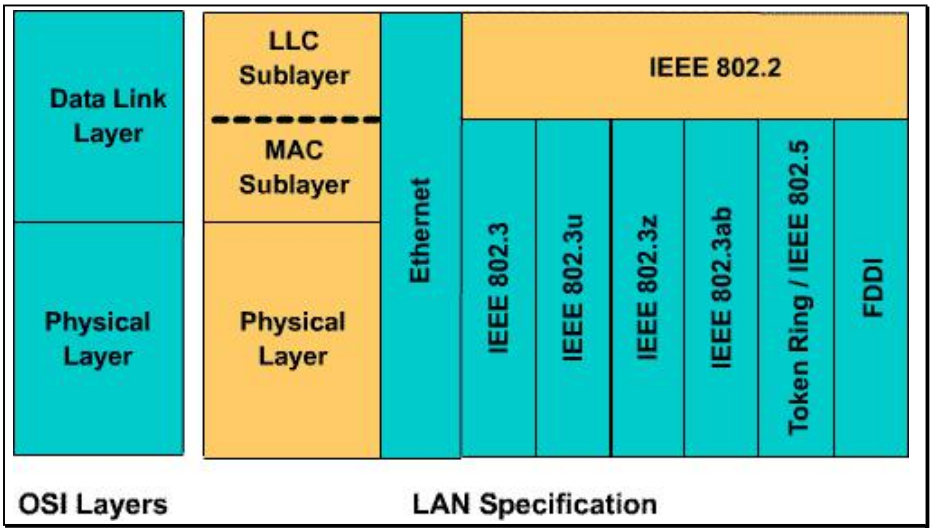
Network Types

2.1 LAN Standards

Figure 1: LAN Standards



Local-area networks (LANs) are high-speed, low-error data networks that cover a relatively small geographic area (up to a few thousand meters). LANs connect workstations, peripherals, terminals, and other devices in a single building or other geographically limited area. LAN standards specify cabling and signaling at the physical and data link layers of the Open System Interconnection (OSI) model. Figure [1] shows how three popular LAN protocols—Ethernet, Token Ring, and FDDI—map to the OSI reference model.

The Institute of Electrical and Electronic Engineers (IEEE) is a professional organization that defines network standards. The IEEE standards are the predominant and best known LAN standards in the world today. IEEE 802.3 specifies the physical layer, Layer 1, and the channel-access portion of the data link layer, Layer 2.

The IEEE divides the OSI data link layer into two separate sublayers. Recognized IEEE sublayers are:

■ Media Access Control (MAC) (transitions down to media)

■ Logical Link Control (LLC) (transitions up to the network layer) LLC IEEE created the LLC sublayer to allow part of the data link layer to function independently from existing technologies. This layer provides versatility in services to network layer protocols that are above it, while communicating effectively with the variety of technologies below it. The LLC, as a sublayer, participates in the encapsulation process.

An LLC header tells the data link layer what to do what a packet once a frame is received. For example, a host will receive a frame and then look in the LLC header to understand that the packet is destined for the IP protocol at the network layer.

MAC The Media Access Control (MAC) sublayer deals with the protocols that a host follows in order to access the physical media. The IEEE 802.3 MAC specification defines MAC addresses, which enable multiple devices to uniquely identify one another at the data link layer. The MAC sublayer maintains a table of MAC address(physical address) of devices. Each device is assigned and must have a unique MAC address if the device is to participate on the network.

Ethernet

Figure 1: CSMA/CD

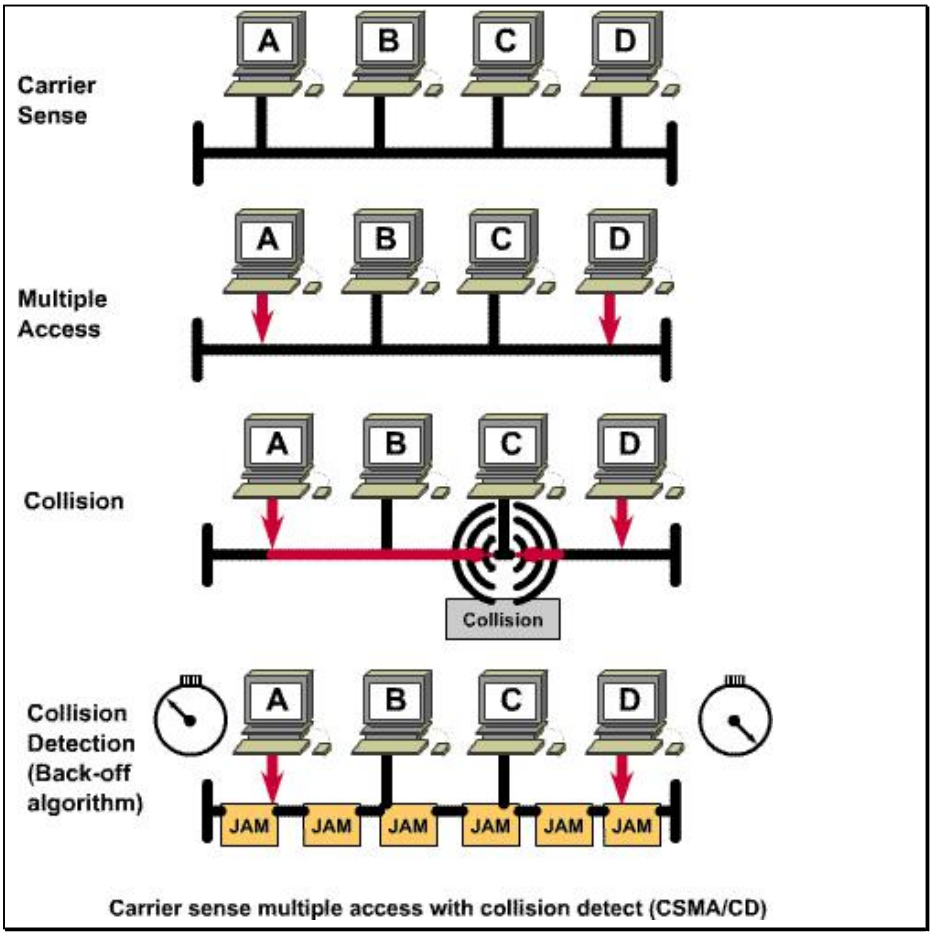
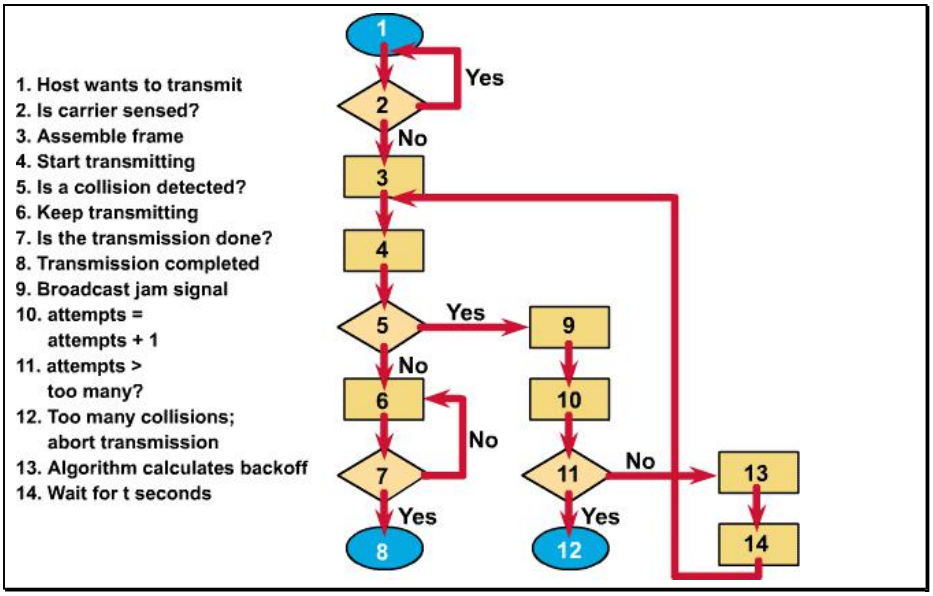


Figure 2: CSMA/CD



Ethernet refers to the family of LAN implementations that includes four main categories:

■**Ethernet and IEEE 802.3**: These LAN specifications operate at 10 megabits per second (Mbps) over coaxial cable.

■**100-Mbps Ethernet**: This single LAN specification, also known as Fast Ethernet, operates at 100 Mbps over twisted-pair cable.

■**Gigabit Ethernet**: An extension of the IEEE 802.3 Ethernet standard, Gigabit Ethernet increases speed tenfold over Fast Ethernet, to 1000 Mbps, or 1 gigabit per second (Gbps).

■**10000-Mbps (10-Gbps) Ethernet**: This version will soon be implemented.

Ethernet signals, or frames, are transmitted to every station connected to the network. Before transmitting, a computer first listens to the channel. If the channe lis idle, the computer sends its data. After a transmission has been sent, the computers on the network once again compete for the next available idle time in order to send another frame. This contention for idle channel time means that no station has an advantage on the network over another.

Ethernet uses *carrier sense multiple access collision detect* (CSMA/CD) to determine which station on the network can talk at any particular time (see Figure [1]).

When a station is transmitting, the signal is referred to as a carrier. The Media Access Control (MAC) "senses" the carrier and consequently restrains itself from broadcasting a signal. If there is no carrier, a station waiting to transmit will know that it is free to do so. This is the *carrier sense* part of the protocol.

There is no priority assigned to any particular station; therefore, all stations on the network have equal access. This is the *multiple access* part of the protocol.
If two or more stations attempt a transmission simultaneously, a "collision" occurs. The stations are alerted to the collision, and they execute a back-off algorithm that randomly reschedules transmission of the frame. This scenario prevents the machines from attempting to "talk" at the same time repeatedly. Collisions are normally resolved in microseconds. This is the *collision detect* part of the protocol. Figure [2] summarizes the CSMA/CD processes.

Fast Ethernet

Figure 1: Fast Ethernet

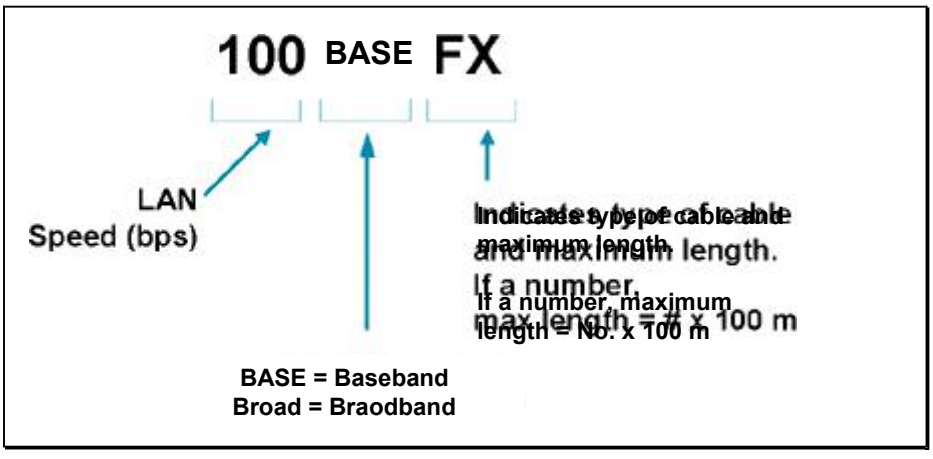


Figure 2: Fast Ethernet Specifications

Protocol	Maximum Segment Length (m)	Transmission Medium	Application
100BASE-FX	400	Two strands of multimode fiber-optic cable	
100BASE-T	100	UTP	100BASE-T function + More
100BASE-T4	100	Four pairs Category 3-5 UTP	
100BASE-TX	100	Two pairs UTP or STP	
100BASE-X	Refers to two strands/pairs, 100BASE-FX and 100BASE-TX		

Ethernet protocols are usually described as a function of data rate, maximum segment length, and medium. As faster types of Ethernet are used, more users can be added to the network without degrading the performance of the network.

The Fast Ethernet standard (IEEE 802.3u) has been established for networks that need higher transmission speeds. It raises the Ethernet speed limit from 10 Mbps to 100 Mbps (see Figure **[1]**) with only minimal changes to the existing cable structure. Data can move from 10 Mbps to 100 Mbps without protocol translation or changes to application and networking software (see Figure **[2]**). Incorporating Fast Ethernet into an existing configuration presents a host of decisions for the network manager.

Fast Ethernet is the ability to transmit and receive Ethernet packets or frames at a rate of 100 Mbps, rather than the 10-Mbps rates as Ethernet. Gigabit Ethernet switches at 1000 Mbps and several Cisco products support this technology. For example, each site in the network must determine:

- The number of users that really need the higher throughput
- Which segments of the backbone need to be reconfigured specifically for 100BASE-T
- The necessary hardware to connect the 100BASE-T segments with existing 10BASE-T segments

Gigabit Ethernet

Figure 1: Gigabit Ethernet Specifications

Protocol	Maximum Segment Length (m)	Transmission Medium
1000BASE-LX	3 km (single mode) > 500m (multimode)	Long-wave laser over single mode and multimode fiber
1000BASE-SX	500m	Short-wave laser over multimode fiber
1000BASE-CS	25m	Balanced shielded 150-ohm two-pair STP copper cable
1000BASE-T	100m	Category 5 UTP copper wiring

Gigabit Ethernet is an extension of the IEEE 802.3 Ethernet standard.

Gigabit Ethernet builds on the Ethernet protocol but increases speed tenfold over Fast Ethernet, to 1000 Mbps, or 1 Gbps. It promises to be a dominant player in high-speed LAN backbones and server connectivity. Because Gigabit Ethernet uses Ethernet to significant advantage, network managers will be able to take advantage of their existing knowledge base to manage and maintain gigabit networks.

The Gigabit Ethernet specification addresses four forms of transmission media:

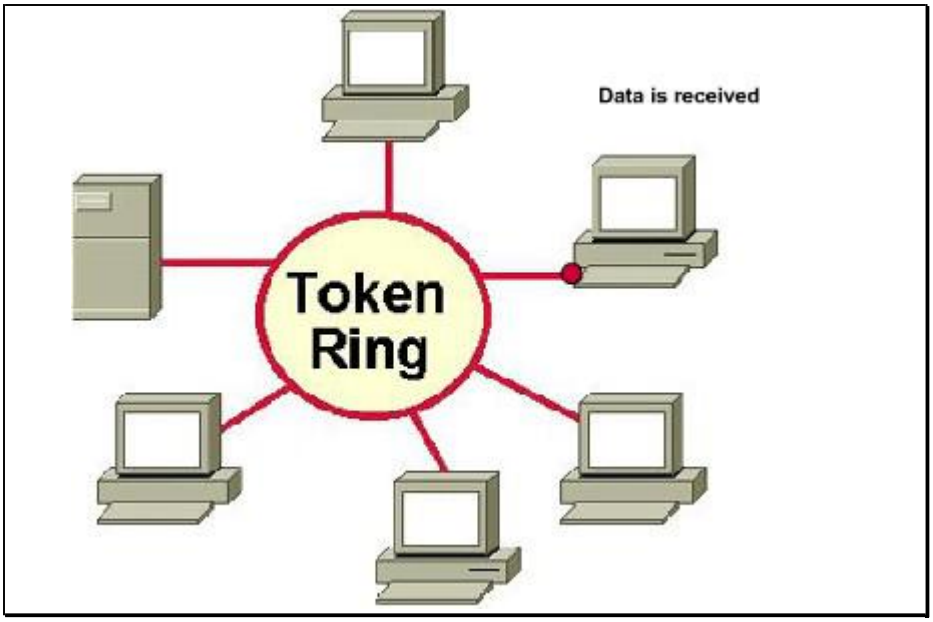
- **1000BASE-LX**: Long-wave laser over single-mode and multimode fiber
- **1000BASE-SX**: Short-wave laser over multimode fiber
- **1000BASE-CX**: Transmission over balanced, shielded, 150-ohm two-pair shielded twisted-pair (STP) copper cable
- **1000BASE-T**: Category 5 unshielded twisted-pair (UTP) copper wiring

The key application of Gigabit Ethernet is expected to be for use in the building backbone for interconnection of wiring closets. A gigabit multilayer switch in the building data center aggregates the traffic in the building and provides connection to servers by way of Gigabit Ethernet or Fast Ethernet. WAN connectivity can be provided by traditional routers or by way of ATM switching.

Gigabit Ethernet can also be used for connecting buildings on the campus to a central multilayer gigabit switch located at the campus data center. Servers located at the campus data center are also connected to the gigabit multilayer switch that provides connectivity to the entire campus.

Token Ring

Figure 1: ATM and Cell Switching



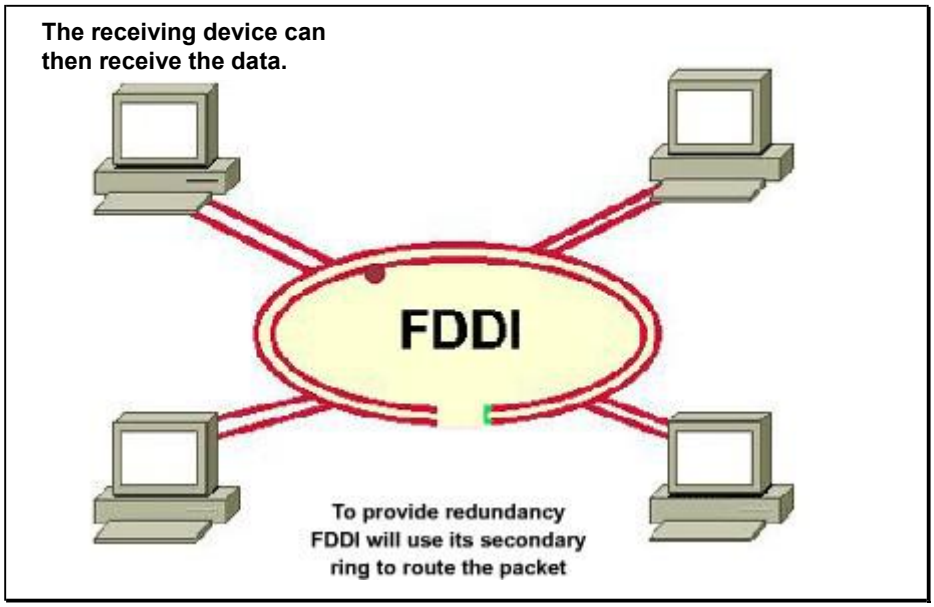
Token Ring technology was originally developed in the 1970s by IBM and remains the company's primary LAN technology. Token Ring is second only to Ethernet/IEEE 802.3 in general LAN popularity. The Token Ring network specifies a star, with all end stations attached to a device called a multistation access unit (MSAU).

Token-passing networks are deterministic, meaning that it is possible to calculate the maximum time that will pass before any end station will be able to transmit. This feature and several reliability features make Token Ring networks ideal for applications in which delay must be predictable and robust network operation is important. Factory automation environments are examples of such applications.

Collisions cannot occur in Token Ring networks. Possession of the token grants the right to transmit. If a node receiving the token has no information to send, it passes the token to the next end station. Each station can hold the token for a maximum period of time.

FDDI

298**Figure 1: FDDI**



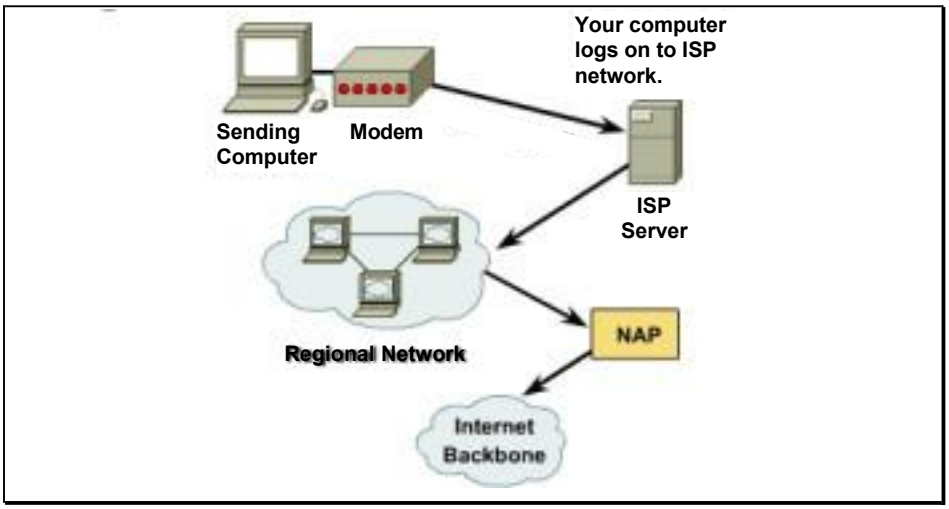
Fiber Distributed Data Interface (FDDI) was developed in the mid-1980s to fill the needs of growing high-speed engineering workstation capacity and network reliability. FDDI is fast, reliable, and it handles a lot of data well. However, it is costly, because of expensive fiber-optic cable. Main applications are legacy corporate and carrier backbones, where reliability and speed are crucial. New FDDI networks are rarely installed.

FDDI is a protocol that uses a 100-Mbps token-passing network of fiber-optic cable, with transmission distances of up to 2 kilometers (km). FDDI uses a dual-ring architecture to provide redundancy. It also allows traffic on each ring to flow in opposite directions (called counter-rotating). The dual rings consist of a primary and a secondary ring. During normal operation, the primary ring is used for data transmission and the secondary ring remains idle.

2.2 WANs

Global Internet

Figure 1: How Internet Components Work Together

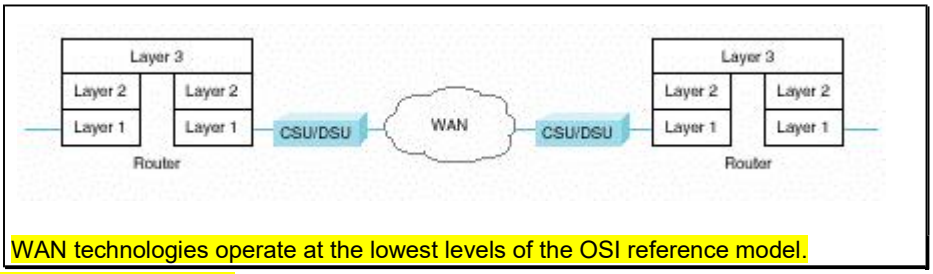


By definition, an internet is a network of networks, and the Internet is made up of thousands of large and small networks that are themselves all over the world. How do the components of the Internet relate to the typical Internet user? When you click to send an e-mail message, the e-mail client application formats the data, and it goes through the following process:

1. The data is broken into manageable chunks, called packets.
2. The networking protocols add header and trailer information.
3. The binary 1s and 0s are converted to electrical signals or light pulses to travel over the physical medium.
4. If your computer is on a LAN, the data travels over the local network to a server or router that is connected to a phone line or dedicated leased line.
5. If a modem connection is used, the packets are encapsulated inside a link protocol, such as Point-to-Point Protocol (PPP) or Serial Line Internet Protocol (SLIP), and the digital signals are modulated to travel over the analog phone line.
6. The signals reach the Internet service provider's (ISP's) remote access server, which is configured to accept dial-in connections, or you might have a direct dedicated link to the ISP. With a dial-in account, you log on to the server by entering a username and password.
7. The computer becomes a remote node on the ISP's local network.
8. The data travels from the ISP's server to the regional network to which the ISP is connected (if you use one of the largest national ISPs, this step may be skipped).
9. Your data travels through one of the major network access points (NAPs), if necessary, and onto the commercial Internet backbone.
10. At the other end, the data goes through another NAP, another regional network, and then the ISP at the receiving side, which delivers the data to the destination computer (for example, the ISP's mail server).
11. The data is finally delivered to the intended user when the user's e-mail client connects to the ISP's or company's mail server and downloads the contents of the mailbox setup for that user account.

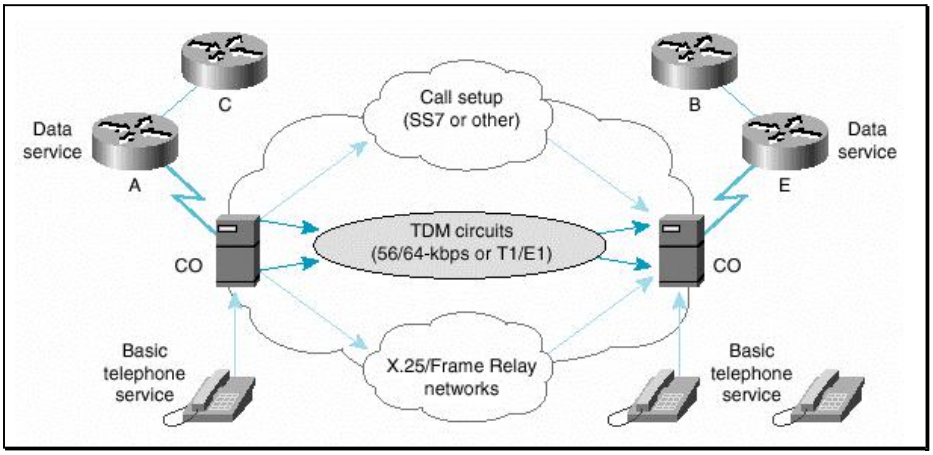
WAN Technology Overview

Figure 1: WAN Technologies



WAN technologies operate at the lowest levels of the OSI reference model.

Figure 2: WAN Services



A WAN is a data communications network that operates beyond a LAN's geographic scope. One way that a WAN is different from a LAN is that, with a WAN, you must subscribe to an outside WAN service provider, such as a regional Bell operating company (RBOC) to use WAN carrier network services. A WAN uses data links, such as Integrated Services Digital Network (ISDN) and Frame Relay, that are provided by carrier services to access bandwidth over wide-area geographies.

A WAN connects the locations of an organization to each other, to locations of other organizations, to external services (such as databases), and to remote users. WANs generally carry a variety of traffic types, such as voice, data, and video. WAN technologies function at the three lowest layers of the OSI reference model: the physical layer, the data link layer, and the network layer. Figure **[1]** illustrates the relationship between the common WAN technologies and the OSI reference model.

WAN Services

Telephone and data services are the most commonly used WAN services. Telephone and data services are connected from the building point of presence (POP) to the WAN provider's central office (CO). The CO is the loc subscriber lines occurs.

An overview of the WAN cloud (see in Figure [2]) organizes WAN provider services into three main types: 444

- **Call setup**—Sets up and clears calls between telephone users. Also called signaling, call setup uses a separate telephone channel not used for other traffic. The most commonly used call setup is Signaling System 7 (SS7), which uses telephone control messages and signals between the transfer points along the way to the called destination.
- **Time-division multiplexing (TDM)**—Information from many sources has bandwidth allocation on a single medium. Circuit switching uses signaling to determine the call route, which is a dedicated path between the sender and the receiver. By multiplexing traffic into fixed time slots, TDM avoids congested facilities and variable delays. Basic telephone service and ISDN use TDM circuits.
- **Frame Relay**—Information contained in frames shares bandwidth with other WAN Frame Relay subscribers. Frame Relay is statistical multiplexed service, unlike TDM, which uses Layer 2 identifiers and permanent virtual circuits. In addition, Frame Relay packet switching uses Layer 3 routing with sender and receiver addressing contained in the packet.

WAN Devices

Figure 1: WAN Devices

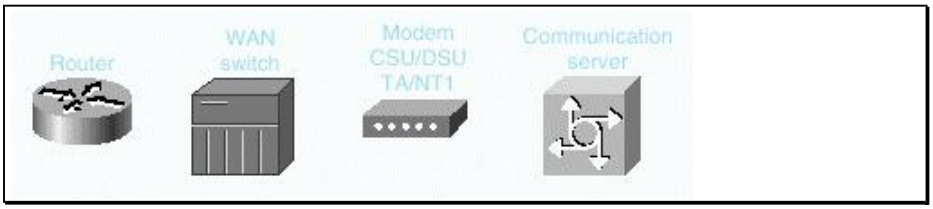
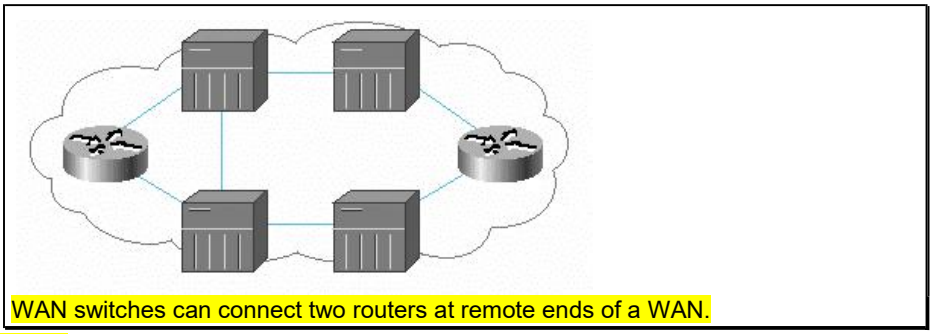
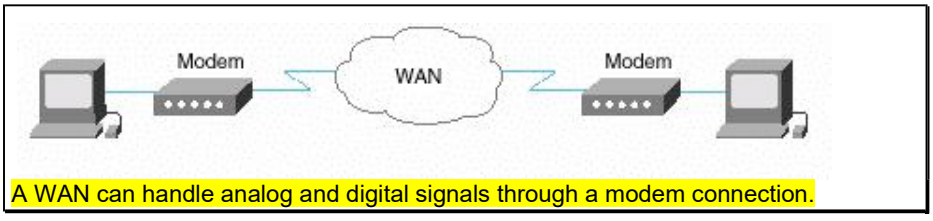


Figure 2: WAN Switches



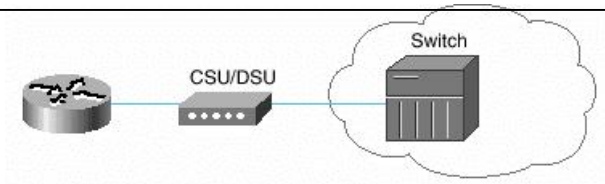
WAN switches can connect two routers at remote ends of a WAN.

Figure 3: Modems



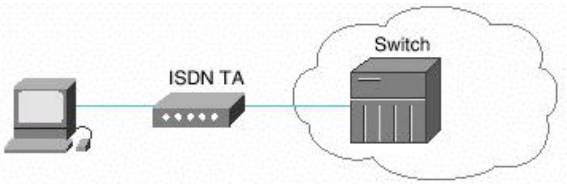
A WAN can handle analog and digital signals through a modem connection.

Figure 4: WAN Standards



In a WAN, the CSU/DSU is placed between the switch and the terminal.

Figure 5: WAN Standards



In a WAN, the TA connects the ISDN to other interfaces, such as switches.

WANs use numerous types of devices, including the following (see Figure [1]): 493

■Routers, which offer many services, including LAN and WAN interface ports.

■WAN switches, which connect to WAN bandwidth for voice, data, and video communication.

■Modems, which interface voice-grade services. Modems include *channel service units/data service units* (CSUs/DSUs) and *terminal adapter/network termination 1*(TA/NT1) devices that interface ISDN services.

■Communication servers, which concentrate dial-in and dial-out user communication.

Routers

Routers are devices that implement the network service. They provide interfaces for a wide range of links and subnetworks at a wide range of speeds. Routers are active and intelligent network devices and thus can participate in managing the network. Routers manage networks by providing dynamic control over resources and supporting the tasks and goals for networks. These goals are connectivity, reliable performance, management control, and flexibility.

WAN Switches

A WAN switch is a multiport networking device that typically switches such traffic as Frame Relay, X.25, and Switched Multimegabit Data Service (SMDS). WAN switches typically operate at the data link layer of the OSI reference model. Figure [2] illustrates two routers at remote ends of a WAN that are connected by WAN switches. In this example, the switches filter, forward, and flood frames based on the destination address of each frame.

Modems

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

CSUs/DSUs

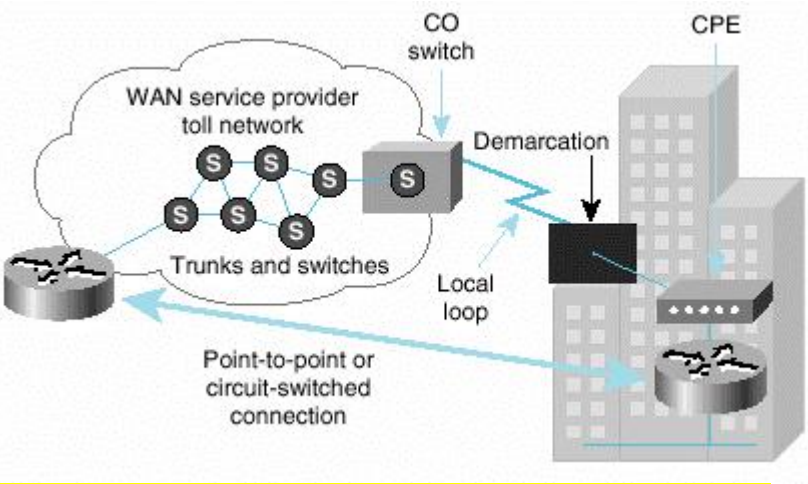
A CSU/DSU is a digital-interface device—or sometimes two separate digital devices—that adapts the physical interface on a *data terminal equipment* (DTE) device (such as a terminal) to the interface of a *data circuit-terminating equipment* (DCE) device (such as a switch) in a switched-carrier network. Figure [4] illustrates the placement of the CSU/DSU in a WAN implementation. Sometimes, CSUs/DSUs are integrated in the router box.

ISDN Terminal Adapters

An ISDN TA is a device used to connect ISDN Basic Rate Interface (BRI) 538 connections to other interfaces. A TA is essentially an ISDN modem. Figure [5] 539 illustrates the placement of a TA in an ISDN environment.

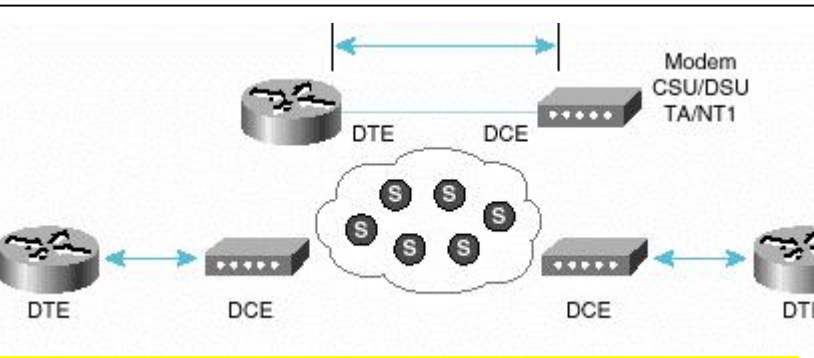
WAN Service Providers and Signaling Standards

Figure 1: WAN Service Providers



An organization makes connections to destinations as point-to-point calls.

Figure 2: DTE/DCE



Data communication over WANs interconnects DTEs so that they can share resources over a wide area.

Figure 3: WAN Link Types and Bandwidth

Line Type	Signal Standard	Bit Rate Capacity
56	DSO	56 kbps
64	DSO	64 kbps
T1	DS1	1.544 Mbps
E1	ZM	2.048 Mbps
E3	M3	34.064 Mbps
J1	Y1	2.048 Mbps
T3	DS3	44.736 Mbps
OC-1	SONET	51.84 Mbps
OC-3	SONET	155.54 Mbps
OC-9	SONET	466.56 Mbps
OC-12	SONET	622.08 Mbps
OC-18	SONET	933.12 Mbps
OC-24	SONET	1244.16 Mbps
OC-36	SONET	1866.24 Mbps
OC-48	SONET	2488.32 Mbps

Advances in technology over the past decade have made a number of additional WAN solutions available to network designers. When you're selecting an appropriate WAN solution, you should discuss the costs and benefits of each with your service providers.

When your organization subscribes to an outside WAN service provider for network resources, the provider gives connection requirements to the subscriber, such as the type of equipment to be used to receive services. As shown in Figure [1], the following are the most commonly used terms associated with the main parts of WAN services:

■**Customer premises equipment (CPE)**—Devices physically located on the subscriber's premises. Includes both devices owned by the subscriber and devices leased to the subscriber by the service provider.

■**Demarcation (or demarc)**—The point at which the CPE ends and the local loop portion of the service begins. Often occurs at the POP of a building.

■**Local loop (or "last-mile")**—Cabling (usually copper wiring) that extendsfr om the demarc into the WAN service provider's central office.

■**CO switch**—A switching facility that provides the nearest point of presence for the provider's WAN service.

■**Toll network**—The collective switches and facilities (called trunks) inside the WAN provider's cloud. The caller's traffic may cross a trunk to a primary center, then to a sectional center, and then to a regional- or international-carrier center as the call travels the long distance to its destination.

DTE/DCE

A key interface in the customer site occurs between the data terminal equipment (DTE) and the data circuit-terminating equipment (DCE). Typically, the DTE is the router, and the DCE is the device used to convert the user data from the DTE into a form acceptable to the WAN service's facility. As shown in Figure **[2]**, the DCE is the attached modem, CSU/DSU, or TA/NT1.

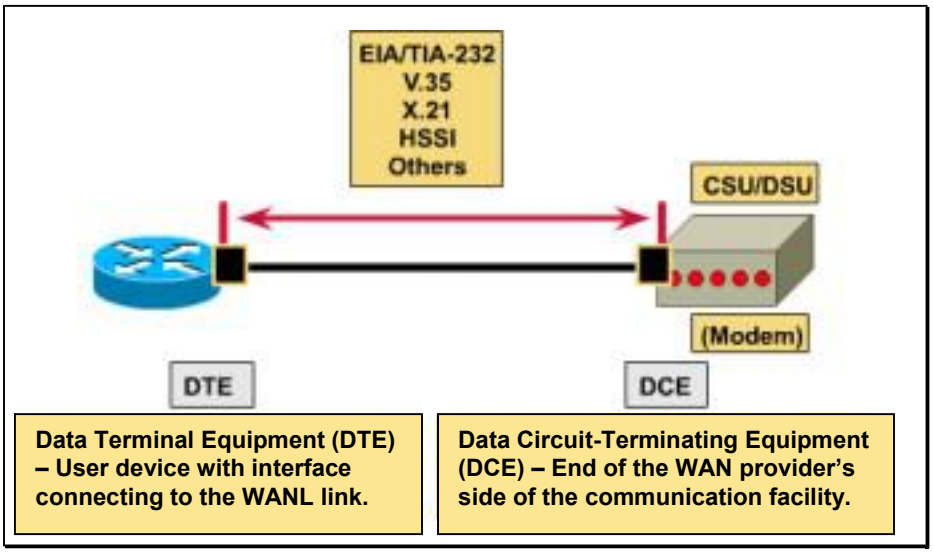
The WAN path between the DTE is called the link, circuit, channel, or line. The DCE primarily provides an interface for the DTE into the communication link in the WAN cloud. The DTE/DCE interface acts as a boundary where responsibility for the traffic passes between the WAN subscriber and the WAN provider. The DTE/DEC interface uses various protocols that establish the codes that the devices use to communicate with each other. This communication determines how call setup operates and how user traffic crosses the WAN.

WAN Signaling Standards and Capacity

WAN links can be ordered from the WAN provider at various speeds that are stated in bits per second (bps) capacity. This bps capacity determines how fast data can be moved across the WAN link. WAN bandwidth is often provisioned in the United States by using the North American Digital Hierarchy, shown in Figure [3].

WANs and Physical Layer

Figure 1: WAN and Physical Layer



The WAN physical layer protocols describe how to provide electrical, mechanical, operational, and functional connections for WAN services. Most WANS require an interconnection that is provided by a communications service provider (such as an ROBOC), an alternative carrier (such as an Internet service provider), or a post, telephone, and telegraph (PTT) agency.

The WAN physical layer also describes the interface between the DTE and the DCE. Typically, the DCE is the service provider and the DTE is the attached device. In Figure **[1]**, the services offered to the DTE are made available through a modem or a CSU/DSU.

Several physical-layer standards define the rules governing the interface between the DTE and the DCE:

■**EIA/TIA-232**—A common physical-layer interface standard developed by Electronic Industries Association (EIA) and Telecommunications Industries Association (TIA) that supports unbalanced circuits at signal speeds of up to 64 kbps. It closely resembles the V.24 specification, and was formerly known as RS-232. This standard has been in place for many years.

■**EIA/TIA-449**—A popular physical-layer interface developed by EIA and TIA. It is essentially a faster (up to 2 Mbps) version of EIA/TIA-232, 645capable of longer cable runs.

■**EIA/TIA-612/613**—A standard describing High Speed Serial Interface (HSSI), which provides access to services at T3 (45 Mbps), E3 (34 Mbps),and Synchronous Optical Network (SONET) STS-1 (51.84 Mbps) rates.The actual rate of the interface depends on the external DSU and the type of service to which it is connected.

■**V.24**—An International Telecommunication Union-Telecommunication Standardization Sector (ITU-T) standard for a physical-layer interface between DTE and DCE.

■**V.35**—An ITU-T standard describing a synchronous, physical-layer protocol used for communications between a network access device and a packet network. V.35 is most commonly used in the United States and in Europe.

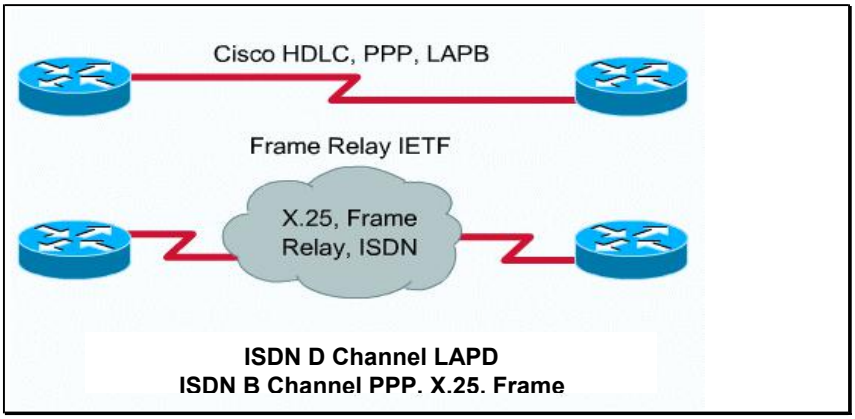
■**X.21**—An ITU-T standard for serial communications over synchronous digital lines. The X.21 protocol is used primarily in Europe and Japan.

■**G.703**—An ITU-T electrical and mechanical specification for connections between telephone company equipment and DTE using British Naval connectors (BNCs) and operating at E1 data rates.

■**EIA-530**—Two electrical implementations of EIA/TIA-449: RS-422 (for balanced transmission) and RS-423 (for unbalanced transmission).

WANs and Data Link Layer

Figure 1: WAN and Data Link Layer



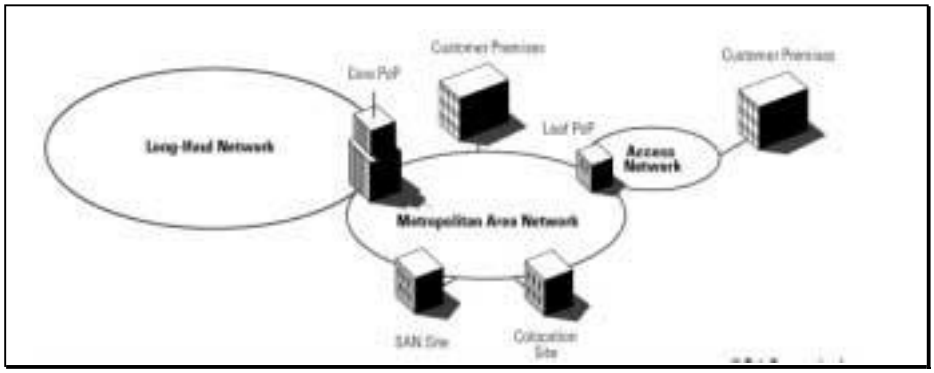
Data link layer protocols are designed to operate over dedicated point-to-point, multipoint, and multiaccess switched services such as Frame Relay. The common data link layer encapsulations associated with synchronous serial linesare listed in Figure [1].

- **Cisco High-Level Data Link Control (HDLC)**: This is an IEEE standard; it may not be compatible with different vendors because of the way each vendor has chosen to implement it. Cisco HDLC supports both point-to- point and multipoint configurations with minimal overhead.
- **Frame Relay**: Frame Relay uses high-quality digital facilities; it uses simplified framing with no error-correction mechanisms, meaning that it can send Layer 2 information much more rapidly than other WAN protocols.
- **Point-to-Point Protocol (PPP)**: This protocol is described by RFC 1661; two standards were developed by the Internet Engineering Task Force (IETF); PPP contains a protocol field to identify the network layer protocol.
- **Simple Data Link Control Protocol (SDLC)**: This protocol is an IBM- designed WAN data link protocol for Systems Network Architecture (SNA) environments; it is largely being replaced by the more versatile HDLC.
- **Serial Line Interface Protocol (SLIP)**: This is a very popular WAN data link protocol for carrying IP packets; it is being replaced in many applications by the more versatile PPP.
- **Link Access Procedure, Balanced (LAPB)**: This data link protocol is used by X.25; it has extensive error-checking capabilities.
- **Link Access Procedure on the D channel (LAPD)**: This WAN data link protocol is used for signaling and call setup on an ISDN D-channel. Data transmissions take place on the ISDN B channels.
- **Link Access Procedures to Frame mode bearer services (LAPF)**: This protocol is for Frame Relay mode bearer services; similar to LAPD, this WAN data link protocol is used with Frame Relay technologies.

2.3 Other Types of Networks

MAN

Figure 1: A MAN



A metropolitan-area network (MAN) is a network that spans a metropolitan area such as a city or suburban area. A MAN usually consists of two or more LANs in a common geographic area. A bank with multiple branches may utilize a MAN. Typically, a service provider is used to connect two or more LAN sites, using T1 private lines or optical services. A MAN can also be created using wireless bridge technology by beaming signals across public areas. The higher optical bandwidths that are currently available make MANs a more functional and economically feasible option than in the past.

Traditionally, most MANs have been designed using either Synchronous Optical Network (SONET) or its close cousin Synchronous Digital Hierarchy (SDH). SONET and SDH are self-healing network architectures that prevent interruption in service by rerouting traffic almost instantaneously in the event of a fiber cut. A ring topology, however, requires provisioning for the maximum bandwidth required in the network on every segment, irrespective of the actual load on the segment.

StorageArea Networks

Figure 1: A Storage Area Network

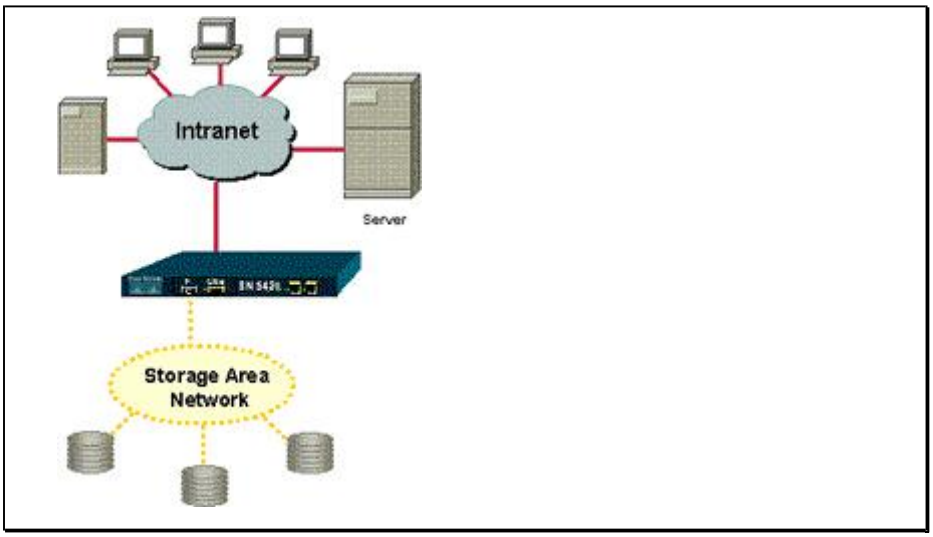


Figure 2: Cisco SN 5420 Router

A storage area network (SAN) is a dedicated high performance network to move data between heterogeneous servers and storage resources. Being a separate dedicated network, it avoids any traffic conflict between clients and servers (see Figure **[1]**).

Adopting SAN technology through the use of *Fibre Channel* and hubs and switches allows high-speed server-to-storage, storage-to-storage, or server-to-server connectivity using a separate network infrastructure which mitigates problems associated with existing network connectivity.
Note: Fibre Channel is a technology for transmitting data between computer devices at a data rate of up to 1 billion bit per second (Gbps). Fibre Channel is especially suited for connecting computer servers to shared storage devices and for interconnecting storage controllers and drives.
SANs also have the potential to allow cable lengths up to 500 meters today and up to 10 km in future so servers in different buildings can share external storage devices. And because the new emerging SAN/VIA (virtual interface architecture) interconnects have low latency and lesser overhead as compared to traditional LAN/WAN networks, they are ideally suited for clustering and mirroring/replication applications.

The features of SANs include:

■**Performance**—SAN enables concurrent access of disk or tape arrays by two or more servers at high speeds across Fibre Channel, providing much enhanced system performance.

■**Availability**—SAN has disaster tolerance built in since data can be mirrored using Fibre Channel SAN up to 10 km away.

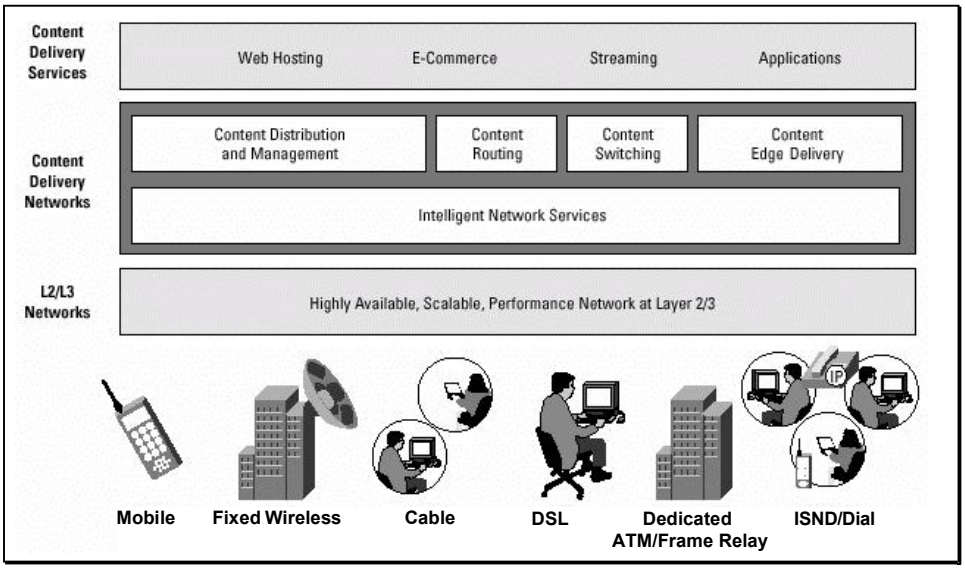
■**Cost**—Since SAN is an independent network, initial costs to set up the infrastructure will be higher but the potential exists for rapid cost erosion as SAN installed base increases.

■**Scalability**—Scalability is natural to SAN architecture, depending on the SAN network management tools used for interoperability. Like a LAN/WAN it can use a variety of technologies. This allows easy relocation of backup data, restore operations, file migration and data replication between heterogeneous environments.

■**Manageability**—SAN is data centric and uses thin protocol for low latency.

Content Networks

Figure 1: Content Networks



A content network is a globally coordinated network of devices designed to accelerate the delivery of information over the Internet infrastructure. By taking advantage of services in the core IP network and Layers 4–7 content-aware capabilities, enterprises and service providers are able to accelerate and improve the use of rich content, such as broadband streaming media, improve network performance, and eliminate the stream of rich media on the infrastructure. Content networks bypass potential sources of congestion by distributing the load across a collection of content engines located close to the viewing audience. RichWeb and multimedia content is replicated to the content engines and users are routed to an optimal content engine. The Cisco content networks solution is a tiered solution that starts with highly reliable and available Layer 2 and Layer 3 networks delivered by the Cisco IOS® Software core network. The Cisco content networks solution is defined in five major technology categories:

1. **Content Distribution and Management**
   Distributes content to the network edge and provides the Business/Operations Support System (BSS/OSS) for the content networks service

2. **Content Routing**
   Locates the optimum site to serve a specific content request based on network topology, network latency, server load, and policy

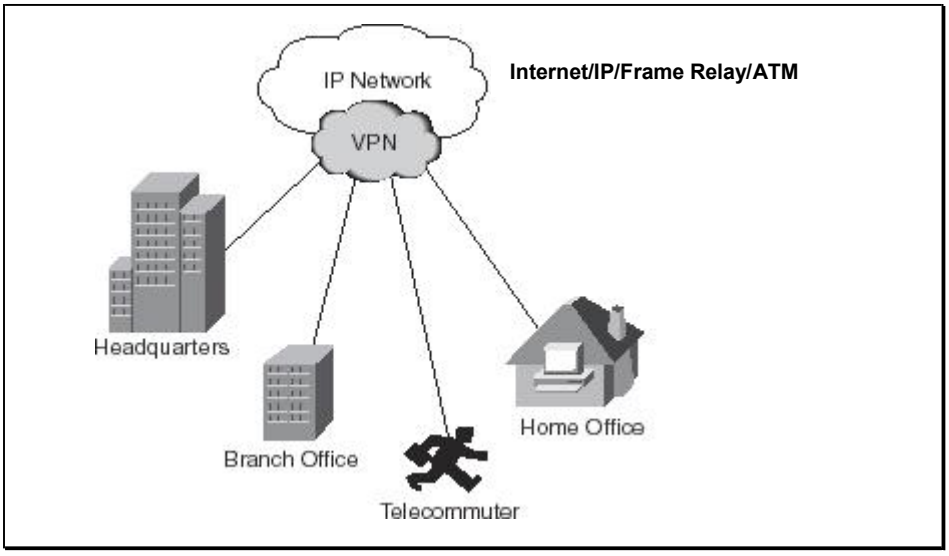
3. **Content Switching**
   Selects the best server within that site to deliver the content request based not only on server availability and load, but also on verification of content and application availability; it provides content services based on end-user session and the specific content requested

4. **Content Edge Delivery**
   Delivers static and streaming content at the network edge and keeps the content continuously fresh

5. **Intelligent Network Services**
   Augments the content networks with IP core services such as Layer 3 QoS, VPNs, security, and multicast—key features that content networks builders can take full advantage of

Virtual Private Network

Figure 1: VPN Components



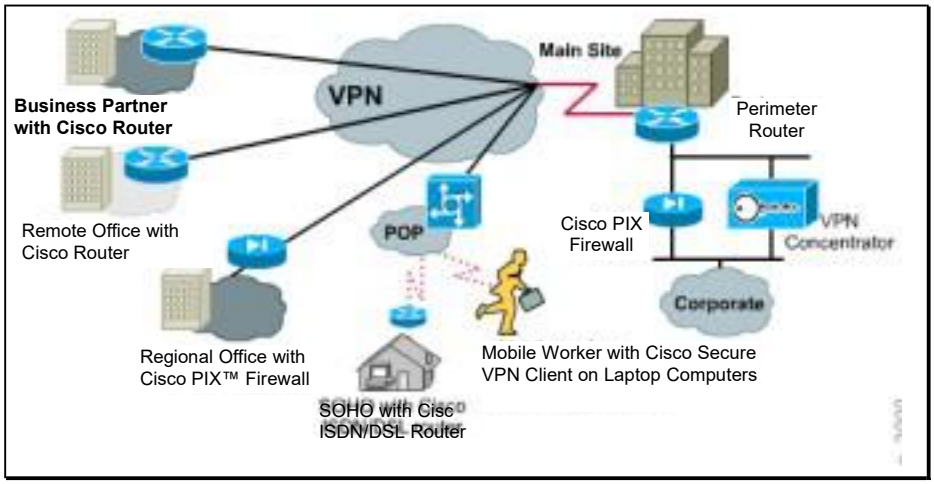
A virtual private network (VPN) is a communications environment in which access is controlled to permit peer connections only within a defined community of interest. It is constructed through some form of partitioning of a common underlying communications medium. This communications medium provides services to the network on a nonexclusive basis. A simpler, more approximate, and less formal definition of a VPN follows:

A VPN is private network that is constructed within a public network infrastructure, such as the global Internet.

Although VPNs might be constructed to address numerous specific business needs or technical requirements, a comprehensive VPN solution provides support for dial in and other remote access, the capability of the VPN service provider to host various services for the VPN customers (for example, Web hosting), and the capability to support not just intra-VPN connectivity, but also inter-VPN connectivity, including connectivity, to the global Internet.

Benefits of VPNs

Figure 1: VPN Technologies



Virtual private networking has significant advantages over previous forms of channel encryption and alternatives. Some of these advantages follow:

■ A single virtual private networking technology can provide privacy for multiple TCP/IP applications Application-level encryption requires different methods for different services. Support for multiple protocols is also possible through tunneling IP using the Point-to-Point Tunneling Protocol (PPTP), the Layer 2 Tunneling Protocol (L2TP), or the Layer 2 Forwarding (L2F) protocol. Providing privacy for multiple TCP/IP applications is especially important in environments in which you want to provide secure access for partners or elecommuters.

■ Encryption services can be provided for all TCP/IP communications between the trusted client and the virtual private networking server. This scenario has the advantage of being transparent to the end user. Because encryption is turned on, the server can enforce it. Cisco products support the latest in VPN technology. A VPN is a service that offers secure, reliable connectivity over a shared public network infrastructure such as the Internet. VPNs maintain the same security and management policies as a private network. They are the most cost-effective method of establishing a point-to-point connection between remote users and an enterprise customer's network. There are three main types of VPNs:

- **Access VPNs**: Access VPNs provide remote access to an enterprise customer's intranet or extranet over a shared infrastructure. Access VPNs use analog, dial, ISDN, digital subscriber line (DSL), mobile IP, and cable technologies to securely connect mobile users, telecommuters, and branch offices.
- **Intranet VPNs**: Intranet VPNs link enterprise customer headquarters,remote offices, and branch offices to an internal network over a shared infrastructure using dedicated connections. Intranet VPNs differ from extranet VPNs in that they allow access only to the enterprise customer's employees.
- **Extranet VPNs**: Extranet VPNs link outside customers, suppliers, partners, or communities of interest to an enterprise customer's network over a shared infrastructure using dedicated connections. Extranet VPNs differ from extranet VPNs in that they allow access to users outside the enterprise.

VPN Topologies

Figure 1: Intranets

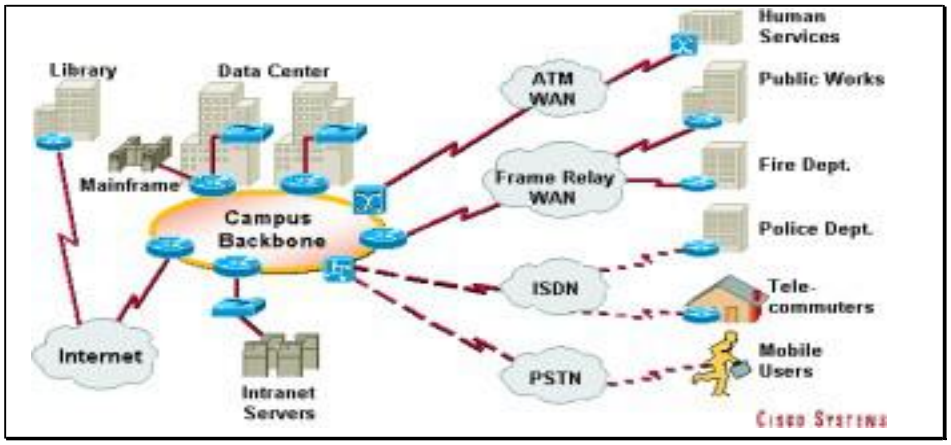
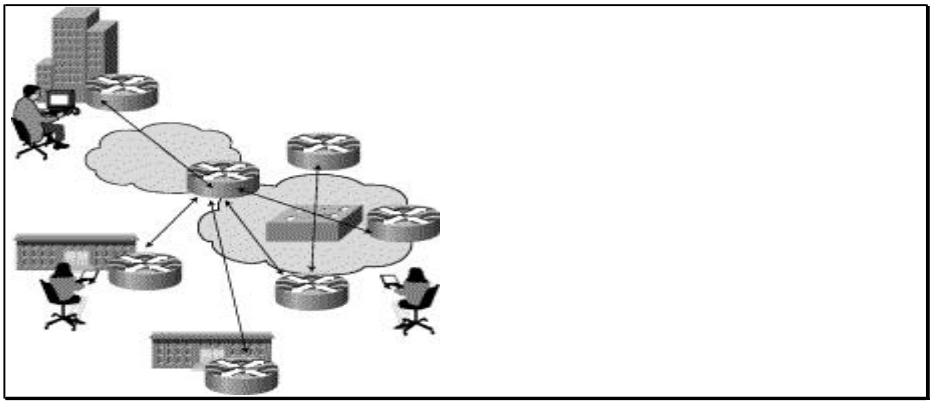


Figure 2: Extranets



Intranets [1]

One common configuration of a LAN is an intranet. Intranet Web servers differ from public Web servers in that, without the needed permissions and passwords, the public does not have access to an organization's intranet. Intranets are designed to be accessed by users who have access privileges to an organization's internal LAN. Within an intranet, Web servers are installed in the network, and browser technology is used as the common front end to access information, such as financial data or graphical, text-based data stored on those servers.

The addition of an intranet on a network is just one of many application and configuration features that can cause an increase in needed network bandwidth over current levels. Because bandwidth has to be added to the network backbone, network administrators should also consider acquiring robust desktops to get faster access into intranets. New desktops and servers should be outfitted with 10/100- Mbps Ethernet network interface cards (NICs) to provide the most configuration, flexibility, thus enabling network administrators to dedicate bandwidth to individual end stations as needed.

Extranets [2]

Extranets refer to applications and services that were intranet based but employed extended, secured access to external users or enterprises. This access is usually accomplished through passwords, user IDs, and other application level security mechanisms. Therefore, an extranet is the extension of two or more intranet strategies with a secure interaction between participant enterprises and their respective intranets.

The extranet maintains control of access to those intranets within each enterprise in the deployment. Extranets link customers, suppliers, partners, or communities of interest to a corporate intranet over a shared infrastructure using dedicated connections. Businesses use the same policies as a private network, including security, quality of service (QoS), manageability, and reliability.