cladding,* surrounds the inner core. A plastic sheath surrounds each fiber. The sheath can either be tight or loose (see Figure 2.6).

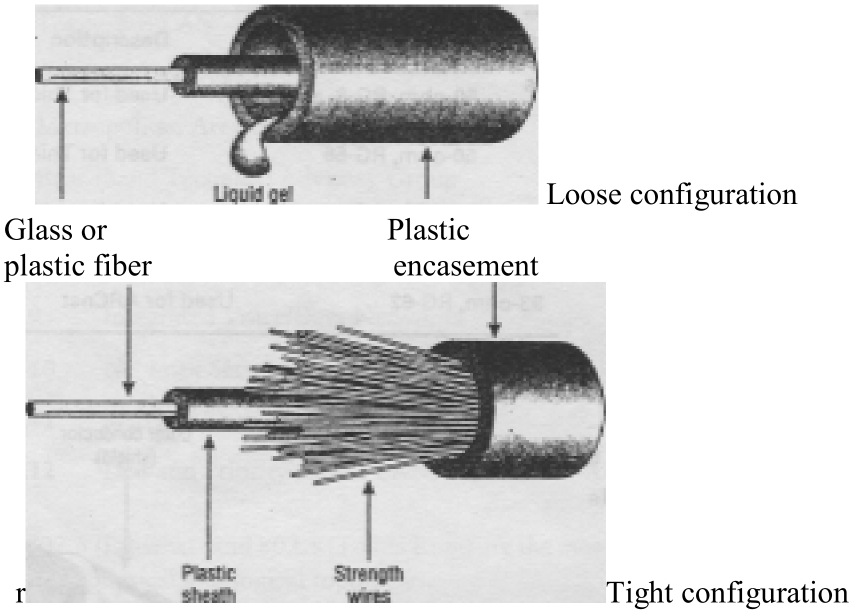


FIGURE **2.6** Fiber-optic cable: loose and tight configurations

Fiber-optic cable is enormously more efficient than the other network cable media. It has much lower attenuation than copper wires, mainly because the light is not radiated out in the way that electricity is radiated from copper cables. Current fiber-optic technologies allow data rates from lOOMbps to 2Gbps. Two disadvantages of fiber-optic cable are that it is more expensive than the other types of cable media and that it is more difficult to install.

CONNECTORS

Three types of connectors are commonly use to connect cables to network interface cards (NICs). These are listed in Table 2.4.

TABLE 2.4 COMMON CONNECTOR TYPES

CONNECTOR	DESCRIPTION
RJ-45	Used to connect UTP cables; 8 conductors
RG-58	Coaxial BNC connector used to connect Thinnet or10Base2 cables
AUI	15-pin connector used for to connect ALH (Attachment Unit Interface) drop cable

WIRELESS MEDIA

Wireless media do not use an electrical or optical conductor. In most cases, the Earth's atmosphere is the physical path for the data. Wireless media is therefore useful when distance or obstructions make bounded media more difficult.

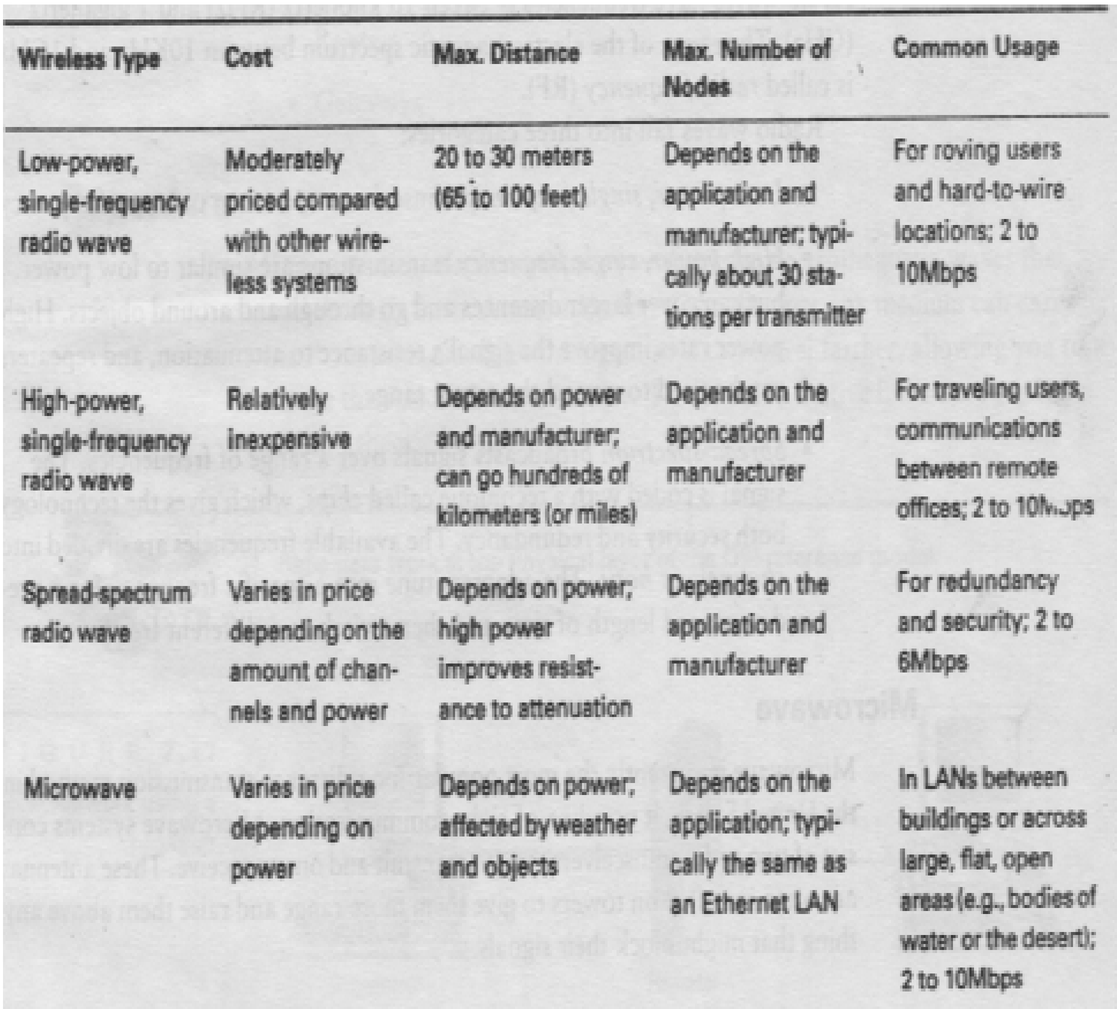
There are three main types of wireless media:

- Radio waves low-power, single frequency; high-power, single frequency; and spread-spectrum

- Microwave
- Infrared

These types are compared in Table 2.5 and described in the following sections

TABLE 2.5: Characteristics of Wireless Media



Wireless Type	Cost	Max. Distance	Max. Number of Nodes	Common Usage
Low-power, single-frequency radio wave	Moderately priced compared with other wireless systems	20 to 30 meters (65 to 100 feet)	Depends on the application and manufacturer; typically about 30 stations per transmitter	For roving users and hard-to-wire locations; 2 to 10Mbps
High-power, single-frequency radio wave	Relatively inexpensive	Depends on power and manufacturer; can go hundreds of kilometers (or miles)	Depends on the application and manufacturer	For traveling users, communications between remote offices; 2 to 10Mbps
Spread-spectrum radio wave	Varies in price depending on the amount of channels and power	Depends on power; high power improves resistance to attenuation	Depends on the application and manufacturer	For redundancy and security; 2 to 6Mbps
Microwave	Varies in price depending on power	Depends on power; affected by weather and objects	Depends on the application; typically the same as an Ethernet LAN	In LANs between buildings or across large, flat, open areas (e.g., bodies of water or the desert); 2 to 10Mbps

RADIO WAVES

Radio waves have frequencies between 10 kilohertz (KHz) and I gigahertz (GHz). The range of the electromagnetic spectrum between IOKHz and I GHz is called *radio frequency* (RF).

Radio waves fall into three categories:

- *Low-power, single frequency* transceivers operate at only one frequency.

- *High-power, single frequency* transmissions are similar to low power,but can cover larger distances and go through and around objects. High power rates improve the signal's resistance to attenuation, and repeaters can be used to extend the signal range.

- *Spread-spectrum* broadcasts signals over a range of frequencies. The signal is coded with a technique called *chips,* which gives the technology both security and redundancy. The available frequencies are divided into *channels* or *hops.* The adapters tune into a specific frequency for a predetermined length of time and then switch to a different frequency.

Microwave

Microwave is currently the most popular long-distance transmission method in the United States. It uses line-of-sight communication. Microwave systems consist of two radio transceivers: one to transmit and one to receive. These antennas are often installed on towers to give them more range and raise them above anything that might block their signals.

Microwave communications comes in two types:

- *Terrestrial microwave* uses Earth-based transmitters and receivers in the low gigahertz range of frequencies (see Figure 2.7). Communications arc line-of-sight and cannot go around corners or through buildings.

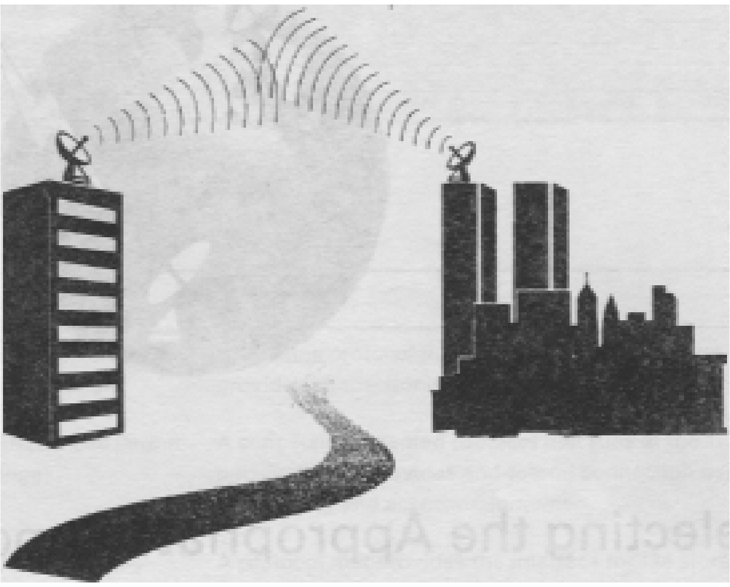


FIGURE 2.7 Terrestrial microwave connecting two buildings

- *Satellite microwave* uses communication satellites that operate in geosynchronous orbit (rotate with the Earth) at 22,300 miles above the Earth see Figure 2.8). Parabolic antennas are used to communicate with the satellite. You might consider satellite transmission for locations that wires cannot reach (such as far out at sea) or when you need to connect thousands of locations worldwide (making cable media verv expensive).

Infrared

Infrared media use infrared light to transmit signals. LEDs (light-emitting diodes) or ILDs (interjection-laser diodes) transmit the signals, and photodiodes receive the signals. Because infrared signals are in the terahertz (higher frequency) range, they have good throughput. The disadvantages of infrared signals are that they cannot penetrate walls or other objects and they are diluted by strong light sources.

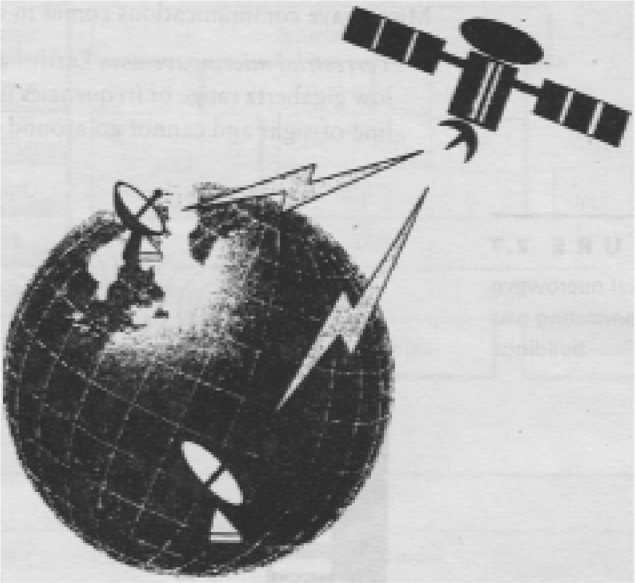


FIGURE 2.8 Satellite microwave

SELECTING THE APPROPRIATE TOPOLOGY

Four physical topologies are typically used for network

- Bus
- Ring
- Star
- Mesh

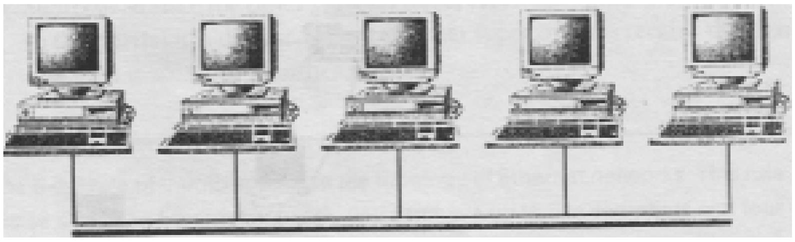


FIGURE 2.9 A physical bus topology

Bus Topology

A bus topology is commonly used for IOBase2 or IOBase5 networks. A typical bus network uses just one or more cables, with no active electronics to amplify the signal or pass it along from computer to computer (see Figure 2.9). When one computer sends a signal up and down the wire (sometimes referred to as *backbone),* all the computers on the network receive the information but only one computer will accept the information; the rest disregard the information

Ring Topology

In a ring topology, each computer is connected to the next computer, with the last one connected to the first (see Figure 2.10). Each device has a receiver and a transmitter that serves as a repeater, passing the signal to the next computer

Star Topology

Star is the standard physical topology for both Ethernet (lOBaseT) and Token Ring networks. In a star topology, all the cables run from the computers to a central location, whfere they are connected by a device called a *hub* or a *switch* (see Figure 2.11). The hub or switch receives the signals from, other computers and routes the signals to the proper destination. If you connect more than one hub together, it is referred to as a *tree* or *hierarchical* topology.

A star physical topology is run as a logical bus topology, which means that all computers receive the signal but only the destination accepts the signal; the rest disregard the information.

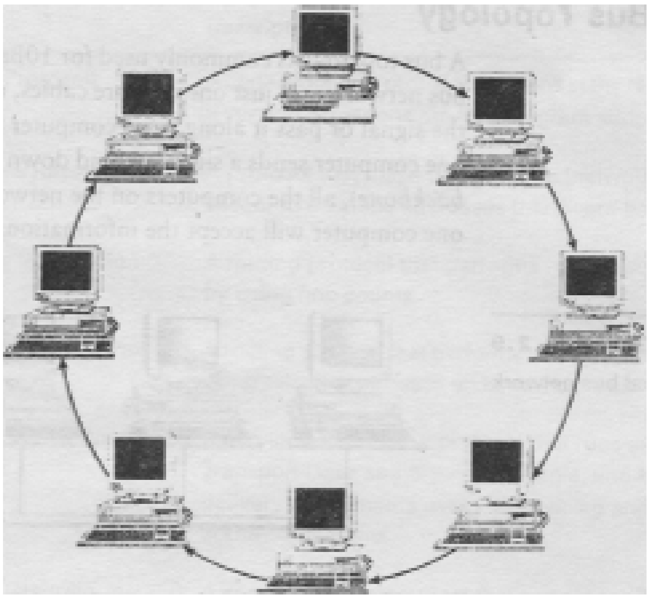


FIGURE 2.10 A physical ring network

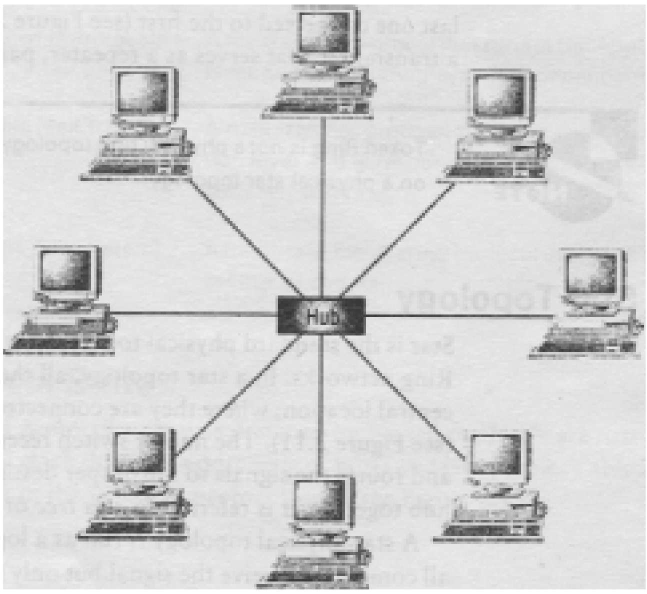


FIGURE 2.11 A physical star network

Four types of hubs are used with star physical topologies:

- *Passive hubs* receive the signal and pass it along without regenerating the signal.

- *Active hubs* receive the signal and pass it along, regenerating or amplifying the signal.

- *Intelligent hubs* are the same as active hubs, but they have a management card for administration.

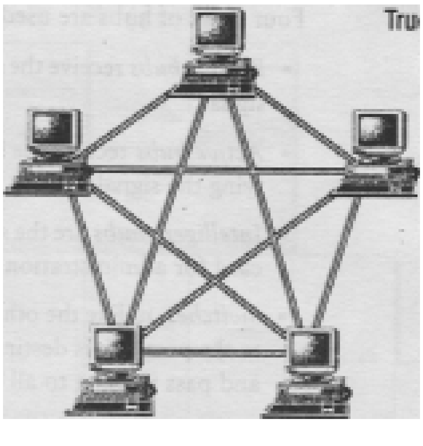
- *Switches,* unlike the other types of hubs, receive a signal and send it only to the port(s) it is destined for. The other types of hubs receive the signal and pass it along to all other ports.

The 5-4-3 rule of thumb applies to the topology of Ethernet networks. This rule states that in an Ethernet network, you can have up to five segments and four repeaters, with only three segments populated.

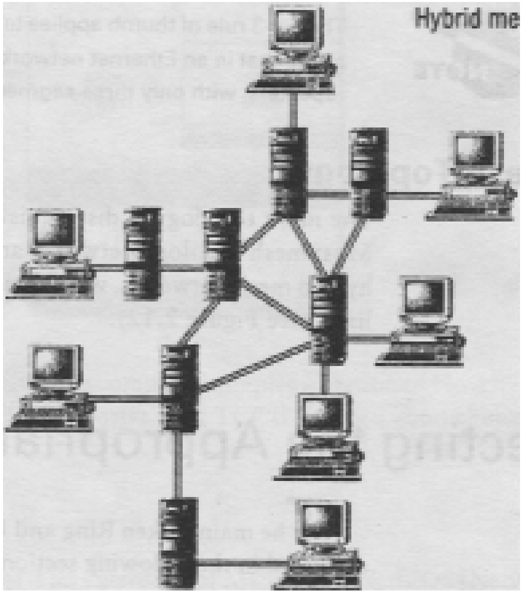
Mesh Topology

The mesh topology is distinguished by redundant links between devices. Most mesh topology networks are not true mesh networks. Instead, they are hybrid mesh networks, with some redundant links rather than all redundant links (see Figure 2.12).

FIGURE 2.12 Physical True Mesh And Hvbrid Mesh Networks



TRUE MESH



HYBRID MESH

PROTOCOLS AND THE WINDOWS NT NETWORKING STRUCTURE

In the Windows NT networking structure (see Figure 2.13), the NDIS interface, NDIS wrapper, and NDIS-compatible drivers enable the TCP/IP, NWLink, NetBEUI, AppleTalk, and DLC protocols to interact simultaneously with the lower layers.

The TDI (Transport Driver Interface) is an interface that enables the server, redirector, and file system drivers to remain independent of the transport protocol.

Windows NT, Windows 95, Windows 3.1, and Windows for Workgroups use SMB for file and print sharing.

DLC is used in Windows NT environments that include HP Jet Direct cards with printers. This protocol is used as a connectivity protocol for IBM mainframes, but it cannot be used as a communication protocol between Microsoft hosts.

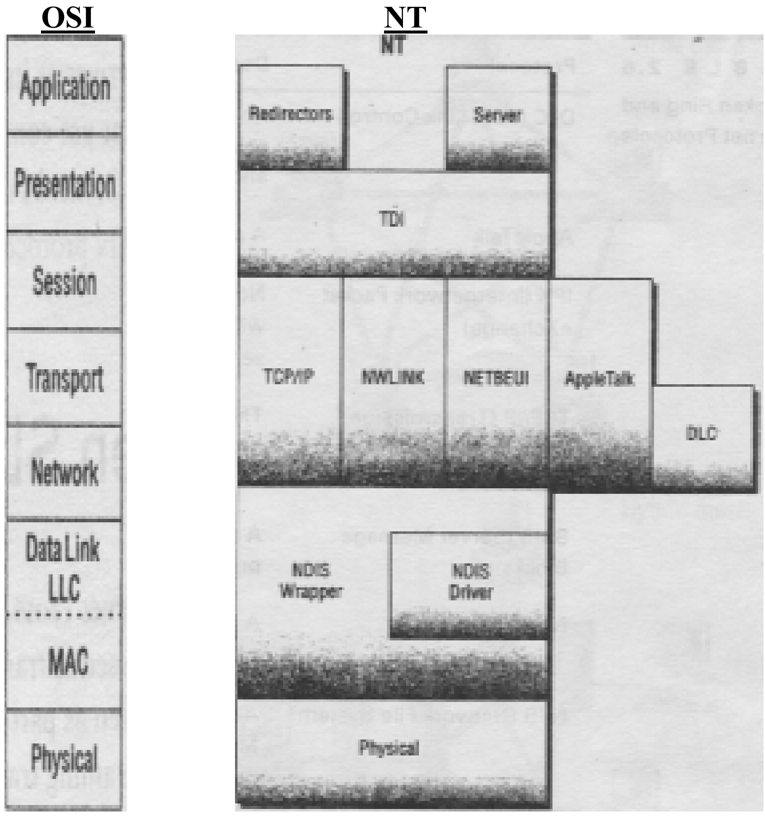


FIGURE 2.13: WINDOWS NT NETWORKING ARCHITECTURE

Windows NT uses its own compatible implementation of Novell's IPX/SPX, called NWLink. NWLink is faster than TCP/IP and is a good choice for small networks.

The NetBEUI Protocol

The NetBEUI protocol is an extension of Microsoft's NetBIOS (Network Basic Input/Output System). This protocol is supplied with all Microsoft network products.

NetBEUI has several advantages:

- It is speedy compared with other protocols.
- It has a small stack size.
- It is compatible with all Microsoft products.

It also has several disadvantages:

- It was designed for small networks.
- It is not routable (but it can be bridged).

- It is generally limited to Microsoft-based networks

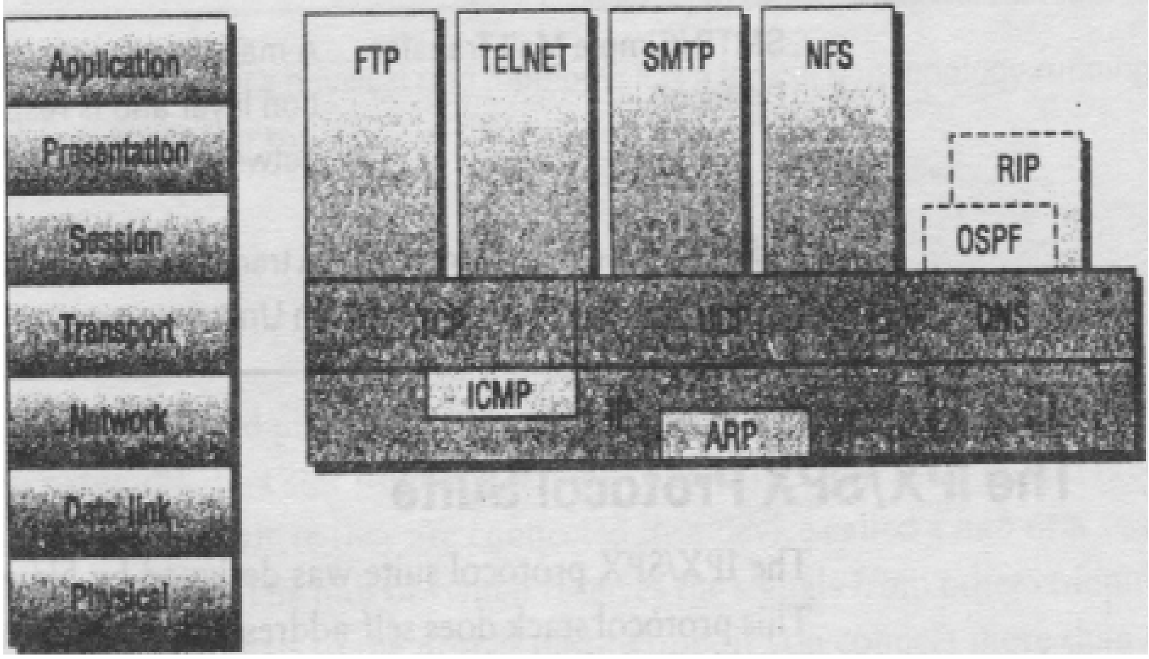
IBM OS/2 LAN Server also supports a compatible NetBEUI protocol

Because of the NDIS standard, NetBEUI can coexist with other, routable protocols. For example, you can use NetBEUI on your LAN and use TCP/IP for your WAN segments. If you use NetBEUI, you must use a bridge or brouter to segment your network.

THE INTERNET PROTOCOL SUITE

The Internet protocol suite was developed along with its namesake, and these protocols have become the de facto standard because of the success of the Internet. The entire protocol suite is sometimes referred to as TCP/IP. The protocols in the Internet protocol suite (see Figure 2.14).

FIGURE 2.14 The Internet Protocol suite compared to the OSI reference model



THE IPX/SPX PROTOCOL SUITE

The IPX/SPX protocol suite was designed by Novell for NetWare networks. This protocol stack does self-addressing of hosts and is routable. Table 2.8 lists the protocols in the IPX/SPX protocol suite (see Figure 2.15).

FIGURE 2.15 The IPX/SPX protocol suite compared to the OSI reference model

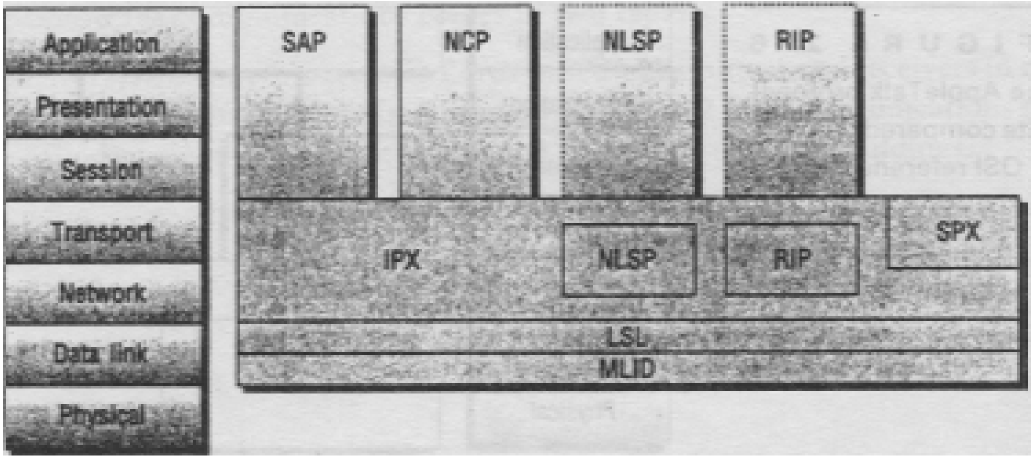


TABLE 2.8
Protocols in the IPX/SPX Protocol Suite

PROTOCOL	DESCRIPTION
IPX (Internetwork Packet exchange)	A routable protocol that runs at the Network layer and provides connectionless datagram service
SPX (Sequenced Packet exchange)	A connection-oriented protocol that runs at the Transport layer and provides end-to-end connection using sequencing and acknowledgments
NCP (NetWare Core Protocol)	A protocol that provides the interface for file storage and retrieval services between workstations and the server

The AppleTalk Protocol Suite

The AppleTalk protocol suite was designed by Apple for the Macintosh computers. Networking capabilities are built into every Macintosh; the client-side AppleShare software is included with the Apple operating system. The AppleTalk protocol also supports LocalTalk, EtherTalk, and TokenTalk. Table 2.9 lists the protocols in the AppleTalk protocol suite (see Figure 2.16).

FIGURE 2.16
The AppleTalk protocol suite compared with the OSI reference model

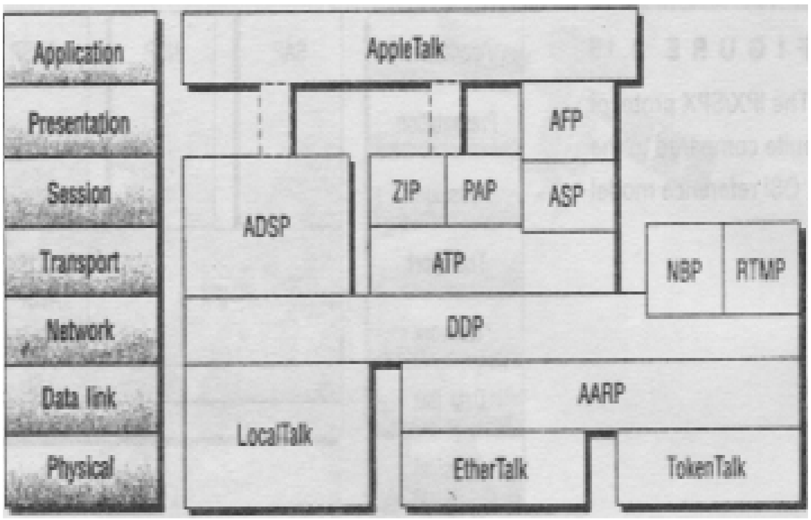


TABLE 2.9
Protocols in the AppleTalk Protocol Suite

PROTOCOL	**DESCRIPTION**
AppleShare	A file and print sharing protocol
AFP (AppleTalk Filing Protocol)	A protocol that provides file sharing between Macs and DOS-based computers, provides an interface for communication between AppleTalk and other network operating systems, and is responsible for file-system security.
DDP (Datagram Delivery Protocol)	A connectionless protocol that runs at the Network layer and provides datagram service between Macs
ATP (AppleTalk Transaction Protocol)	A connectionless protocol that runs at the Transport layer and provides reliable transmissions, using acknowledgments

SELECTING THE APPROPRIATE CONNECTIVITY DEVICES

To expand a LAN, you can divide it into separate segments, which can allow you to reduce the number of broadcasts and increase security. Connecting these segments together creates an *internetwork.* There are five connectivity devices that can be used to connect your segments together to create your internetwork:

- **Repeaters**
- **Bridges**
- **Brouters**
- **Routers**
- **Gateways**

REPEATERS

All transmission media attenuate (weaken) the electromagnetic waves that travel through them. Attenuation limits the distance any medium can carry data. A repeater amplifies the signal so it can travel farther, allowing you to increase the size of the network (see Figure 2.17). Active hubs have repeaters built into them.

Repeaters work at the Physical layer of the OSI reference model.

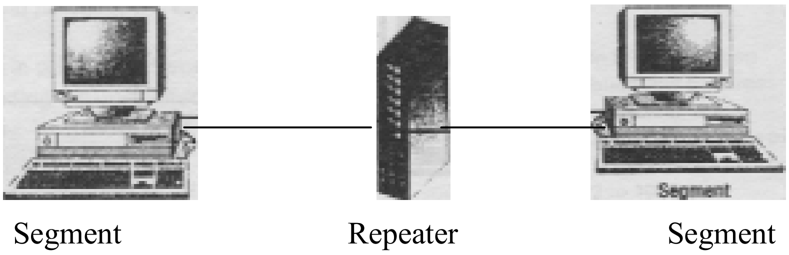


FIGURE 2.17 A network using a Repeater

Repeaters fall into two categories:

- *Amplifiers* simply amplify the entire incoming signal.

- *Signal-regenerating repeaters* create an exact duplicate of incoming data by identifying it amidst the noise, reconstructing it, and retransmitting only the desired information.

BRIDGES

Bridges connect network segments and are useful for small networks and for protocols that cannot be routed, such as NetBEUI. Unlike a repeater, which simply passes on all the signals it receives, a bridge selectively determines the appropriate segment to which it should pass a signal. It does this by reading the MAC address (sometimes referred to as the hardware address) of all the signals it receives (see Figure 2.18).

Bridges work at the MAC sublayer of the Data-Link layer of the OS! Reference model.

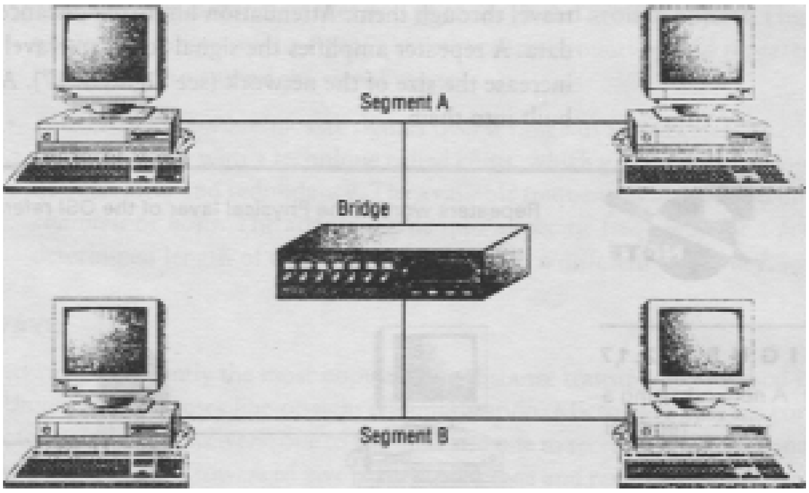


FIGURE 2.18 A bridged network

ROUTERS

Routers use logical and physical addressing to connect two or more logically separate networks (see Figure 2.19). They accomplish this connection by organizing a large network into smaller logical network segments. Each of these smaller subnetworks (also know as *subnets)* is given a logical address. Routers use a route-discovery algorithm to determine possible routes through the internetwork.

Routers are a combination of both hardware and software. The hardware consists of the physical interfaces to the networks in an internetwork. Routers work at the Network layer of the OSI reference model.

Routers can be configured in two ways:

- With *static routing,* the administrator configures the routers with the paths to different networks.

- With *dynamic routing,* a routing protocol uses broadcasts to talk to the other routers on the network to determine the routes to different networks. The two common methods of dynamic routing are distance-vector (RIP) and link-state (OSPF).

Network A

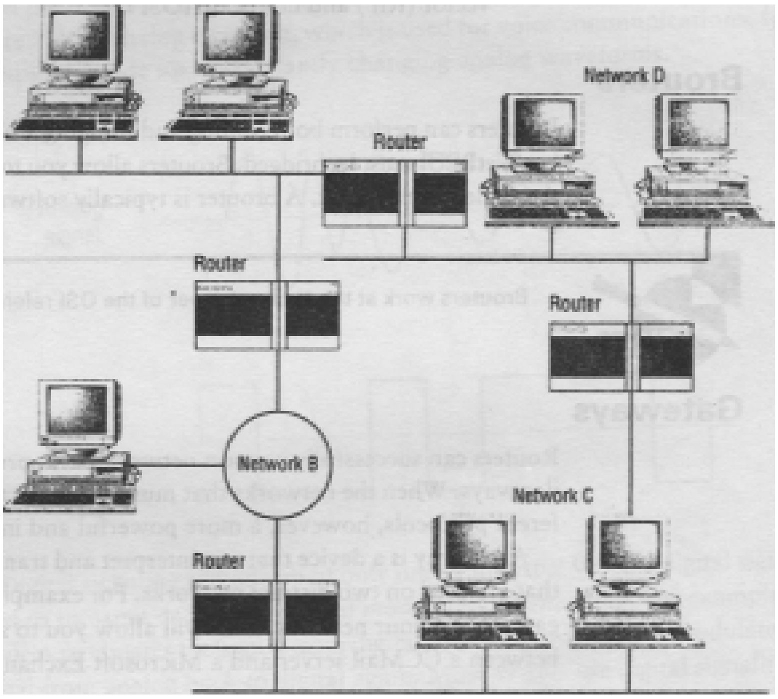


FIGURE 2.19A network using routers

BROUTERS

Brouters can perform both routing and bridging. For example, IP can be routed, but NetBEUI must be bridged. Brouters allow you to run both protocols through the same internetwork. A brouter is typically software that runs on a router. Brouters work at the Network layer of the OSI reference model.

GATEWAYS

Routers can successfully connect networks with protocols that function in similar ways. When the networks that must be connected are using completely different protocols, however, a more powerful and intelligent device is required. A gateway is a device that can interpret and translate the different protocols that are used on two distinct networks. For example, you might have an e-mail gateway on your network. This will allow you to seamlessly exchange mail between a CCMail server and a Microsoft Exchange mail server. Gateways function at all layers of the OSI reference model

SELECTING WAN CONNECTION SERVICE

WANs originated to solve the problem of connecting a LAN to workstation or another remote LAN when the distances exceed cable media specifications or when physical cable connections are not possible. WANs can use various telecommunication services for their connections

Analog versus Digital Signaling

WAN connection services can use either *analog* or *digital* signaling. Analog signaling, which is used for voice communications, for example, is made up of constantly changing analog waveforms.

Digital signaling is made up of only ones and zeros. When a digital signal is used to transmit data, this is called *modulating* or *encoding.* For example, a modem modulates the signal from digital to analog, and then demodulates the signal from analog back to digital again. Most WANs use digital signaling.

Dial-up versus Leased Lines

The PSTN (public switched telephone network) offers two types of lines connections

- With *dial-up lines,* the subscriber pays for what is used. There is no dedicated path.
- With *leased lines,* the subscriber receives dedicated bandwidth, guaranteed by the provider.

Types of WAN Connection Services

Some of the WAN connection services are described in the following sections.

X.25

X.25 was the first packet-switching network standard. This standard spans the Physical through Network layer protocols.

X.25 assumes that the LAPB (Link Access Procedures-Balanced) protocol is being used. LAPB is a full-duplex, bit-oriented, synchronous clocking protocol.

The disadvantage of X.25 is that it is slower than the other WAN connection services because of the flow-control and error-checking techniques it uses. It supports transmission speeds up to only 64Kbps.

Frame Relay

Frame Relay is an upgrade to the X.25 packet-switching network, with fast, variable-length packets. Frame Relay was created to be part of the B-ISDN(Broadband Integrated Services Digital Network).

In this implementation, the overhead from X.25 has been eliminated, and the Frame Relay networks use the higher-layer protocols to provide error control (see Figure 2.22). Because Frame Relay assumes a lower error rate, it transfers data at higher data rates than X.25 (from 56Kbps to 1.544Mbps).

ISDN

ISDN (Integrated Services Digital Network) is an upgrade to the old telephone network (see figure 2.23). ISDN was created to be a dial-up service rather than dedicated line.

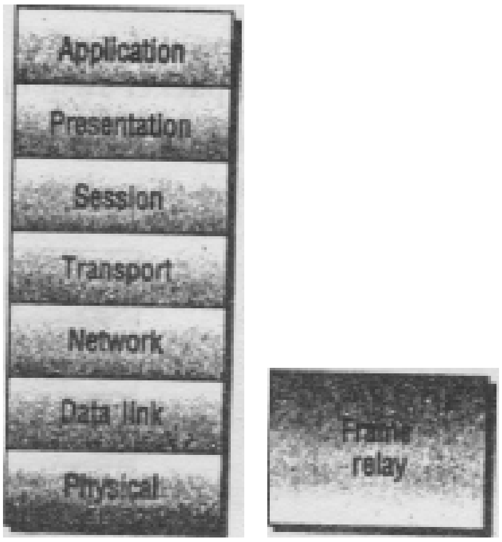


FIGURE 2,22 Frame Relay and the OSI Reference Model

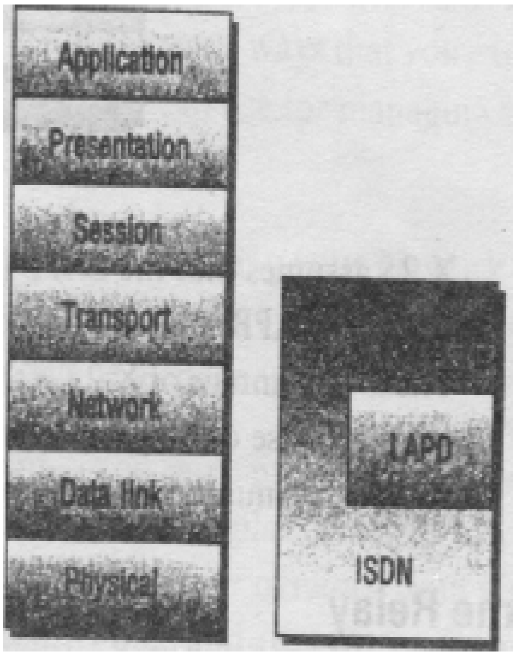


FIGURE 2.23 ISDN and the OSI Reference Model

Two types of ISDN are commonly in use today:

- *Basic Rate ISDN* (BRI) (also called *2B+D)* consists of three channels: two for data at 64KB each, called B channels, and one 16KB channel used for signaling and link management, called a D channel. BRI has speeds up to 128Kbps.

- *Primary Rate ISDN* (PRI) uses the entire bandwidth of a Tl (23 channels, with the twenty-fourth as the D channel). It has speeds up to 1.544Mbps.

ATM

ATM (Asynchronous Transfer Mode) uses fixed-length, 53-byte cells to transfer data at very fast rates. Cells are 53 bytes long with a 5-byte header. ATM can be used for voice, data, fax, real-time video, CD-quality audio, and imaging.

The *Asynchronous* in ATM means that time-slots don't occur periodically, as with TDM (time-division multiplexing). Instead, time slots are given on a first-come, first-served, or priority, basis. Time-sensitive traffic like video can be given priority time slots over less time-sensitive traffic like data.

The same-size cells allow for a very high efficiency in data transmission, with some equipment achieving speeds up to 2Gbps. The most common ATM data transmission speeds are 155Mbps and 622Mbps.

Because ATM isn't concerned about the Physical layer specifications, it can run on different hardware platforms. As ATM is a relatively new technology compared to Ethernet and Token Ring, onlv a few companies build ATM hardware.

T1 and T3

Tl connection services are available from the PSTN. T1 lines are point-to-point connections across 24 channels, with a speed of 1.544Mbps. Each channel is 64Kbps, and Tl service can be divided to create different sizes of fractional lines.

T3 lines are point to-point connections across 28 Tl lines, with a speed of 44.736Mbps. Fractional Tl or T3 lines are portions of Tl or T3 lines. You can purchase only the number of channels that you need or can afford.

Switched 56

Switched *56* is a dial-up service, used on demand, that you can lease from the PSTN. It provides 56Kbps connections. Switched *56* leased-line service provides more bandwidth than regular analog modems at less cost than a full Tl leased line.

SONET

SONET (Synchronous Optical Network) is a high-speed, fiber-optic system that can transfer data between two points at speeds of greater than IGbps. It can be used as a carrier service for WAN connection services, such as ATM and ISDN.

CHOOSING AN ADMINISTRATIVE PLAN

It is important to understand and plan how you are going to administer your network. In your administrative plan, you should consider the following elements of your network:

Resources Hardware devices, such as hard drives and printers, that can be shared in the network.

Network shares The areas of a hard drive or printers you have chosen to share.

Permissions The security assigned to a particular resource. Security can be share-level (or password-protected), with read-only or full-access permissions, or through access permissions, with access rights granted to users or groups through an access control list (ACL).

Users The accounts for the people who will be connecting to your network.

Groups The accounts that simplify user and security administration. You can assign rights to groups instead of individual users, and place users who share a common trait or who need access to a common resource in the groups.

Rights The abilities given to users and groups to manage or use different resources.

NETWORK CONFIGURATION

Before you can plan the specifics of administering your network, you need to configure your servers and clients to suit your business requirements, as well as to facilitate managing your network. Your network configuration considerations include the following:

- Network growth and how you will maintain the level of security required as your network expands
- Server applications and how they will integrate into your network
- Client operating systems, including non-Windows clients

NETWORK GROWTH

One of the biggest challenges in administering a network is planning for network growth. Here, we will outline some ways that you can manage a growing network, including some tools you can use for managing a TCP/IP network regardless of its size.

Document Your Network: Documenting your network will help tremendously when trouble strikes or you need to expand your network. Keeping your documentation up-to-date can be a challenge, but it's worth the effort.

Protect Your Environment: You must protect your network from intentional and accidental damage. A security plan will help you keep your network safe from intruders. You can protect your network from viruses by using scanning software. Both your security plan and anti-virus software should change as your network changes (you should update your virus-scanning software every month). See the "Security Management" section later in this unit for more information about planning your network's security.

Expand Your Network with Routers and Gateways: By building your network with routers and gateways, rather than with repeaters and bridges, you will be better able to handle network growth. However the cost might not justify the means if your network is small or your budget does not allow you to buy expensive routers. Repeaters and bridges can actually hinder network management if your network grows too fast or too large. You do not want to put too many stations on a segment or to exceed cable specifications.

Choose Protocols Carefully: You should choose protocols that will grow with your network. Do not run more protocols than you actually need. Running multiple protocols on a network that needs only one or two will waste precious bandwidth with broadcasts. Here are some points to keep in mind about various protocols:

- NetBEUI is suitable for very small workgroups.
- You should run either NWLink or TCP/IP in large organizations.
- IPX can be very chatty in large organizations, but it is self-addressing and easy to administer.
- TCP/IP probably will be the primary protocol of the future, and it might be a good idea to plan your network accordingly.

Use DHCP to Assign IP Addresses: For a TCP/IP network, you can use DHCP (Dynamic Host Configuration Protocol) to dynamically assign IP addresses for hosts. DHCP was initially created for organizations that had fewer IP addresses than hosts. At that time, IP addresses were not used or needed as often as they are now, and a client could get away with having an IP address when it was available. We know that that is impossible today, but DHCP is still a good option.

If a network uses static IP addresses on all its hosts, duplicate addresses could easily turn up on the network. Then both computers with the same address would not work on the network. If used correctly, DHCP's dynamic assignments can prevent duplicate IP addressing. DHCP can also keep a database of who has which address, which is useful for troubleshooting network problems.

Use WINS to Resolve NetBIOS Names: Another useful tool for TCP/IP networks is WINS (Windows Internet Naming Service). WINS resolves NetBIOS names to IP addresses. When communicating from host to host, regardless of whether the host is a client or a server, the NetBIOS (computer) name must be resolved to an IP address. There are a couple of ways to do this, but resolving names through WINS is by far the best method.

WINS is dynamic, which means that whenever any user gets a DHCP address,the computer can automatically register its NetBIOS name and IP address with WINS. Then, rather than needing to broadcast a NetBIOS name to get its IP address, the client will ask the WINS server to resolve the name, therefore saving precious bandwidth and time.

Use DNS to Resolve Host Names DNS (Domain Name Service) is used to resolve host names (not NetBIOS names) to IP addresses. However, you can configure DNS to use WINS to resolve a WINS address, if you are using Windows NT DNS services.

Typically, DNS is used to resolve names on the Internet, but Windows NT 5 will have a dynamic DNS (like WINS). Also, NetBIOS naming is being phased out. So, in the future, WINS will not be used (except to be backward compatible), and DNS will be a standard server in networks.

Use Host Tables: A HOSTS file, typically used in Unix networks, is a table of host names assigned to IP addresses, not unlike DNS or WINS. The only difference is that you need to have one on every client computer. Furthermore, if one name is added or changed, you must add or change it on every machine, which is very inefficient. DNS and WINS were created to solve this problem. HOSTS (the name must be plural) files can be used in all Windows, Unix, and DOS clients.

An LMHOSTS file provides the same service for NetBIOS names that a HOSTS file does for host names, but it can also preload names and IP addresses into RAM to speed up resolution. LMHOSTS can be used on all Microsoft Windows clients, but like HOSTS, it must be updated on all machines.

INSTALLING AND CONFIGURING MULTIPLE NETWORK ADAPTERS

Il~ network adapter, or network interface card (NIC), is a piece of hardware that requires software (a driver) to run it. The NIC also has the hardware address burned into FROM (Programmable Read-Only Memory) on the card. This is sometimes referred to as the *MAC address,* because the MAC sublayer of the Data Link layer is responsible for maintaining hardware addresses. Each MAC address is 6 bytes longthe first 3 bytes are from the IEEE, and the last 3 bytes are assigned by the manufacturer.

A NIC may store card information in the base memory address area of the system's memory.A NIC coordinates the digital signaling between the PC and the cable. The NIC is responsible for the following tasks:

- Making the connection between the cable and the computer itself.
- Sending ones and zeros over the cable in a logical manner.
- Taking information from the network driver and following the driver's instructions.

Multi-homing Techniques

The Windows NT operating system is capable of handling multiple NICs in the system at the same time (called *multi-homing).* You might consider using multiple NICs to segment your network or to put a computer in more than one network.

SEGMENTING YOUR NETWORK

The Windows NT operating system is capable of being an IP router. This will let you cheaply segment your network. Figure 3.13 shows an example of Windows NT Server running as a router.

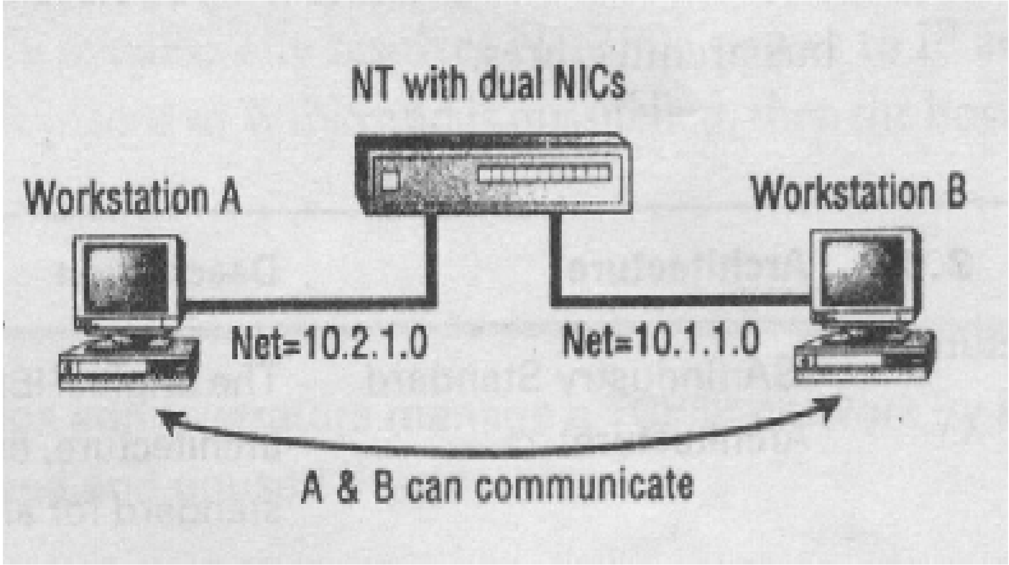


FIGURE **3.13** Windows NT Server running as a router

Putting a Computer in Different Networks

If you install a second NIC in your workstation or server, your computer could be in two networks simultaneously (see Figure 3.14).

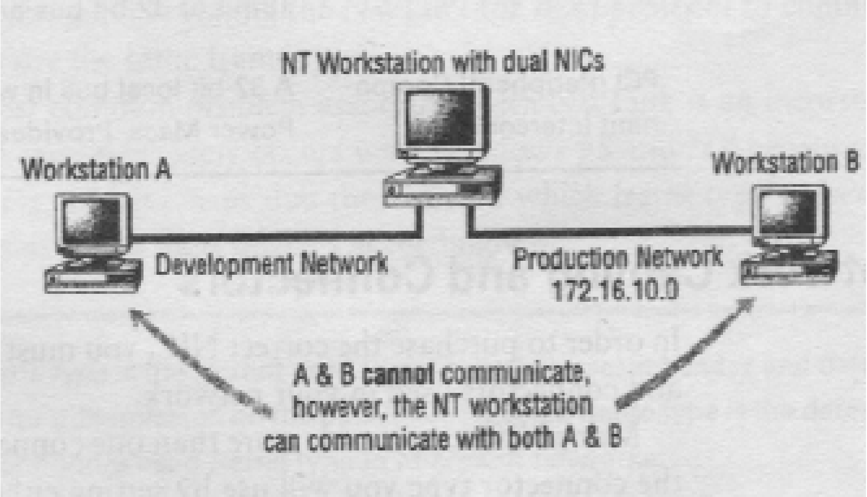

NT Workstation with dual NICs
Workstation A
Workstation B
Development Network
Production Network
172.16.10.0
A & B cannot communicate,
however, the NT workstation
can communicate with both A & B

FIGURE 3.14 A Windows NT workstation in two different networks at the same time

For example, suppose that you had a production network and a development network. You would like to connect your workstation to the production network in order to get e-mail, use file and print services, and so on. You would also like to access the development network from your workstation, but you want to keep your development network independent of the production net- work to avoid extra traffic on the production network. You could install a second NIC into the development network. Then you would be able to access both networks from the same workstation.

NETWORK ADAPTER INSTALLATION

If you are not using Plug and Play, or Windows NT did not detect your network interface card, follow these steps to configure and install the card in Windows NT:

- Place the card into the machine after configuring the jumpers and dip switches if needed, or use the software configuration utility that came with the card.
- Install the software driver.
- Add the protocols.
- Add the client software.
- Attach the network cable.

Before you buy a network interface card for Windows NT, check the Hardware Compatibility List (HCL) to make sure that it is compatible with your system.

HARDWARE CONFLICTS

IRQs (interrupt request lines) are hardware lines over which devices such as input/output ports, keyboard, disk drives, and network interface cards can send messages or interrupts to the CPU. The interrupts are built into the hardware of the computer and are assigned different levels of priority so that the CPU can understand which requests are the most important requests. Network adapters are typically preconfigured for a particular IRQ. You will need to make sure that the IRQ settings for your devices do not conflict, particularly if you have multiple NICs in the same server.

CONCLUSION

This training at Smriti Netcom Pvt Ltd. was a new experience for me. After This Training I found many changes in myself, I not only gained knowledge but added many positive qualities to my Personality and also got a practical approach towards life.

I would like to thank the college staff, who cooperated with me and allowed me to train at this prestigious company.

I would also like to thank and express my gratitude, for the guidance and support which I received from the employees at Smriti Netcom Pvt Ltd. During the course of training they not only trained me, but showed the professional and systematic way of doing things. Their cooperation and suggestions were invaluable.