CHAPTER 17.6
DATA NETWORKS AND INTERNET

Matthew N. O. Sadiku

The coming of the information age has brought about unprecedented growth in telecommunications-based services, driven primarily by the Internet, the information superhighway. Within a short period of time, the volume of data traffic transported across communications networks has grown rapidly and now exceeds the volume of voice traffic. While voice networks, such as the ubiquitous telephone network, have been in use for over a century, computer data networks are a recent phenomenon.

A computer communications network is an interconnection of different devices to enable them to communicate among themselves. Computer networks are generally classified into three groups on the basis of their geographical scope: local area networks (LANs), metropolitan area networks (MANs), and wide area networks (WANs). These networks differ in geographic scope, type of organization using them, types of services provided, and transmission techniques. LANs and WANs are well-established communication networks. MANs are relatively new. On the one hand, LAN is used in connecting equipments owned by the same organization over relatively short distances. Its performance degrades as the area of coverage becomes large. Thus LANs have limitations of geography, speed, traffic capacity, and the number of stations they are able to connect. On the other hand, WAN provides long-haul communication services to various points within a large geographical area, e.g., a nation or continent. With some of the characteristics of LANs and some reflecting WANs, the MAN embraces the best features of both.

We begin this chapter by looking at the open systems interconnection (OSI) reference model, which is commonly used to describe the functions involved in data communication networks. We then examine different LANs, MANs, and WANs including the Internet.

OSI REFERENCE MODEL

There are at least two reasons for needing a standard protocol architecture such as the OSI reference model. First, the uphill task of understanding, designing, and constructing a computer network is made more manageable by dividing it into structured smaller subtasks. Second, the proliferation of computer systems has created heterogeneous networks—different vendors, different models from the same vendor, different data formats, different network management protocols, different operating systems, and so on. A way to resolve this heterogeneity is for vendors to abide by the same set of rules. Attempts to formulate these rules have preoccupied standards bodies such as International Standards Organization (ISO), Consultative Committee for International Telephone and Telegraph (CCITT) [now known as International Telecommunication Union (ITU)], Institute of Electrical and Electronics Engineers (IEEE), American National Standards Institute (ANSI), British Standards Institution (BSI), and European Computer Manufacturers Association (ECMA). Here we consider the more universal standard protocol architecture developed by ISO.

The ISO divides the task of networking computers into seven layers so that manufacturers can develop their own applications and implementations within the guidelines of each layer. In 1978, the ISO set up a committee

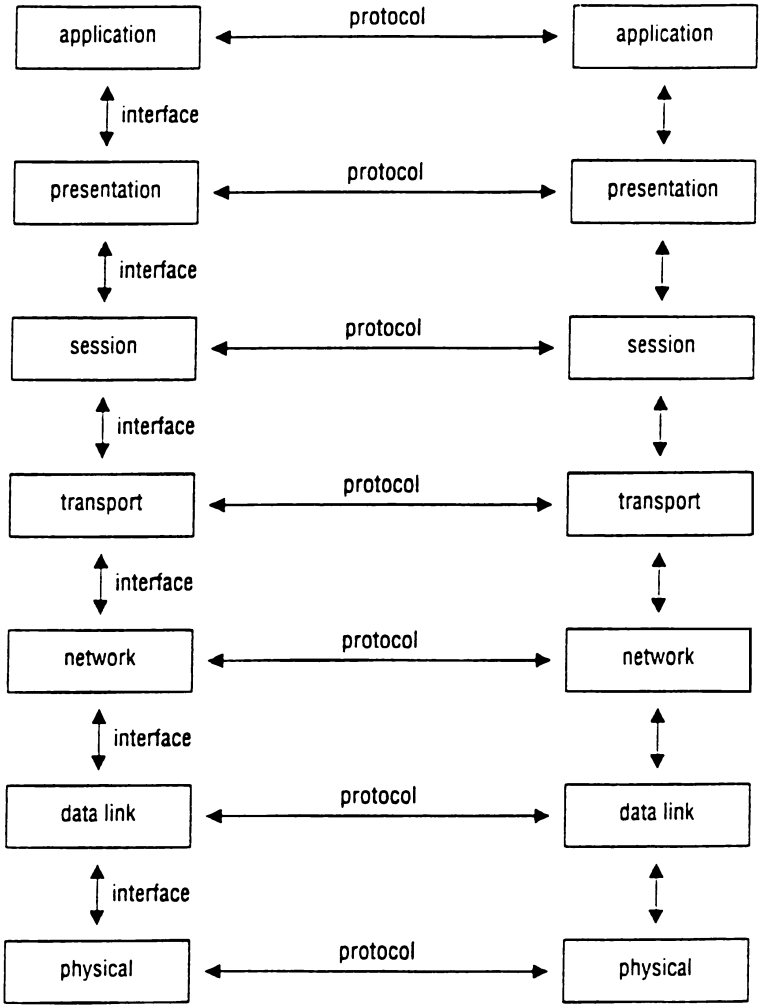


FIGURE 17.6.1 OSI reference model.

to develop a seven-layer model of network architecture (initially for WANs), known as the OSI. The model serves as a means of comparing different layers of communication networks. Also, the open model is standard-based rather than proprietary-based; one system can communicate with another system using interfaces and protocols that both systems understand. Network users and vendors have "open systems" in which any standard computer device would be able to interoperate with others.

The seven layers of the OSI model are shown in Fig. 17.6.1 and briefly explained as follows. We begin with the application layer (layer 7) and work our way down.

- *Application Layer*: This layer (layer 7) allows transferring information between application processes. It is implemented with host software. It is composed of specific application programs and its content varies with individual users. By application, we mean a set of information-processing desired by the user. Typical applications (or user programs) include login, password check, wordprocessing, spreadsheet,

graphics program, document transfer, electronic mailing system, virtual terminal emulation, remote database access, network management, bank balance, stock prices, credit check, inventory check, and airline reservation. Examples of application layer protocols are Telnet (remote terminal protocol), file transfer protocol (FTP), simple mail transfer protocol (SMTP), remote login service (rlogin), and remote copy protocol (rcp).

- *Presentation Layer*: This layer (layer 6) presents information in a way that is meaningful to the network user. It performs functions such as translation of character sets, interpretation of graphic commands, data compression/decompression, data reformatting, and data encryption/decryption. Popular character sets include American Standard Code for Information Interchange (ASCII), Extended Binary Coded Decimal Interchange Code (EBCDIC), and Alphabet 5.
- *Session Layer*: A session is a connection between users. The session layer (layer 5) establishes the appropriate connection between users and manages dialog between them i.e., controlling starting, stopping, and synchronization of the dialog. It decides the type of communication such as two-way simultaneous (full duplex), two-way alternate (half-duplex), one-way, or broadcast. It is also responsible for checking for user authenticity and providing billing. For example, login and logout are the responsibilities of this layer. IBM's network basic input/output system (NetBIOS), sequenced packet exchange (NetWare's SPX), manufacturing automation protocol (MAP), and technical and office protocol (TOP) operate at this layer.
- *Transport Layer*: This layer (layer 4) uses the lower layers to establish reliable end-to-end transport connections for the higher layers. Its other function is to provide the necessary functions and protocols to satisfy a quality of service (QoS) (expressed in terms of time delay, throughput, priority, cost, and security) required by the session layer. It creates several logical connections over the same network by multiplexing end-to-end user addresses onto the network. It fragments messages from the session layer into smaller units (packets or frames) and reassembles the packets into messages at the receiving end. It also controls the end-to-end flow of packets, performs error control and sequence checking, acknowledges successful transmission of packets, and requests retransmission of corrupted packets. For example, the transmission control protocol (TCP) of TCP/IP and Internet transport protocol (ITP) of Xerox operate at this level.
- *Network Layer*: This layer (layer 3) handles routing procedure and flow control. It establishes routes (virtual circuits) for packets to travel and routes the packets from their source to destination and controls congestion. (Routing is of greater importance on MANs and WANs than on LANs.) It carries addressing information that identifies the source and ultimate destination. It also counts transmitted bits for billing information. It ensures that packets arrive at their destination in a reasonable amount of time. Examples of protocols designed for layer 3 are X.25 packet switching protocol and X.75 gateway protocol, both by CCITT. Also, the Internet protocol (IP) of TCP/IP and NetWare's Internetwork Packet Exchange (IPX) operate at this layer.
- *Data Link Layer*: This layer (layer 2) specifies how a device gains access to the medium specified in the physical layer. It converts the bit pipe provided by the physical layer into a packet link, which is a facility for transmitting packets. It deals with procedures and services related to the node-to-node data transfer. A major difference between the data link layer and the transport layer is that the domain for the data link layer is between adjacent nodes, whereas that of the transport layer is end-to-end. In addition, the data link layer ensures error-free delivery of data; hence it is concerned with error-detection, error correction, and retransmission. The error control is usually implemented by performing checksums on all bits of a packet after a cyclic redundancy check (CRC) process. This way, any transmission errors can be detected. The layer is implemented in hardware and is highly dependent of the physical medium. Typical examples of data link protocols are binary synchronous communications (BSC), synchronous data link control (SDLC), and high-level data link control (HDLC). For LANs and MANs, the data link layer is decomposed into the media-access control (MAC) and the logical link control (LLC) sublayers.
- *Physical Layer*: This layer (layer 1) consists of a set of rules that specifies the electrical and physical connection between devices. It is implemented in hardware. It is responsible for converting raw bits into electrical signal and physically transmitting them over a physical medium such as coaxial cable or an optical fiber between adjacent nodes. It provides standards for electrical, mechanical, and procedural characteristics required to transmit the bit stream properly. It handles frequency specifications, encoding the data, defining voltage or current levels, defining cable requirements, defining the connector size, shapes, and pin number, and so on. RS-232, RS-449, X.21, X.25, V.24, IEEE 802.3, IEEE 802.4, and IEEE 802.5 are examples of physical-layer standards.

TABLE 17.6.1 Summary of the Functions of OSI Layers

Layer	Name	Function
7	Application layer	Transfers information between application processes
6	Presentation layer	Syntax conversion, data compression, and encryption
5	Session layer	Establishes connection and manages a dialog
4	Transport layer	Provides end-to-end transfer of data
3	Network layer	End-to-end routing and flow control
2	Data link layer	Medium access, framing, and error control
1	Physical layer	Electrical/mechanical interface

A summary of the functions of the seven layers is presented in Table 17.6.1. The seven layers are often subdivided into two. The first consists of the lower three layers (physical, data link, and network layers) and is known as the communications subnetwork. The upper three layers (session, presentation, and application layers) are termed the host process. The upper layers are usually implemented by networking software on the node. The transport layer is the middle layer, separating the data-communication functions of the lower three layers and the data-processing functions of the upper layers. It is sometimes grouped with the upper layers as part of the host process or grouped with the lower layers as part of data transport.

LOCAL AREA NETWORKS

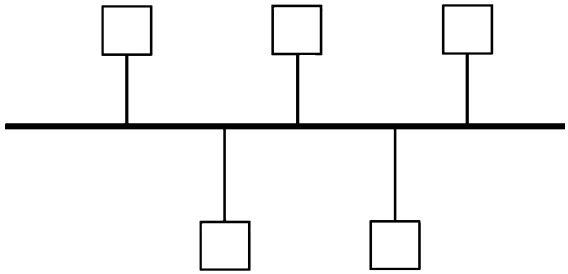
A LAN is a computer network that spans a geographically small area. It consists of two or more computers that are connected together to share expensive resources such as printers, exchange files, or allow electronic communications. Most LANs are confined to a single building or campus. They connect workstations, personal computers, printers, and other computer peripherals. Users connected to the LAN can use it to communicate with each other. LANs are capable of transmitting data at very fast rates, much faster than data can be transmitted over a telephone line; but the distances are limited. Also, since all the devices are located within a single establishment, LANs are usually owned and maintained by an organization. A key motivation for using LANs is to increase the productivity and efficiency of workers.

LANs differ from MANs and WANs by geographic coverage, data transmission and error rates, topology and data routing techniques, ownership, and sometimes by the type of traffic. Unique characteristics that differentiate LANs include:

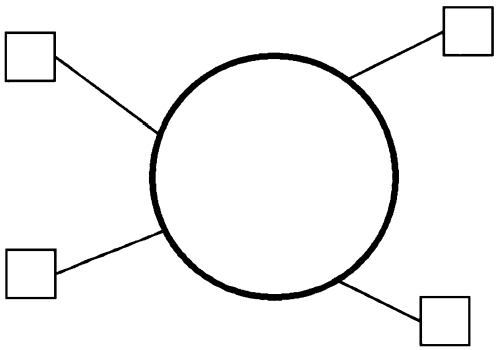
- LANs generally operate within a few kilometers, spanning only a small geographical area.
- LANs usually have very high bit rates, ranging from 1 Mbps to 10 Gbps.
- LANs have a very low error rate, say $1{:}10^8$.
- A LAN is often owned and maintained by a single private company, institution, or organization using the facility.

There are different kinds of LANs. The following features differentiate one LAN from another:

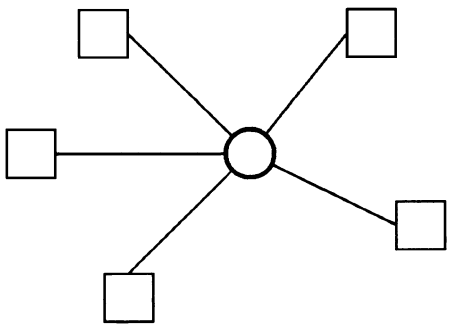
- *Topology*: The geometric arrangement of devices on the LAN. As shown in Fig. 17.6.2, this can be bus, ring, star, or tree.
- *Protocols*: These are procedures or rules that govern the transfer of information between devices connected to a LAN. Protocols are to computer networks what languages are to humans.



(a) Bus

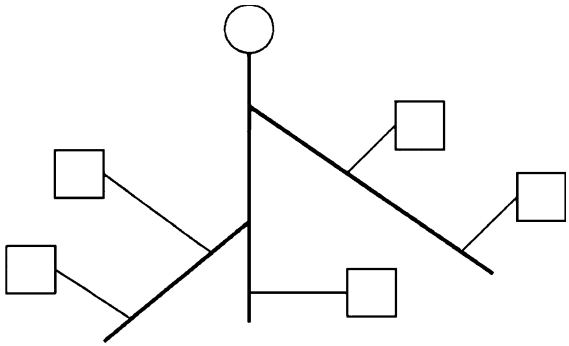


(b) Ring



(c) Star

FIGURE 17.6.2 Typical LAN topologies.



(d) Tree

FIGURE 17.6.2 (*Continued*)

- *Media*: The transmission medium connecting the devices can be twisted-pair wire, coaxial cables, or fiber optic cables. Wireless LAN use radio waves as media. Of all these media, optic fiber is the fastest but the most expensive. Common LANs include Ethernet, token ring, token bus, and star LAN. For bus or tree LANs, the most common transmission medium is coaxial cable. The two common transmission methods used on coaxial cable are baseband and broadband. A baseband LAN is characterized by the use of digital technology; binary data are inserted into the cable as a sequence of pulses using Manchester or Differential encoding scheme. A broadband LAN employs analog signaling and a modem. The frequency spectrum of the cable can be divided into channels using frequency division multiplexing (FDM). One of the most well-known applications of broadband transmission is the community antenna television (CATV). However, baseband LANs are more prevalent.

The Institute of Electrical and Electronics Engineers (IEEE) has established the following eight committees to provide standards for LANs:

- IEEE 802.1—standard for LAN/MAN bridging and management
- IEEE 802.2—standard for logical link control protocol
- IEEE 802.3—standard for CSMA/CD protocol
- IEEE 802.4—standard for token bus MAC protocol
- IEEE 802.5—standard for token ring MAC protocol
- IEEE 802.7—standard for broadband LAN
- IEEE 802.10—standard for LAN/MAN security
- IEEE 802.11—standard for wireless LAN

Token ring is a network architecture that uses token passing technology and ring-type network structure. Although token ring is standardized in IEEE 802.5 standard, its use has quite much faded to few organizations. Ethernet (IEEE 802.3) is the most popular and the least expensive high-speed LAN.

Ethernet is a LAN architecture developed by Xerox Corp. in cooperation with DEC and Intel in 1976. The IEEE 802.3 standard refined the Ethernet and made it globally accepted. Ethernet has since become the most popular and most widely deployed LAN in the world.

Conventional Ethernet uses a bus or star topology and supports data transfer rates of 10 Mbps. It uses a protocol known carrier sense multiple access with collision detection (CSMA/CD) as an access method to handle simultaneous demands. Each station or node attached to the Ethernet must sense the medium before transmitting data to see if any other station is already sending something. If the medium appears to be idle,

then the station can begin to send data. If two stations sense the medium idle and transmit at the same time, collision may take place. When such a collision occurs, the two stations stop transmitting, wait, and try again later after a randomly chosen delay period. The delay period is determined using Binary Exponential Backoff.

Ethernet is one of the most widely implemented LAN standards. A newer version of Ethernet, called *Fast Ethernet* (or 100Base-T) supports data transfer rates of 100 Mbps. Gigabit Ethernet (or 1000Base-T) delivers at 1 Gbps speed. Upcoming 10 Gbps version of Ethernet is expected to be ready by 2002.

Security is an important issue with LANs since they are designed to provide access to many users. Network security is a measure designed to protect LAN users against attacks that originate from the network and other networks such as Internet connected to it. When individuals send private communications through a LAN, they desire secure communications. Currently, there are no systems in wide use that will keep data secure as they transit a public network. Several methods are being used to prevent attacks. One approach is to encrypt data as they leave one machine and decrypt it at the destination. Encryption is the fundamental tool for ensuring security in data networks. Another approach is to regulate which packets can go between two sites. For example, firewalls are placed between an organization's LAN and the Internet. A firewall is simply a group of components that collectively form a barrier between two networks.

METROPOLITAN AREA NETWORKS

Metropolitan area networks are basically an outgrowth of LANs. A variety of users and applications drive the requirements for MANs. The requirements include cost, scalability, security, reliability, compatibility with existing and future networks, and management issues. To meet these requirements, several proposals have been made for MAN protocols and architectures. Of these proposed MANs, fiber distributed data interface (FDDI) and distributed queue dual bus (DQDB) have emerged as standards that compete for use as backbones.

FDDI

In the mid 1970s, it was recognized that the existing copper technology would be unsuitable for future communication networks. Optical fibers offer some benefits over copper in that they are essentially immune to electromagnetic interference (EMI), have low weight, do not radiate, and reduce electrical safety concerns.

FDDI was proposed by the American National Standard Institute (ANSI) as a dual token ring that supports data rates of 100 Mbps and uses optical fiber media. An optical fiber is a thin, flexible glass or plastic structure (or waveguide) through which light is transmitted.

The FDDI specification recommends an optical fiber with a core diameter of 62.5 μm and a cladding diameter of 125 μm. There are two types of optical-fiber mode: single mode and multimode. A mode is a discrete optical wave or signal that propagates down the fiber. In a single mode fiber, only the fundamental mode can propagate. In multimode fiber, a large number of modes are coupled into the cable, making it suitable for the less costly light-emitting diode (LED) light source. The advantages of fiber optics over electrical media and the inherent advantages of a ring design contribute to the widespread acceptance of FDDI as a standard.

FDDI is a collection of standards formed by ANSI X3T9.5 task group over a period of 10 years. The standards produced by the task group cover physical hardware, physical and data link protocol layers, and a conformance testing standard. The original standard, known as *FDDI-I*, provides the basic data-only operation. An extended standard, *FDDI-II*, supports hybrid data and real-time applications.

FDDI is a follow-on to IEEE 802.5 (token ring) in that FDDI is based on token ring mechanics. Although the FDDI MAC protocol is similar (but not identical) to token ring, there are some differences. Unlike in token ring, FDDI performs all networking monitoring and control algorithms in a distributed way among active stations and does not need an active monitor. (Hence the term "distributed" in FDDI.) Whenever any device is down, other devices reorganize and continue to function, including token initialization, fault recovery, clock synchronization, and topology control.

The key highlights of FDDI are summarized as follows:

- ANSI standard through the X3T9.5 committee
- Dual counter-rotating ring topology for fault tolerance
- Data rate of 100 Mbps
- Total ring loop of size 100 km
- Maximum of 500 directly attached stations or devices
- 2 km maximum distance between stations
- Variable packet size (4500 bytes, maximum)
- 4B/5B data encoding scheme to ensure data integrity
- Shared medium using a timed-token protocol
- Variety of physical media, including fiber and twisted pair
- 62.5/125 μm multimode fiber-optic-based network
- Low bit error rate of 10^{-9} (one in one billion)
- Compatibility with IEEE 802 LANs by use of IEEE 802.2 LLC
- Distributed clocking to support large number of stations
- Support for both synchronous and asynchronous services

FDDI has two types of nodes: stations and concentrators. The stations transmit information to other stations on the ring and receive from them. Concentrators are nodes that provide additional ports for attachments of stations to the network. A concentrator receives data from the ring and forwards it to each of the connected ports sequentially at 100 Mbps. While a station may have one or more MAC, a concentrator may or may not have a MAC. As shown in Fig. 17.6.3, each FDDI station is connected to two rings, primary and secondary simultaneously. Stations have active taps on the ring and operate as repeaters. This allows the FDDI network to be so large without signal degradation. The network uses its primary ring for data transmission, while the secondary ring can be used either to ensure fault tolerance or for data. When a station or link fails, the primary and secondary rings form a single one-way ring, isolating the fault while maintaining a logical path among users, as shown in Fig. 17.6.4. Thus, FDDI's dual-ring topology and connection management functions establish a fault-tolerance mechanism.

FDDI was developed to conform with the OSI reference model. FDDI divides the physical layer of the OSI reference model into two sublayers: physical layer dependent (PMD) and physical layer (PHY), while the data link layer is split into two sublayers: media access control (MAC) and IEEE 802.2 LLC. A comparison of the FDDI architectural model to the lower two layers of the OSI model along with the summary of the functions of the FDDI standards is illustrated in Fig. 17.6.5. The FDDI MAC uses a timed-token rotation (TTR) protocol for controlling access to the medium. With the protocol, the MAC in each station measures the time that has elapsed since the station last received a token. Each station on the FDDI ring uses three timers to regulate its operation. The station management (SMT) controls the other three layers (PMD, PHY, and MAC) and ensures proper operation of the station. It handles such functions as initial FDDI ring initialization, station insertion and removal, ring's stability, activation, connection management, address administration, scheduling policies, collection of statistics, bandwidth allocation, performance and reliability monitoring, bit error monitoring, fault detection and isolation, and ring reconfiguration.

Though the original FDDI, described above, provides a bounded delay for synchronous services, the delay can vary. FDDI was initially envisioned as a data-only LAN. The full integration of isochronous and bursty data traffic is obtained with the enhanced version of the protocol, known as FDDI-II. FDDI-II is described by the hybrid ring control (HRC) standard that specifies an upward-compatible extension of FDDI. FDDI-II adds one document, HRC, to the existing four documents that specify FDDI standard. FDDI-II builds on original FDDI capabilities and supports integrated voice, video, and data capabilities but maintains the same transmission rate of 100 Mbps. FDDI-II therefore expands the range of applications of FDDI. FDDI-II supports both packet switched (synchronous and asynchronous) and circuit switched (isochronous) traffic. It can connect high-performance workstations, processors, and mass storage systems with bridges, routers, and gateways to other LANs, MANs, and WANs.

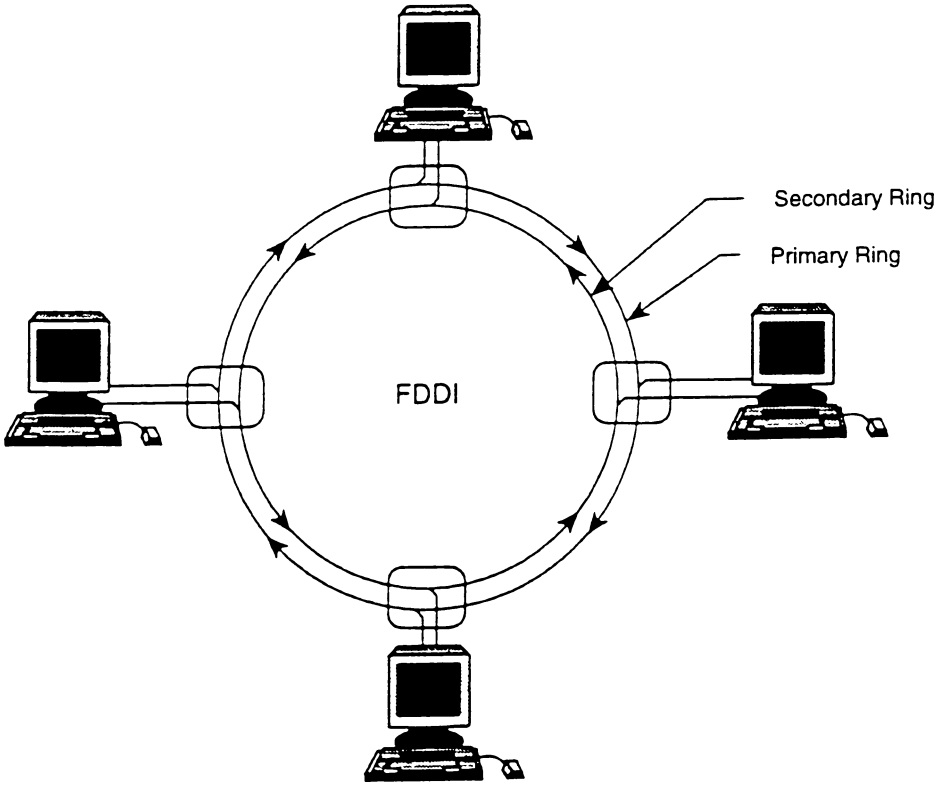


FIGURE 17.6.3 FDDI rings.

DQDB and SMDS

The IEEE 802 committee perceived the need for high-speed services over wide areas and formed the IEEE 802.6 MAN committee in 1982. The committee reached a consensus to use the DQDB as the standard MAC protocol. A by-product of DQDB is the switched multimegabit data service (SMDS).

The DQDB standard is both a protocol and a subnetwork. It is a subnetwork in that it is a component in a collection of networks to provide a service. The term "distributed-queue dual-bus" refers to the use of a dual-bus topology and a MAC technique based on the maintenance of distributed queues. In other words, each station connected to the subnetwork maintains queues of outstanding requests that determine access to the MAN medium. The DQDB subnetwork provides all stations on the dual bus with the knowledge of the frames queued at all other stations, thereby eliminating the possibility of collision and improving data throughput.

The DQDB subnetwork has many features, some of which make it attractive for high-speed data services. Such features include:

- *Shared media*: It extends the capabilities of shared media systems over large geographical areas.
- *Dual bus*: Its use of two separate buses carrying data simultaneously and independently makes it distinct from IEEE 802 LANs.
- *High speed*: It operates at a variety of data rates, ranging from 34 Mbps to 155 Mbps.

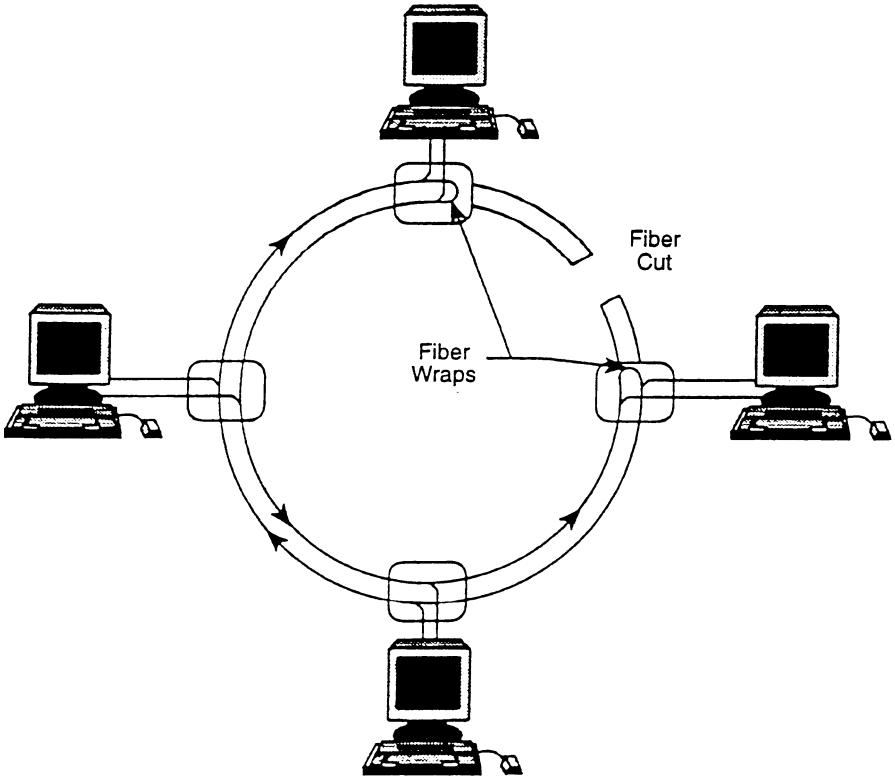


FIGURE 17.6.4 FDDI isolates fault without impairing the network.

- *Compatibility with legacy LANs*: It is compatible with IEEE 802.X LAN standards. A DQDB station should recognize the 16-bit and 48-bit addresses used by IEEE 802.X LAN standards. DQDB is designed to support data traffic under connectionless IEEE 802.2 LLC.
- *Fault tolerance*: It is tolerant to transmission faults when the system is configured in a loop.
- *Congestion control*: It is based on a distributed queuing algorithm as a way of resolving congestion.
- *Segmentation*: Its use of ATM technique allows long variable length packets to be segmented into short fixed-length segments. This provides efficient and effective support for small and large packets and for isochronous data.
- *Flexibility*: It uses a variety of media including coaxial cable and fiber optics. It can simultaneously support both circuit switched and packet switched services.
- *Compatibility*: It is compatible with current IEEE 802 LANs and future networks such as BISDN.

The DQDB network span of about 50 km, transmission rate of about 150 Mbps, and slot size of 53 bytes allow many slots to be in transit between the nodes. DQDB supports different types of traffic, which may be classified into two categories, isochronous and nonisochronous (asynchronous).

The DQDB dual-bus topology is shown in Fig. 17.6.6. As both buses are operational at all times, the capacity of the subnetwork is twice the capacity of each bus. In this network, nodes are connected to two unidirectional buses, which operate independently and propagate in opposite directions as shown in Fig. 17.6.6. Every node is able to send information on one bus and receive on the other bus. The head station (frame generator) generates a frame every 125 μs to suit digitized voice requirement. The frames are continuously generated on

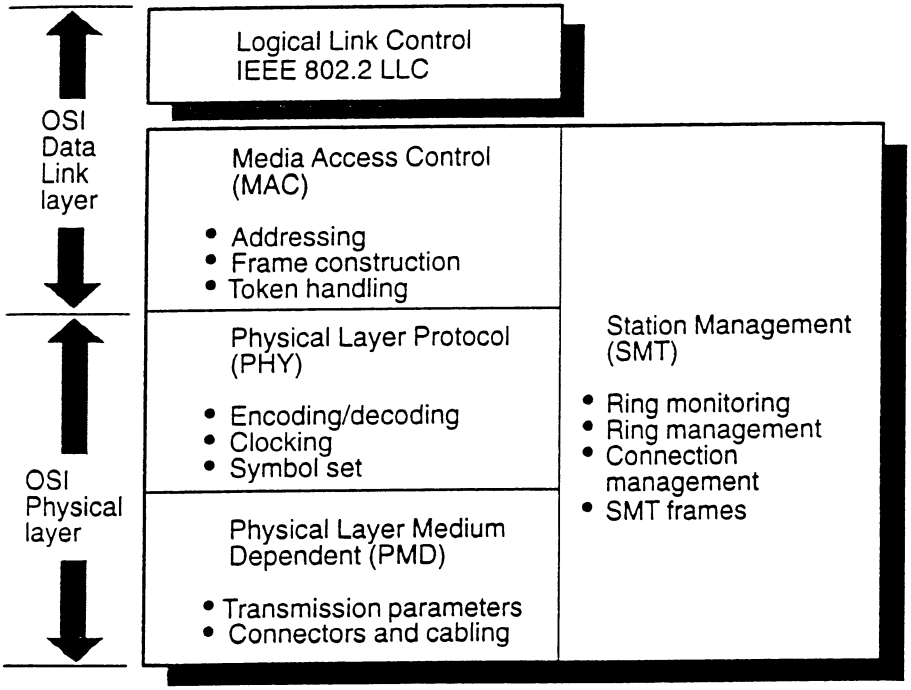


FIGURE 17.6.5 Summary of the functions of the FDDI standards.

each bus so that there is never any period of silence on the bus. The frame is subdivided into equal-sized slots. The empty slots generated can be written into by other nodes. The end station (slave frame generator) terminates the forward bus, removes all incoming slots, and generates the same slot pattern at the same transmission rate on the opposite bus. The slots are 53 octets long, the same as ATM cells, to make DQDB MANs compatible to BISDN.

SMDS represents the first broadband service to make use of DQDB MAN standard and technologies. The need for a high-speed, connectionless data service that provides both high transmission speed, low delay, and

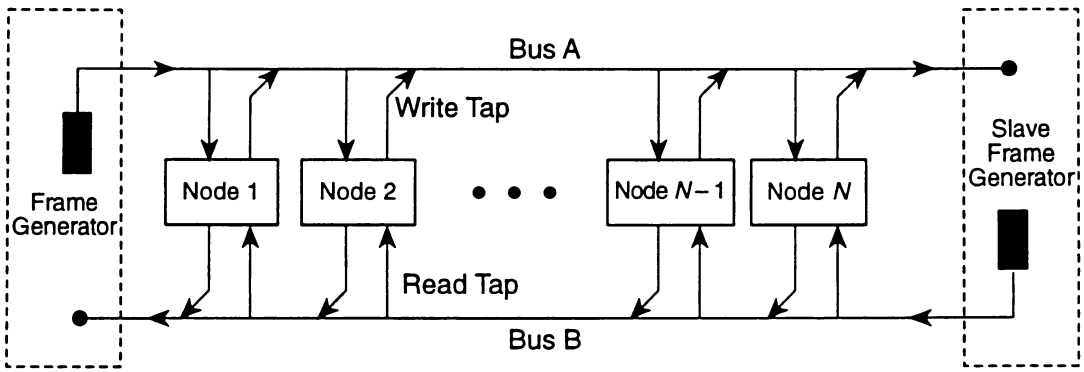


FIGURE 17.6.6 Open bus topology of DQDB network.

a simple, efficient protocol adaptation for LAN interconnection led to a connectionless data service known as *switched multisegment data service* in the United States or *connectionless broadband data service* (CBDS) in Europe. SMDS is the first service offering of DQDB. It is a cell-based, connectionless, packet-switched network that focuses on transmitting data and data only.

SMDS was developed by Bell Communications Research (Bellcore), the research arm of the seven Bell regional holding companies and popularized by the SMDS Interest Group (SIG).

SMDS is not a technology but a service. Although a DQDB can be configured as either a loop bus or an open bus, SMDS uses the open bus topology. SMDS is a connectionless, public, cell-switched data service. The service is connectionless because there is no need for setting up a physical or virtual path between two sites. SMDS offers services characteristically equivalent to LAN MAC. It operates much the same way as a LAN, but over a greater geographical area with a larger number of users.

Compared with other competing high-speed technologies such as FDDI, SMDS has no theoretical distance limitation as FDDI. FDDI's use of tokens limits the perimeter of the FDDI ring to about 60 mi. The data rate of FDDI (100 Mbps) does not match any of the standardized public transmission rate, whereas SMDS is based on standard public network speeds. FDDI will probably be used for high-speed LANs and complement SMDS rather than compete with it.

WIDE AREA NETWORKS

A WAN is an interconnected network of LANs and MANs. A WAN connects remote LANs and ties remote computers together over long distances. Computers connected to a WAN are often connected through public networks, such as the telephone system. They can also be connected through leased lines or satellites. WANs are, by default, heterogeneous networks that consist of a variety of computers, operating systems, topologies, and protocols. The largest WANs in existence is the Internet.

Because of the long distance involved, WANs are usually developed and maintained by a nation's public telecommunication companies (such as AT&T in the United States), which offer various communication services to the people. Today's WANs are designed in the most cost-effective way using optical fiber. Fiber-based WANs are capable of transporting voice, video, and data with no known restriction to bandwidth. Such WANs will remain cutting edge for years to come. There is also the possibilitiy of connecting networks using wireless technologies.

Circuit and Packet Switching

For a WAN, communication is achieved by transmitting data from the source node to the destination node through a network of intermediate switching nodes. Thus, unlike a LAN, a WAN is a switched network. There are many types of switched networks, but the most common methods of communication are circuit switching and packet switching. Circuit switching is a much older technology than packet switching. Circuit switching systems are ideal for communications that require data to be transmitted in real time. Packet-switching networks are more efficient if some amount of delay is acceptable.

Circuit switching is a communication method in which a dedicated path (channel or circuit) is established for the duration of a transmission. This is a type of point-to-point network connection. A switched circuit is maintained while the sender and recipient are communicating, as opposed to a dedicated circuit, which is held open regardless of whether data are being sent or not. The most common circuit-switching network is the telephone system.

Packet switching is a technique whereby the network routes individual packets of data between different destinations based on addressing within each packet. A packet is a segment of information sent over a network. Any message exceeding a network-defined maximum length (a set size) is broken up into shorter units, known as packets. Packet-switching is the process by which a carrier breaks up messages (or data) into these segments, bundles, or packets by the source data terminal equipment (DTE) before they are sent. Each packet is switched and transmitted individually through the network and can even follow different routes to its destination and may arrive out of order.

Most modern WAN protocols, such as TCP/IP, X.25, and frame relay, are based on packet-switching technologies. Besides data networks such as the Internet, wireless services such as cellular digital packet data (CDPD) employ packet switching.

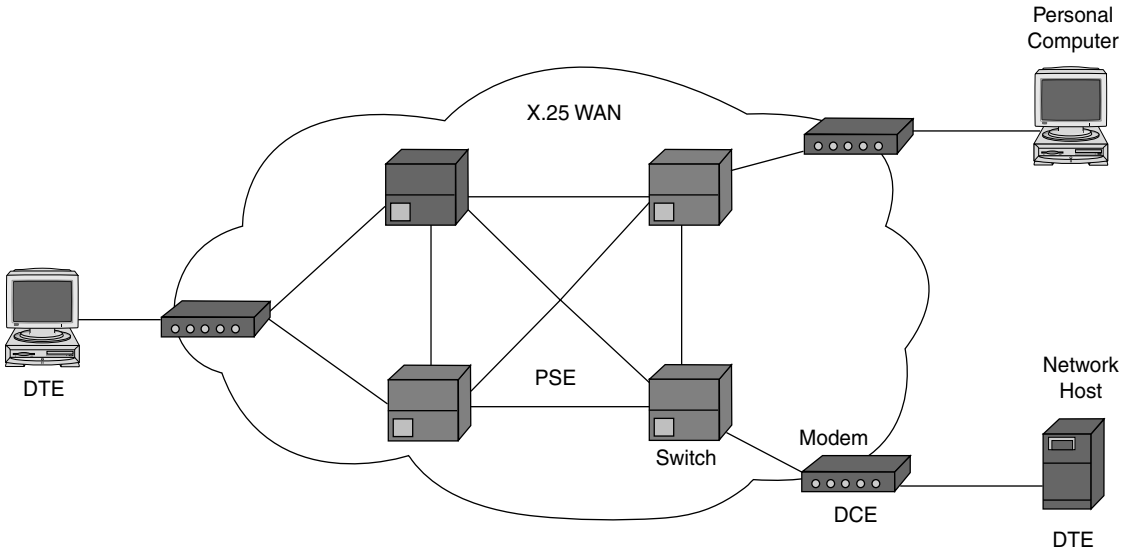


FIGURE 17.6.7 DTEs, DCEs, and PSEs make up an X.25 network.

X.25

For roughly 20 years, X.25 was the dominant player in the WAN packet-switching technology until frame relay, SMDS, and ATM appeared. X.25 has been around since the mid-1970s and so is pretty well debugged and stable. It was originally approved in 1976 and subsequently revised in 1977, 1980, 1984, 1988, 1992, and 1996. It is currently one of the most widely used interfaces for data communication networks. There are literally no data errors on modern X.25 networks.

X.25 is a communications packet-switching protocol designed for the exchange of data over a WAN. It is regarded as a standard, a network, or an interface protocol. It is a popular standard for packet-switching networks approved in 1976 by the International Telecommunication Union—Telecommunication Standardization Sector (ITU-T) for WAN communications. It defines how connections between user devices and network devices are established and maintained. X.25 uses a connection-oriented service that ensures that packets are transmitted in order. Through statistical multiplexing, X.25 enables multiple users to share bandwidth, as it becomes available, therefore ensuring flexible use of network resources among all users. X.25 is also an interface protocol in that it spells the required interface protocols that enable a DTE to communicate with data circuit-terminating equipment (DCE), which provides access to the network. The DTE-DCE link provides full-duplex multiplexing allowing a virtual circuit to transmit in either direction.

X.25 network devices fall into three general categories: DTE, DCE, and packet-switching exchange (PSE). DTE devices are user end systems that communicate across the X.25 network. They are usually terminals, personal computers, or network hosts, and are located on the premises of individual subscribers. DCE devices are carrier's equipment, such as modems and packet switches, that provide the interface between DTE devices and a PSE and are generally located in the carrier's facilities. PSEs are switches that compose the bulk of the carrier's network. They transfer data from one DTE device to another. Figure 17.6.7 illustrates the relationships between the three types of X.25 network devices.

The packet assembler/disassembler (PAD) is a device commonly found in X.25 networks. PADs are used when a DTE device is too simple to implement the full X.25 functionality. The PAD is located between a DTE device and a DCE device, and it performs three primary functions: buffering, packet assembly, and packet disassembly. The PAD buffers data sent to or from the DTE device. It also assembles outgoing data into packets and forwards them to the DCE device; this includes adding an X.25 header. Finally, the PAD disassembles incoming packets before forwarding the data to the DTE; this includes removing the X.25 header.

A virtual circuit is a logical connection created to ensure reliable communication between two network devices. Two types of X.25 virtual circuits exist:

- *Switched Virtual Circuits (SVCs)*: SVCs are very much like telephone lines; a connection is established, data are transferred, and then the connection is released. They are temporary connections used for sporadic data transfers.
- *Permanent Virtual Circuits (PVCs)*: A PVC is similar to a leased line in that the connection is always present. PVCs are permanently established connections used for frequent and consistent data transfers. Therefore, data may always be sent, without any call setup.

Maximum packet sizes vary from 64 to 4096 bytes, with 128 bytes being a default on most networks.

X.25 users are typically large organizations with widely dispersed and communications-intensive operations in sectors such as finance, insurance, transportation, utilities, and retail. For example, X.25 is often chosen for zero-error tolerance applications by banks involved in large-scale transfers of funds, or by government uses that manage electrical power networks.

Frame Relay

Frame relay is a simplified form of packet switching (similar in principle to X.25) in which synchronous frames of data are routed to different destinations depending on header information. It is basically an interface used for WAN. It is used to reduce the cost of connecting remote sites in any application that would typically use expensive leased circuits.

Frame relay is an *interface*, a method of multiplexing traffic to be submitted to a WAN. Carriers build frame relay networks using switches. The physical layout of a sample frame relay network is depicted in Fig. 17.6.8. The CSU/DSU is the channel service unit/data service unit. This unit provides a "translation" between the telephone company's equipment and the router. The router actually delivers information to the CSU/DSU over a serial connection, much like the computer uses a modem, only at a much higher speed.

All major carrier networks implement PVCs. These circuits are established via contract with the carrier and typically are built on a flat-rate basis. Although SVCs have standards support and are provided by the major frame relay backbone switch vendors, they have not been widely implemented in customer equipment or carrier networks.

Two major frame relay devices are frame relay access devices (FRADs) and routers. Stand-alone FRADs typically connect small remote sites to a limited number of locations. FRAD is also known as *frame relay assembler/disassembler*. Frame relay routers offer more sophisticated protocol handling than most FRADs. They may be packaged specifically for frame relay use, or they may be general-purpose routers with frame relay software.

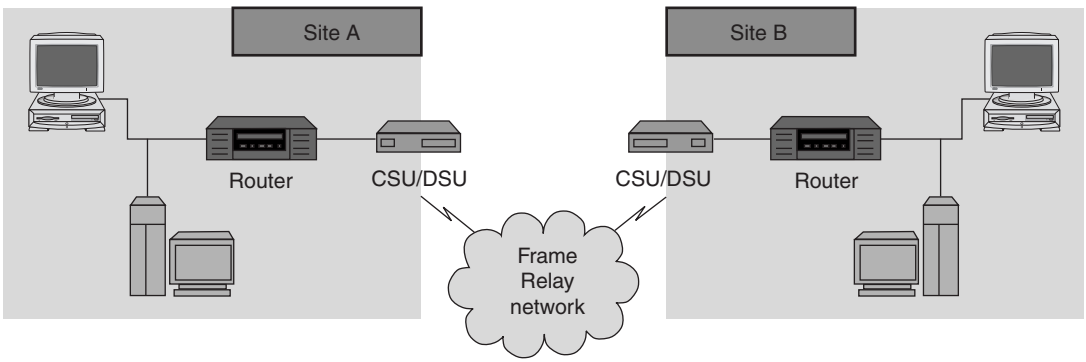


FIGURE 17.6.8 Physical layout of a typical frame relay network.

Frame relay is the fastest growing WAN technology in the United States. In North America it is fast taking on the role that X.25 has had in Europe. It is used by large corporations, government agencies, small businesses, and even Internet service providers (ISPs). The demand for frame relay services is exploding, and for two very good reasons—speed and economics. Frame relay is consistently less expensive than equivalent-leased services and provides the bandwidth needed for other services such as LAN routing, voice, and fax.

INTERNET

The Internet is a global network of computer networks (or WAN) that exchange information via telephone, cable television, wireless networks, and satellite communication technologies. It is being used by an increasing number of people worldwide. As a result, the Internet has been growing exponentially with the number of machines connected to the network and the amount of network traffic roughly doubling each year. The Internet today is fundamentally changing our social, political, and economic structures, and in many ways obviating geographic boundaries.

Internet Protocol Suite

The Internet is a combination of networks, including the Arpanet, NSFnet, regional networks such as NY sernet, local networks at a number of universities and research institutions, and a number of military networks. Each network on the Internet contains anywhere from two to thousands of addressable devices or nodes (computers) connected by communication channels. All computers do not speak the same language, but if they are going to be networked they must share a common set of rules known as *protocols.* That is where the two most critical protocols, transmission control protocol/Internet-working protocol (TCP/IP), come in. Perhaps the most accurate name for the set of protocols is the *Internet protocol suite*. (TCP and IP are two of the protocols in this suite.) TCP/IP is an agreed-upon standard for computer communication over Internet. The protocols are implemented in software that runs on each node.

The TCP/IP is a layered set of protocols developed to allow computers to share resources across a network. Figure 17.6.9 shows the Internet protocol architecture. The figure is by no means exhaustive, but shows the major protocols and application components common to most commercial TCP/IP software packages and their relationship.

As a layered set of protocols, Internet applications generally use four layers:

- *Application Layer*: This is where application programs that use the Internet reside. It is the layer with which end users normally interact. Some application-level protocols in most TCP/IP implementations include FTP, TELNET, and SMTP. For example, FTP (file transfer protocol) allows a user to transfer files to and from computers that are connected to the Internet.
- *Transport Layer*: It controls the movement of data between nodes. TCP is a connection-based service that provides services need by many applications. User datagram protocol (UDP) provides connectionless services.
- *Internet Layer*: It handles addressing and routing of the data. It is also responsible for breaking up large messages and reassembling them at the destination. IP provides the basic service of getting datagrams to their destination. Address resolution protocol (ARP) figures out the unique address of devices on the network from their IP addresses.
- *Network Layer*: It supervises addressing, routing, and congestion control. Protocols at this layer are needed to manage a specific physical medium, such as Ethernet or a point-to-point line.

TCP/IP is built on connectionless technology. IP provides a *connectionless*, *unreliable*, *best-effort* packet delivery service. Information is transferred as a sequence of datagrams. Those datagrams are treated by the network as completely separate.

TCP sends datagrams to IP with the Internet address of the computer at the other end. The job of IP is simply to find a route for the datagram and get it to the other end. In order to allow gateways or other intermediate

Application Layer	TELNET, FTP, Finger, Http, Gopher, SMTP, and so forth	DNS, RIP, SNMP, and so forth	
Transport Layer	TCP	UDP	
Internet Layer	IP		ARP
Network Layer	Ethernet, Token ring, X.25, FDDI, ISDN, SMDS, DWDM, Frame Relay, ATM, SONET/SDH, Wireless, xDSL, and so forth		

FIGURE 17.6.9 Abbreviated Internet protocol suite.

systems to forward the datagram, it adds its own header, as shown in Fig. 17.6.10. The main things in this header are the source and destination Internet address (32-bit addresses, such as 128.6.4.194), the protocol number, and another checksum. The source Internet address is simply the address of your machine. The destination Internet address is the address of the other machine. The protocol number tells IP at the other end to send the datagram to TCP. Although most IP traffic uses TCP, there are other protocols that can use IP, so one has to tell IP which protocol to send the datagram to. Finally, the checksum allows IP at the other end to verify that

Bit 0 31

Version (4)	IHL (4)	Service Type (8)	Total Length (16)	
Identification (16)			Flags (3)	Fragment Offset (13)
Time to Live (8)		Protocol (8)	Header Checksum (16)	
Source Address (32)				
Destination Address (32)				
Options (Variable)				Padding (Variable)

FIGURE 17.6.10 IP header format (20 bytes).

the header was not damaged in transit. IP needs to be able to verify that the header did not get damaged in transit, or it could send a message to the wrong place. After IP has tacked on its header, the message looks like what is in Fig. 17.6.10.

Addresses and Addressing Scheme

For IP to work, every computer must have its own number to identify itself. This number is called the IP address. You can think of an IP address as similar to your telephone number of postal address. All IP addresses on a particular LAN must start with the same numbers. In addition, every host and router on the Internet has an address that uniquely identifies it and also denotes the network on which it resides. No two machines can have the same IP address. To avoid addressing conflicts, the network numbers have been assigned by the InterNIC (formerly known simply as NIC).

Blocks of IP addresses are assigned to individuals or organizations according to one of three categories—Class A, Class B, or Class C. The *network* part of the address is common for all machines on a local network. It is similar to a postal zip code that is used by a post office to route letters to a general area. The rest of the address on the letter (i.e., the street and house number) are relevant only within that area. It is only used by the local post office to deliver the letter to its final destination. The *host* part of the IP address performs this same function. There are five types of IP addresses:

- *Class A format*: 126 networks with 16 million hosts each; an IP address in this class starts with a number between 0 and 127
- *Class B format*: 16,382 networks with up to 64K hosts each; an IP address in this class starts with a number between 128 and 191
- *Class C format*: 2 million networks with 254 hosts each; an IP address in this class starts with a number between 192 and 223
- *Class D format*: Used for multicasting, in which a datagram is directed to multiple hosts
- *Class E format*: Reserved for future use

The IP address formats for the three classes are shown in Fig. 17.6.11.

IPv6

Most of today's Internet uses Internet Protocol Version 4 (IPv4), which is now nearly 25 years old. Because of the phenomenal growth of the Internet, the rapid increase in palmtop computers, and the profusion of smart cellular phones and PDAs, the demand for IP addresses has outnumbered the limited supply provided by IPv4. In response to this shortcoming of IPv4, the Internet Engineering Task Force (IETF) approved IPv6 in 1997.

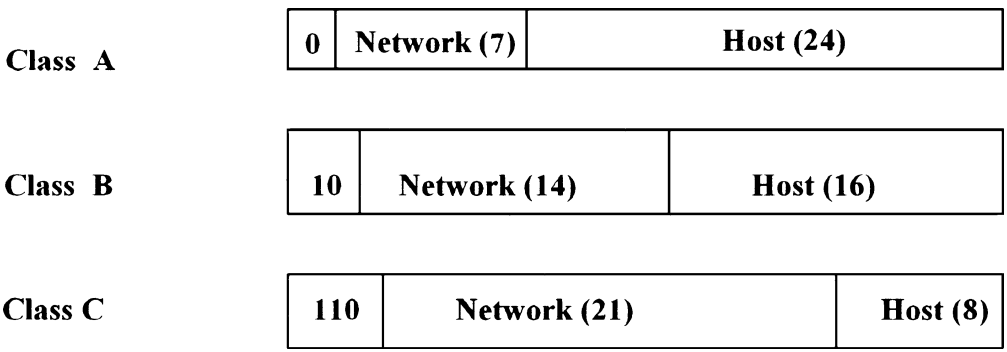


FIGURE 17.6.11 IP Address formats.

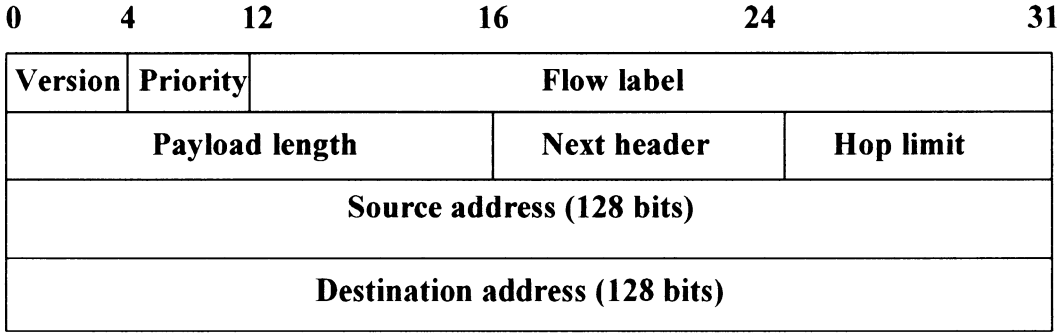


FIGURE 17.6.12 IPv6 header format.

IPv4 will be replaced by Internet Protocol Version 6 (IPv6), which is sometimes called the Next Generation Internet Protocol (or IPng). IPv6 adds many improvements and fixes a number of problems in IPv4, such as the limited number of available IPv4 addresses.

With only a 32-bit address field, IPv4 can assign only 2^{32} different addresses, i.e., 4.29 billion IP addresses, which are inadequate in view of rapid proliferation of networks and the two-level structure of the IP addresses (network number and host number). To solve the problem of severe IP address shortage, IPv6 uses 128-bit addresses instead of the 32-bit addresses of IPv4. That means IPv6 can have as many as 2^{128} IP addresse, which is roughly 3.4×10^{38} or about 340 billion billion billion billion unique addresses.

The IPv6 packet consists of the IPv6 header, routing header, fragment header, the authentication header, TCP header, and application data. The IPv6 packet header is of fixed length, whereas the IPv4 header is of variable length. The IPv6 header consists of 40 bytes as shown in Fig. 17.6.12. It consists of the following fields:

- *Version* (*4 bits*): This is the IP version number, which is 6.
- *Priority* (*4 bits*): This field enables a source to identify the priority of each packet relative to other packets from the same source.
- *Flow Label* (*24 bits*): The source assigns the flow label to all packets that are part of the same flow. A flow may be a single TCP connection or a multiple of TCP connections.
- *Payload Length* (*16 bits*): This field specifies the length of the remaining part of the packet following the header.
- *Next Header* (*8 bits*): This identifies the type of header immediately following the header.
- *Hop Limit* (*8 bits*): This is to set some desired maximum value at the source and the field denotes the remaining number of hops allowed for the packet. It is decremented by 1 at each node the packet passes and the packet is discarded when the hop limit becomes zero.
- *Source Address* (*128*): The address of the source of the packet.
- *Destination Address* (*128 bits*): The address of the recipient of the packet.

There are three types of IPv6 addresses:

1. Unicast is used to identify a single interface.
2. Anycast identifies a set of interfaces. A source may use an anycast address to contact any node from a group of nodes.
3. Multicast identifies a set of interfaces. A packet with a multicast address is delivered to all members of the group.

IPv6 is expected to gradually replace IPv4, with the two coexisting for a number of years during a transition period. IPv6 may be most widely deployed in mobile phones, PDAs, and other wireless terminals in the future.

BISDN AND ATM

ISDN is a high-speed communication network, which allows voice, data, text, graphics, music, video, and other source material to be transmitted simultaneously across the world using end-to-end digital connectivity. ISDN stands for Integrated Services Digital Network. "Digital network" means that the user is given access to a telecom network ensuring high-quality transmission via digital circuits, while "integrated services" refers to the simultaneous transmission of voice and data services over the same wires. This way, computers can connect directly to the telephone network without first converting their signals to an analog form using modems. This integration brings with it a host of new capabilities combining voice, data, fax, and sophisticated switching. And because ISDN uses the existing local telephone wiring, it is equally available to home and business customers. ISDN was intended to eventually replace the traditional plain old telephone service (POTS) phone lines with a digital network that would carry voice, data, and video.

ISDN service is available today in most major metropolitan areas and probably will be completely deployed throughout the United States very soon. Many ISPs now sell ISDN access. However, the idea of using existing copper wiring to provide this network decreased ISDN capabilities in reality. When the digital video systems started to develop in the 1980s, it was soon noticed that the maximum bandwidth (2.048 Mbps) of the ISDN is not enough. That is why broadband ISDN (BISDN) was born.

BISDN is a digital network operating at data rates in excess of 2.048 Mbps—the maximum rate of standard ISDN. BISDN is a second generation of ISDN. BISDN is not only an improved ISDN but also a complete redesign of the "old" ISDN, now called narrowband ISDN. It consists of ITU-T communication standards designed to handle high-bandwidth applications such as video. The key characteristic of broadband ISDN is that it provides transmission channels capable of supporting rates greater than the primary ISDN rate. Broadband services are aimed at both business applications and residential subscribers.

BISDN's foundation is cell switching, and the international standard supporting it is *Asynchronous Transfer Mode* (ATM). Because BISDN is a blueprint for ubiquitous worldwide connectivity, standards are of the utmost importance. Major strides have been made in this area by the International Telecommunications Union-Telecommunications (ITU-T) during the past decade. More recently, the ATM Forum has advanced that agenda.

ATM is a fast packet-oriented transfer mode based on asynchronous time-division multiplexing. The words *transfer mode* say that this technology is a specific way of transmitting and switching through the network. The term *asynchronous* refers to the fact that the packets are transmitted using asynchronous techniques (e.g., on demand), and the two end points need not have synchronized clocks. ATM will support both circuit switched and packet switched services. ATM can handle any kind of information, i.e., voice, data, image, text, and video in an integrated manner.

An ATM network is made up of an ATM switch and ATM end points. An ATM switch is responsible for cell transit through an ATM network. An ATM end point (or end system) contains an ATM network interface adapter. Examples of ATM end points are workstations, routers, digital service units (DSUs), LAN switches, and video coder-decoders (CODECs). An ATM network consists of a set of ATM switches interconnected by point-to-point ATM links or interfaces. ATM switches support two primary types of interfaces: user-network interface (UNI) and network-network interface (NNI). The UNI connects ATM end systems (such as hosts and routers) to an ATM switch. The NNI connects two ATM switches.

In ATM the information to be transmitted is divide into short 53 byte packets or cells. There are reasons for such a short cell length. First, ATM must deliver real-time service at low bit rates. Thus the size allows ATM to carry multiple forms of traffic. Both time-sensitive traffic (voice) and time-insensitive traffic (data) can be carried with the best possible balance between efficiency and minimal packetization delay. Second, using short, fixed-length cells allows for time-efficient and cost-effective hardware such as switches and multiplexers.

Each ATM cell consists of 48 bytes for information field and 5 bytes for header. The header is used to identify cells belonging to the same virtual channel and thus used in appropriate routing. The ATM cell structure is shown in Fig. 17.6.13. The cell header comes in two forms: the UNI header and the NNI header. The UNI is described as the point where the user enters the network. The NNI is the interface between networks. The typical header therefore looks like that shown in Fig. 17.6.14 for the UNI. The header is slightly different for NNI, as shown in Fig. 17.6.15.

ATM is connection-oriented and connections are identified by the virtual channel identifier (VCI). A virtual channel (VC) represents a given path between the user and the destination. A virtual path (VP) is created by multiple virtual channels heading to the same destination. The relationship between virtual channels and

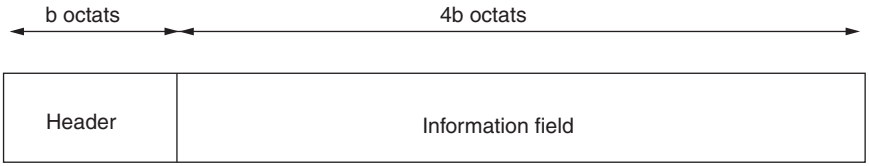
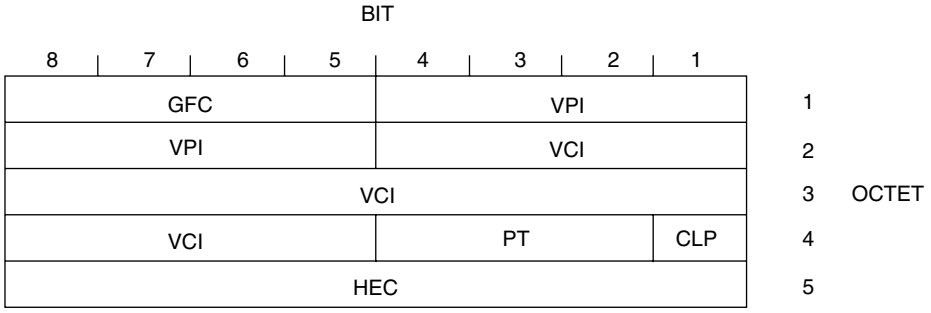
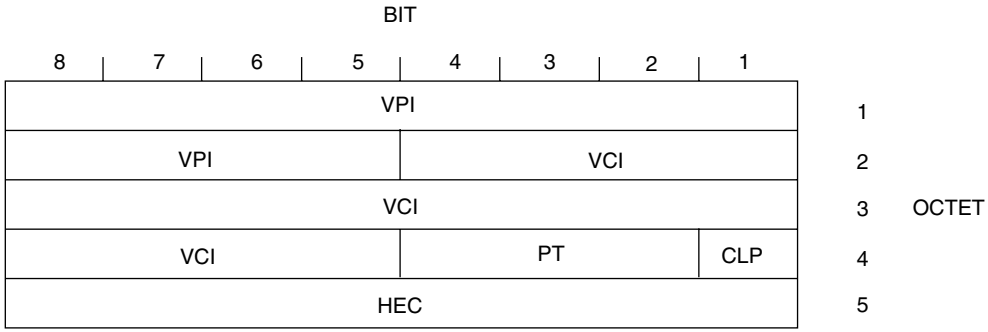


FIGURE 17.6.13 ATM cell structure.



VPI	virtual path identifier	PT	payload type
VCI	virtual channel indentifier	CLP	cell loss priority
HEC	header error control	GFC	ganaric flow control

FIGURE 17.6.14 ATM cell header for UNI.



VPI	virtual path identifier	PT	payload type
VCI	virtual channel indentifier	CLP	cell loss priority
HEC	header error control		

FIGURE 17.6.15 ATM cell header for NNI.

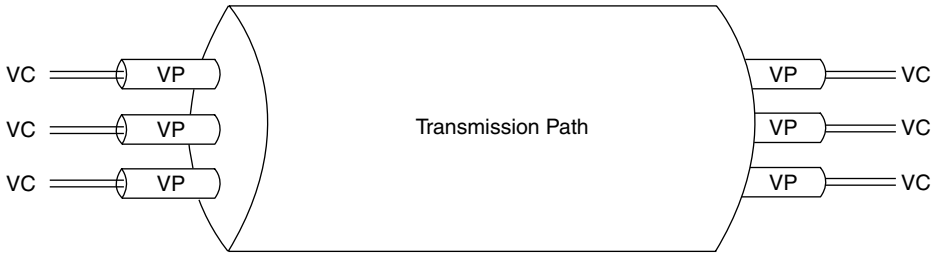


FIGURE 17.6.16 Relationship between virtual channel, virtual path, and transmission path.

virtual paths is illustrated in Fig. 17.6.16. A virtual channel is established at connection time and torn down at termination time. The establishment of the connections includes the allocation of a virtual channel identifier and/or virtual path identifier (VPI) and also includes the allocation of the required resources on the user access and inside the network. These resources, expressed in terms of throughput and quality of service (QoS), can be negotiated between user and network either before the call set up or during the call. Having both virtual paths and channels make it easy for the switch to handle many connections with the same origin and destination.

ATM can be used in existing twisted pair, fiber-optic, coaxial, and hybrid fiber/coax (HFC), SONET/SDH, T1, E1, T3, E3, E4, and so on, for LAN and WAN communications. ATM is also compatible with wireless and satellite communications.

Figure 17.6.17 depicts the architecture for the BISDN protocol. It is evident that the BISDN protocol uses a three-plane approach. The user plane (U-plane) is responsible for user information transfer including flow control and error control. The U-plane contains all of the ATM layers. The control plane (C-plane) manages the call-control and connection-control functions. The C-plane shares the physical and ATM layers with the U-plane, and contains ATM adaptation layer (AAL) functions dealing with signaling. The management plane (M-plane) includes plane management and layer management. This plane provides the management functions and the capability to transfer information between the C- and U-planes. The layer management performs layer-specific management functions, while the plane management deals with the complete system.

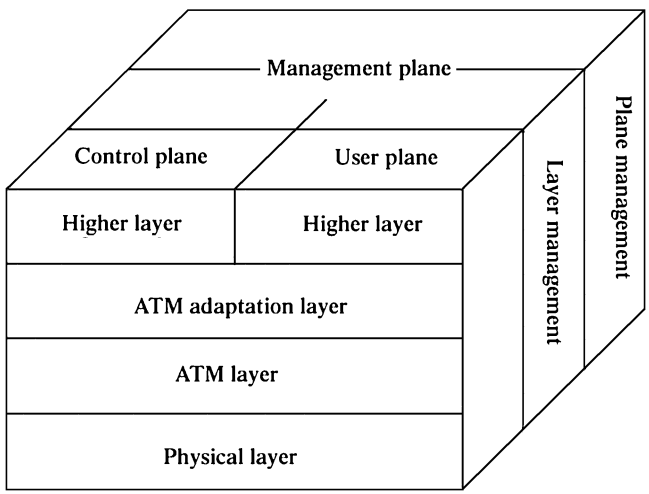


FIGURE 17.6.17 BISDN protocol reference model.

Figure 17.6.17 also shows how ATM fits into BISDN. The ATM system is divided into three functional layers, namely, the physical layer, the ATM layer, and the ATM adaptation layer.

BISDN access can be based on a single optical fiber per customer site. A variety of interactive and distribution broadband services is contemplated for BISDN: high-speed data transmission, broadband video telephony, corporate videoconferencing, video surveillance, high-speed file transfer, TV distribution (with existing TV and/or high-definition television), video on demand, LAN interconnection, hi-fi audio distribution, and so forth.